Preface

The information infrastructure – comprising computers, embedded devices, networks and software systems – is vital to operations in every sector: information technology, telecommunications, energy, banking and finance, transportation systems, chemicals, agriculture and food, defense industrial base, public health and health care, national monuments and icons, drinking water and water treatment systems, commercial facilities, dams, emergency services, commercial nuclear reactors, materials and waste, postal and shipping, and government facilities. Global business and industry, governments, indeed society itself, cannot function if major components of the critical information infrastructure are degraded, disabled or destroyed.

This book, *Critical Infrastructure Protection II*, is the second volume in the annual series produced by IFIP Working Group 11.10 on Critical Infrastructure Protection, an active international community of scientists, engineers, practitioners and policy makers dedicated to advancing research, development and implementation efforts related to critical infrastructure protection. The book presents original research results and innovative applications in the area of infrastructure protection. Also, it highlights the importance of weaving science, technology and policy in crafting sophisticated, yet practical, solutions that will help secure information, computer and network assets in the various critical infrastructure sectors.

This volume contains twenty edited papers from the Second Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, held at George Mason University, Arlington, Virginia, March 17–19, 2008. The papers were selected from forty-two submissions, which were refereed by members of IFIP Working Group 11.10 and other internationally-recognized experts in critical infrastructure protection.

The chapters are organized into six sections: themes and issues, infrastructure security, control systems security, security strategies, infrastructure interdependencies, and infrastructure modeling and simulation. The coverage of topics showcases the richness and vitality of the discipline, and offers promising avenues for future research in critical infrastructure protection.

This book is the result of the combined efforts of several individuals and organizations. In particular, we thank Rodrigo Chandia and Eric Goetz for their tireless work on behalf of IFIP Working Group 11.10. We gratefully acknowl-

edge the Institute for Information Infrastructure Protection (I3P), managed by Dartmouth College, for nurturing IFIP Working Group 11.10 and sponsoring some of the research efforts whose results are described in this volume. We also thank the Department of Homeland Security and the National Security Agency for their support of IFIP Working Group 11.10 and its activities. Finally, we wish to note that all opinions, findings, conclusions and recommendations in the chapters of this book are those of the authors and do not necessarily reflect the views of their employers or funding agencies.

Mauricio Papa and Sujeet Shenoi

Chapter 2

CYBERSPACE POLICY FOR CRITICAL INFRASTRUCTURES

Dorsey Wilkin, Richard Raines, Paul Williams and Kenneth Hopkinson

Abstract The first step in preparing any battlespace is to define the domain for attack and maneuver. The various military service components have directed authority to focus their efforts in specific domains of operations (e.g., naval operations are mainly in the maritime domain). However, cyberspace operations pose challenges because they span multiple operational domains. This paper focuses on U.S. cyberspace policy related to defending and exploiting critical infrastructure assets. Also, it examines the issues involved in delineating responsibility for U.S. defensive and offensive operations related to critical infrastructures.

Keywords: Critical infrastructure, cyberspace operations, policy

1. Introduction

Protecting and controlling cyberspace are daunting challenges. Cyberspace is pervasive and has no single owner or controller. Yet, practically every critical infrastructure component relies on cyberspace resources for its operation. Disruption of these resources can dramatically affect industry, government and the citizenry.

The U.S. Department of Defense (DoD) – like its counterparts in other countries – is responsible for providing the military forces needed to protect the nation's security. It is, therefore, critical to understand the DoD's roles and responsibilities associated with protecting critical infrastructure assets as well as exploiting those of an adversary in time of war.

This paper examines U.S. cyberspace policy related to defending and exploiting critical infrastructure assets. It traces the evolution of the definition of critical infrastructure from Executive Order 13010 in 1996 to Homeland Security Presidential Directive 7 in 2003. Also, it analyzes the issues involved in delineating responsibility for U.S. defensive and offensive operations focused on critical infrastructures.

