FOREWORD

REDEFINING NATIONAL SECURITY IN TODAY'S WORLD OF INFORMATION TECHNOLOGY AND EMERGENT THREATS

WALTER GARY SHARP, SR.*

We are at war—right now. We are in a cyberwar.

The Honorable John J. Hamre[1]
U.S. Deputy Secretary of Defense
23 February 1999

The disintegration of the Soviet Union has radically transformed threats to international peace and security as well as traditional notions of national security. Over the last decade, the sudden void of political restraints imposed during the previous forty-four years of a United States—Soviet Union bipolar world has fueled the proliferation of weapons of mass destruction and their long-range missile delivery systems, the increase of intrastate ethnic conflict and the Balkanization of states, the threat of terrorism, and the transnational influence of organized crime. Advances in information technology have aided the spread of these emergent threats to international peace and security, and have dramatically enhanced their synergy.

Information technology, particularly the Internet, creates vulnerabilities that constitute an emergent threat to international peace and security. Although not as patently destructive as more traditional threats such as the terrorist use of weapons of mass destruction, the new vulnerabilities created by information technology will have a far more profound effect on international peace and security and traditional notions of national security than the end of the United States—Soviet Union bipolar world.

---

* Principal National Security Policy Analyst, Aegis Research Corporation, Falls Church, Virginia; and Adjunct Professor of Law, Georgetown University Law Center. The opinions and conclusions expressed herein are those of the author and do not necessarily reflect the views of any governmental agency or private enterprise.

1. John Donnelly & Vince Crawley, *Hamre To Hill: 'We're In A Cyberwar,'* DEF. WK., Mar. 1, 1999, at 1.

The open architecture of the Internet is ideally suited for asymmetrical warfare, corporate espionage, and criminal activity. States, private industry, and individuals are all vulnerable—either from the information they voluntarily post on the Internet or from unauthorized access of their information systems that are intended to be closed to the public. Dedicated and persistent CyberSpace[2] actors such as recreational hackers, corporations seeking a competitive advantage, organized criminals, terrorists, and states can now gain access to almost *any* Internet-linked information infrastructure in the world. These trespassers can anonymously pry into a state's public, sensitive, and classified computers; collect a wide range of government and business information; steal and transfer money out of bank accounts; steal long-distance phone services or eavesdrop on conversations; manipulate any electronic data such as pre-launch telemetry calculations for space programs; interfere with air traffic control or emergency services; cause train wrecks or oil spills; deceive decision makers; influence public opinion; and cause physical destruction from remote locations abroad. Execution of an organized, large-scale attack against a state or a business can begin anonymously with the stroke of a single key on a computer keyboard, with commands being delivered around the world literally at the speed of light.

Information technology has markedly changed traditional notions of national security in two ways. First, it has made the daily operation of state governments more dependent upon private industry and commercial infrastructures, while at the same time, it has made the nongovernment sector more accessible and vulnerable to cyberattack. Indeed, a state's private industry and critical infrastructures are now its soft underbelly—easier to exploit than hardened government targets. Second, private industry and critical infrastructures are so inter-linked and interdependent that an organized attack could potentially have a significant adverse impact on the ability of a state to defend itself or to maintain its economic vitality in a global market. The United States, for example, declared in Executive Order 13010 that eight categories of "national [commercial] infrastructures are so vital that their incapacity or destruction [by either physical or cyberattack] would have a debilitating impact on the defense or economic security of the United States."[3] These eight categories defined by

2. I define CyberSpace as: the environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the Internet and the World Wide Web.

3. Exec. Order No. 13,010, 61 Fed. Reg. 37, 47 (1996).

Executive Order 13010 are telecommunications, electrical power systems, gas and oil storage, transportation, banking and finance, water supply systems, emergency services (including medical, police, fire and rescue), and continuity of government.[4] Attacks on the private industry and commercial infrastructures of a state are now inextricably linked with the national security of that state more than ever before.