Please use the following format when citing this chapter:

Wilkin, D., Raines, R., Williams, P. and Hopkinson, K., 2008, in IFIP International Federation for Information Processing, Volume 290; *Critical Infrastructure Protection II*, eds. Papa, M., Shenoi, S., (Boston: Springer), pp. 17–28.

2. Defining Critical Infrastructure

Several definitions of "critical infrastructure" have been articulated. For example, Moteff and Parfomak [10] define it as:

> "[t]he framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the [nation], the smooth functioning of government at all levels, and society as a whole."

However, in preparation for combat, it is imperative that the battlespace be well defined and scoped by the applicable authority. Furthermore, areas of responsibility must be explicitly delineated. To ensure proper coordination between government and the private sector in the area of critical infrastructure protection, nothing less than Presidential direction will suffice.

2.1 Executive Order 13010

Growing concerns about terrorism in the United States – largely due to the World Trade Center and Oklahoma City bombings in 1993 and 1995, respectively – led to serious efforts focused on protecting the nation's critical infrastructure assets. Meanwhile, the massive growth of the Internet during the 1990s changed the national defense focus from the physical realm to the cyber realm. To address these issues, President Clinton signed Executive Order (EO) 13010 on July 15, 1996 [6]. It emphasized that critical infrastructures "... are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."

EO 13010 expounded on previous documents by categorizing threats as "physical threats," which are threats to tangible property, or "cyber threats," which are threats of electronic, radio frequency or computer-based attacks on the information and/or communications components that control critical infrastructures.

EO 13010 identified the following infrastructure sectors: telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire and rescue) and continuity of government.

Finally, the order established the President's Commission on Critical Infrastructure Protection (PCCIP) that was tasked with assessing the scope and nature of the vulnerabilities and threats to U.S. critical infrastructures and recommending a comprehensive implementation strategy for critical infrastructure protection.

2.2 Presidential Decision Directive 63

In response to EO 13010, the PCCIP provided the following recommendations [13]:

Table 1. PDD 63 lead agency assignments.

Sector	**Lead Agency**
Information and Communications	Department of Commerce
Banking and Finance	Department of the Treasury
Water	Environmental Protection Agency
Aviation Highways Mass Transit Pipelines Rail Waterborne Commerce	Department of Transportation
Emergency Law Enforcement Services	Department of Justice/FBI
Emergency Fire Services Continuity of Government Services	Federal Emergency Management Agency
Public Health Services	Health and Human Services
Electric Power Oil and Gas Production and Storage	Department of Energy

- Conduct research and development in information assurance, monitoring and threat detection, vulnerability assessment and systems analysis, risk management and decision support, protection and mitigation, and incident response and recovery.

- Increase the federal investment in infrastructure assurance research to $500 million in FY99 and incrementally increase the investment over a five-year period to $1 billion in FY04.

- Establish a focal point for national infrastructure assurance research and development efforts and build a public/private-sector partnership to foster technology development and technology transfer.

Acting on the PCCIP recommendations, President Clinton signed Presidential Decision Directive (PDD) 63 on May 22, 1998, mandating law enforcement, foreign intelligence and defense preparedness to achieve and maintain critical infrastructure protection [7]. PDD 63 was the first document to assign lead agency responsibilities for critical infrastructure protection (Table 1). However, the DoD was not listed.

For three years, PDD 63 was the principal defining document for critical infrastructure protection. It was put to the test by the events of September 11, 2001.

2.3 Executive Orders 13228 and 13231

Responding to the lack of coordination before, during and after the terrorist attacks of September 11, 2001, President George W. Bush signed EO 13228 on October 8, 2001 that established the Office of Homeland Security [2]. The order gave the Office of Homeland Security the responsibility for coordinating the executive branch's efforts to detect, prepare, prevent, protect, respond and recover from terrorist attacks within the United States.