Governments and private industry overlooked these cyber vulnerabilities in their rush to take advantage of the extraordinary benefits of the Internet and the World Wide Web. Only in the last few years has the U.S. Government publicly acknowledged what private industry is still reluctant to accept. During the military exercise *Eligible Receiver* in June 1997, for example, the U.S. National Security Agency demonstrated that a hostile enemy state could disrupt computer operations at major U.S. military commands, cause large-scale blackouts in the commercial sector, and interrupt emergency phone service in major cities in the United States.[5] The following year, the United States acknowledged that two California teenagers with an Israeli mentor broke into sensitive DoD systems in February 1998 and eluded U.S. law enforcement authorities for nearly a month.[6] Although they did not compromise national security or penetrate any classified systems, their attacks highlighted sensitive vulnerabilities during the planning for military airstrikes in Iraq.[7] In February 1999, the Deputy Secretary of Defense testified during a closed session before two House National Security Committee panels that military computer systems are under siege by a coordinated, organized attack by an unknown source—in short, the United States is "in a cyberwar."[8]

In an effort to foster public debate and increase awareness within private industry, as well as explore how to shape the rule of law to protect a nation's information infrastructures, the Duke University School of Law hosted a major two-day conference on April 20-21, 1998, entitled *National Information Infrastructure Protection in the 21st Century*. This conference was co-sponsored by the Center on Law, Ethics and National Security, Duke University School of Law;

---

4. *See id.*

5. Bradley Graham, *U.S. Studies New Threat: Cyber Attack*, WASH. POST, May 24, 1998, at A1.

6. *See id.*

7. *See id.*

8. Donnelly & Crawley, *supra* note 1, at 1.

the Center for National Security Law, University of Virginia School of Law; and Aegis Research Corporation, Falls Church, Virginia. The principal theme of the conference was to identify emerging roles for industry and government in protecting the information infrastructures of the United States from cyber threats.

Before an audience of over two hundred attendees, the conference assembled distinguished speakers and panelists for discussion and debate over the responsibilities and roles of industry and government in protecting information infrastructures, the threat of economic warfare and corporate espionage, the potential contours of information conflict in the 21st Century, the role of encryption in protecting information, and how to respond and recover from a cyberattack.

This conference was the first of its kind that provided a detailed overview of all of the major issues in protecting the United States information infrastructure. This overview included an introduction to why our society is vulnerable to cyberattack, how the government is increasingly dependent upon private industry and commercial infrastructures, the seminal work on information assurance by the Congress of the United States, the work of the President's Commission on Critical Infrastructure Protection, how the draft Presidential Decision Directive that was under interagency review at the time of the conference would implement the work of the President's Commission, and the many varied implications for the legal community. The legal implications discussed ranged from online commercial law, constitutional issues concerning privacy and warrantless searches, economic warfare and corporate espionage, encryption, future targeting issues under the law of armed conflict, and response and reconstruction. The three principal conclusions that ran throughout the conference reflected the rapidly evolving role of private industry in the national security of the United States, the fundamental importance of a partnership between private industry and government, and the critical need for sharing information between private industry and the government.

This issue of the *Duke Journal of Comparative & International Law* includes the keynote presentation of Congressman Goss and three articles addressing a number of the major challenges involved in protecting a nation's critical infrastructure from cyberattack raised at the Conference.

Congressman Goss, one of the first leaders on Capitol Hill who became concerned about the protection of our information infra-

structure, begins his presentation by observing most people are complacent or apathetic about our national security and distrustful of the government despite the fact that threats to the security of our nation are far more dangerous and complex than they were during the Cold War. He next highlights the alarming vulnerabilities of the Department of Defense information infrastructure revealed by exercise *Eligible Receiver* in June 1997 despite the artificial constraints imposed on the exercise attack team, and voices great concern over the danger of an "electronic Pearl Harbor" that could have occurred if the attack was conducted by a hostile adversary. He also calls for national leadership and a "consistent and comprehensive" foreign policy that will build the indications and warnings process, information assurance infrastructure, and public awareness necessary to defend the United States from cyberattack. Congressman Goss concludes his remarks with a discussion of the dangers that uncrackable encryption pose to our national security and law enforcement capabilities, and thus the legitimate need for court-sanctioned access to all suspect communications.