EO 13228 explicitly mentioned several critical infrastructure assets:

- Energy production, transmission and distribution services and critical facilities
- Other utilities
- Telecommunication systems
- Facilities that produce, use, store or dispose of nuclear material
- Public and privately owned information systems
- Special events of national significance
- Transportation systems, including railways, highways, shipping ports and waterways, airports and civilian aircraft
- Livestock, agriculture and systems for the provision of water and food for human use and consumption

EO 13228 designated many of the same critical infrastructure assets as PDD 63. However, it added nuclear sites, special events and agriculture.

On October 16, 2001, President Bush signed EO 13231 that created the President's Critical Infrastructure Protection Board (PCIPB) [3]. Like the PCCIP, the PCIPB was tasked with coordinating activities related to the protection of critical infrastructure assets and recovery from attacks. However, the PCIPB's primary function was to serve as the liaison between the President and the Office of Homeland Security. Interestingly, although EOs 13228 and 13231 stemmed from acts of terrorism launched by external enemies, the DoD was not mentioned in either executive order.

2.4 PATRIOT Act of 2001

The U.S. Congress passed the PATRIOT Act in 2001 that extended the capabilities of the newly created Office of Homeland Security. The act sought "[t]o deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes" [17]. In Section 1016 of the PATRIOT Act, known as the Critical Infrastructure Protection Act of 2001, Congress updated the definition of critical infrastructure as follows:

> "... systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

The act also appropriated $20 million to the DoD to ensure that any "physical or virtual disruption of the operation of the critical infrastructures of the United States [would] be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States."

The PATRIOT Act was the first document to give the DoD some responsibility for critical infrastructure protection. However, it did not give the DoD any authority or direction; these would eventually come from future documents.

2.5 National Strategy for Homeland Security

Executive Order 13228 created the Office of Homeland Security, the PATRIOT Act gave it broader authority and, on July 16, 2002, President George W. Bush signed the National Strategy for Homeland Security (NSHS) to organize and prioritize its efforts [11].

The NSHS used the same definition of critical infrastructure as the PATRIOT Act. However, it added chemical, postal and shipping services to the list of critical infrastructures identified by EO 13228 because they "help sustain our economy and touch the lives of Americans everyday." The NSHS specified eight major initiatives related to critical infrastructure protection:

- Unify America's infrastructure protection efforts in the Department of Homeland Security.
- Build and maintain a complete and accurate assessment of America's critical infrastructure and key assets.
- Enable effective partnerships with state and local governments and the private sector.
- Develop a national infrastructure protection plan.
- Secure cyberspace.
- Harness the best analytic and modeling tools to develop effective protective solutions.
- Guard America's critical infrastructure and key assets against "inside" threats.
- Partner with the international community to protect the transnational infrastructure.

The NSHS defined the lead agencies responsible for securing specific sectors of the U.S. critical infrastructure (Table 2). In particular, it modified the lead

Table 2. NSHS lead agency assignments [11].

Sector	Lead Agency
Agriculture	Department of Agriculture
Meat and Poultry	Department of Agriculture
Other Food Products	Department of Health and Human Services
Water	Environmental Protection Agency
Public Health	Department of Health and Human Services
Emergency Services	Department of Homeland Security
Continuity of Government	Department of Homeland Security
Continuity of Operations	All Departments and Agencies
Defense Industrial Base	Department of Defense
Information and Telecommunications	Department of Homeland Security
Energy	Department of Energy
Transportation	Department of Homeland Security
Banking and Finance	Department of the Treasury
Chemical Industry and Hazardous Materials	Environmental Protection Agency
Postal and Shipping	Department of Homeland Security
National Monuments and Icons	Department of the Interior

agencies designated by PDD 63 for all but three sectors. Also, it required agencies to report directly to the newly-created Department of Homeland Security (DHS). Created by the Homeland Security Act of November 25, 2002, DHS is a cabinet-level department that united 22 distinct federal entities and absorbed the responsibilities of the Office of Homeland Security.

The NSHS designated the DoD as the lead authority for the defense industrial base. Also, it extended the scope of critical infrastructure to include transnational systems and identified cyberspace security as a primary initiative. However, the NSHS did not define the domain of cyberspace.

2.6 National Strategy to Secure Cyberspace

In February 2003, the PCIPB released the National Strategy to Secure Cyberspace (NSSC) [14]. Developed as an implementation component of the NSHS, the NSSC is intended to "engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact."

The NSSC specifically defines cyberspace as the "hundreds of thousands of interconnected computers, servers, routers, switches and fiber optic cables that make ... critical infrastructures work." Cyberspace is global in design and is, therefore, open to anyone, anywhere in the world. Under the NSSC, the primary strategic objective is to prevent cyber attacks against America's critical infrastructures. This is to be accomplished by delving deeper into the

defense of critical infrastructures in order to detail cyber vulnerabilities and to develop strategies for mitigating attacks.

The NSSC is currently the highest-level document to identify digital control systems (DCSs) and supervisory control and data acquisition (SCADA) systems as vital to operations in the various critical infrastructure sectors. In its Security Threat and Vulnerability Reduction Program, the NSSC states that securing DCSs and SCADA systems is a national priority because "... the incapacity or destruction of [these] systems and assets would have a debilitating impact."

The NSSC is the first government document to mention offensive cyber operations as a response to cyber attacks. (Up to this point, government documents only focused on defensive operations related to critical infrastructure protection.) In particular, the NSSC states:

> "When a nation, terrorist group or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner. The United States will be prepared for such contingencies."

Finally, the NSSC lists the major risk factors involved in securing critical infrastructures from cyberspace attacks. It observes that cyberspace-related vulnerabilities persist because security implementations require investments that companies cannot afford, security features are not easily adapted to the space and/or power requirements of small systems, and security measures often reduce performance and impact the synchronization of large real-time processes.

2.7 Homeland Security Presidential Directive 7

On December 17, 2003, President George W. Bush signed the Homeland Security Presidential Directive (HSPD) 7 [4], which superseded PDD 63. HSPD-7 is the most up-to-date executive document on critical infrastructure identification, prioritization and protection. It uses the same definition for critical infrastructure as the PATRIOT Act and lists the same sectors and lead agencies as the NSHS.

HSPD-7 ordered all federal departments and agencies to develop plans for protecting the critical infrastructures that they own or operate by July 2004. These plans had to address the identification, prioritization, protection and contingency planning (including the recovery and reconstitution of essential capabilities) of all physical and cyber resources.

2.8 Defense Critical Infrastructure Program

In response to HSPD-7, DoD Directive 3020.40 [8] was issued on August 19, 2005 to update policy and assign responsibilities for the Defense Critical Infrastructure Program (DCIP). The directive defines the defense critical infrastructure as "DoD and non-DoD networked assets essential to project, support and sustain military forces and operations worldwide."

Table 3. DCIP lead agency assignments.

Assignment	Lead Agency
Defense Industrial Base	Defense Contract Management Agency
Financial Services	Defense Finance and Accounting Service
Global Information Grid	Defense Information Systems Agency
Health Affairs	Assistant Secretary of Defense for Health Affairs
Intelligence, Surveillance and Reconnaissance	Defense Intelligence Agency
Logistics	Defense Logistics Agency
Personnel	DoD Human Resources Activity
Public Works	U.S. Army Corps of Engineers
Space	U.S. Strategic Command
Transportation	U.S. Transportation Command

The DCIP identifies ten critical sectors and the lead agencies responsible for the sectors (Table 3). It also requires the Secretary of every military department to designate an Office of Primary Responsibility (OPR) for identifying, prioritizing and protecting defense critical infrastructure assets.

3. Offensive Cyber Operations Authority

While defensive measures can protect critical infrastructures, deterrence is not achieved purely by defensive means. History has shown that, in most cases, offensive operations achieve better results than adopting a completely defensive posture where attacks are simply endured. If military power is used, the Law of Proportionality may dictate that an offensive cyber capability be used "in kind". The NSSC states that when an "adversary attacks the [United States] through cyberspace ... [it] reserves the right to respond in an appropriate manner" [14]. The Commander of the U.S. Strategic Command (STRATCOM) has testified to Congress that "a purely defensive posture poses significant risks" and "the defense of the nation is better served by capabilities enabling [it] to take the fight to [its] adversaries" [5]. A computer network attack capability is necessary to ensure the defense of critical infrastructures. Cyberspace superiority is achieved by simultaneously exploiting the adversary's critical infrastructure assets.