The rapidly evolving confluence of the technological leadership of American private industry and the information component of national security, and its simultaneous transformation into a "national information power" strategy, are examined by Captain William Gravell, U.S. Navy, in his article entitled *Some Observations Along the Road to "National Information Power."* As one of the prescient engineers of the U.S. Government's construct of information warfare, Captain Gravell is uniquely qualified to begin his article with a description of information warfare and an organizational history of information. He describes a simple approach to information warfare that views information and associated technologies "as tools of great importance and power"—tools that we should enhance and protect when used by us and our friends, and that we should attack and degrade when used by our opponents. While offensive aspects of information warfare are uniquely governmental, Captain Gravell observes that the "persons, processes, and above all, equities" of information warfare defense inextricably embraces the commercial sector. Accordingly, the defense of our nation from cyberattack requires a sharing of information between industry and government that will enable the government to establish an "Indications and Warning" process that identifies an ongoing attack. Captain Gravell concludes his article with a visionary discussion of a "national information power" strategy that aggressively promotes and defends

America's informational goods and services. His discussion of this strategy is formulated around the question, "What are the Vital National Interests of the United States in the Information Age?" Since the clear direction of such a strategy is economic globalization, an author's note by Captain Gravell provides a brief overview of the principal issues guiding and pacing the international political and legal debate.

Perhaps the most contentious issue of the conference was addressed by F. Lynn McNulty in his article entitled *Encryption's Importance to Economic and Infrastructure Security*. This article provides a discussion of the diverse privacy, infrastructure protection, law enforcement, national security, and commercial equities that must be reconciled before a workable solution to the encryption issue is found. Contrary to the views of Congressman Goss, Mr. McNulty supports the unrestricted use of encryption for legitimate purposes. Mr. McNulty begins his article with a very important discussion of cryptography policy development—citing the reason for much of the public's distrust of the government on the encryption issue is due to the Clinton administration's key-escrow based Clipper chip proposal of 1993. His detailed discussion of the export policies of the United States demonstrates the practical futility of attempting to regulate encryption, and the corresponding cost in billions of dollars to the American encryption industry in the loss of market share. Mr. McNulty closes his article with a call for greater public debate and a more moderate approach by the U.S. Government.

The final article is a comprehensive discussion of the challenges that computer crime and cyberattacks present to the law enforcement community. In his article entitled *The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium*, Michael Sussmann describes the criminal potential of networked computers and the Internet as one of the most "systemic and pervasive" threats that the law enforcement community has ever faced. He asks the reader to imagine a criminal in Russia who hacks his way through information systems of Sweden and Italy to steal from a bank in New York, and then describes the awkward situation wherein that the FBI must have the assistance and cooperation of Russia, Sweden, and Italy to even begin to solve the crime. Complicating matters, Mr. Sussmann reports that many people do not realize the threat exists on such a global level and that "technical solutions, laws and legal processes, and cooperation among governments and with industry are far behind where they need to be for law enforcement to

stay a step ahead of the bad guys." This article defines computer crime, highlights the investigative challenges posed by transnational criminal activities, and makes a convincing argument that international cooperation among states is the only foundation for any effective national approach to solving computer crime. Mr. Sussmann defines what types of cooperation must be achieved by the international community to effectively combat computer crime, and concludes his article with a description of what is being done by the Department of Justice and multilateral organizations to combat computer crime.

The conference speakers and attendees were very successful in drawing out the complexities of the U.S. domestic issues involved in protecting our national information infrastructure and identifying what international cooperation must be achieved to protect the united States from cyberattack. And the contributors to this journal—Congressman Goss, Captain Gravell, Mr. McNulty, and Mr. Sussmann—have done a superb job in capturing the major challenges facing the United States as it struggles to understand how to protect its national information infrastructure in the 21st century.