3.1 Civilian Authority

In accordance with current law, HSPD-7 and the NSHS, the Department of Homeland Security (DHS) is the single accountable entity with the "responsibility for coordinating cyber and physical infrastructure protection efforts" [11]. DHS has created red teams for testing critical infrastructure defenses and training personnel in the private and public sectors [16]. Could DHS red teams be used to attack an adversary's critical infrastructure assets?

The technology exists for DHS red teams to conduct offensive operations well inside U.S. (or friendly) borders. However, important legal issues must be considered before civilians may conduct offensive cyber operations.

The Law of Armed Conflict comprises the Geneva Conventions, the Hague Conventions, various treaties and a vast body of case law. The law incorporates several rules that govern the use of civilians during times of war [12]. If a civilian uses software to infiltrate an adversary's critical infrastructure and negatively impact its citizens, the adversary can legally view the infiltration as an "attack" under Article 49.1. According to Article 52.2, software may be classified as a weapon when used in an attack on a critical infrastructure target because "[its] nature, location, purpose or use make [it] an effective contribution to military action." Also the civilian is a combatant under Article 51.3 because "civilians shall enjoy the protection afforded by [the Geneva Convention], unless and for such time as they take a direct part in hostilities."

Civilians who are designated as combatants can face serious problems if apprehended by an adversary. Under Articles 44.3 and 44.4, if a civilian combatant does not distinguish himself from the civilian population while engaged in an attack and if he is apprehended by the adversary while failing to distinguish himself, he would forfeit his right to be a prisoner of war. Of course, under Article 45.2, he would have the right to assert his entitlement to prisoner-of-war status before a judicial tribunal and to have that question adjudicated. The tribunal may then consider the civilian as a lawful combatant under Article 44.3 of Protocol I of the Geneva Convention [12] or as an unlawful combatant and label him a spy, mercenary or terrorist. An unlawful combatant is not a prisoner of war and can be tried and punished in accordance with local laws. He could be executed by firing squad like the mercenaries in Angola in 1976 [1].

3.2 Department of Defense Authority

Although EO 13010 raised the issue of using cyber operations to attack critical infrastructure assets as far back as 1996, it was not until 2001 that the Quadrennial Defense Review identified information operations (IO), which includes cyber operations, as a core capability of future military forces [15]. The concept was codified on May 3, 2002, when then Secretary of Defense Rumsfeld signed the classified Defense Planning Guidance (DPG 04) for the fiscal years 2004 through 2009 [15]. DPG 04 directed that "IO become a core military competency, fully integrated into deliberate and crisis action planning and capable of executing supported and supporting operations." Furthermore, it mandated that the Chairman of the Joint Chiefs of Staff develop an "IO Roadmap" that would address the full scope of IO as a core competency and include supporting studies focused on policy, plans, organization, education, career force, analytic support, psychological operations, operations security, electronic warfare, military deception and computer network operations.

The Unified Command Plan 02 (Change 2) was approved by the President on January 2, 2003. It identified six core IO capabilities: computer network attack (CNA), computer network defense (CND), electronic warfare (EW), op-

eration security (OPSEC), psychological operations (PSYOPS) and military deception (MILDEC) [15]. Furthermore, it created the new office of the Under Secretary of Defense (Intelligence) within the Office of the Secretary of Defense for IO matters. STRATCOM was assigned as the combatant command responsible for "integrating and coordinating DoD IO that cross geographic areas of responsibility or across the IO core capabilities." Subsequently renamed as Offensive Cyber Operations, STRATCOM was responsible for "identifying desired characteristics and capabilities for CNA, conducting CNA in support of assigned missions and integrating CNA capabilities in support of other combatant commanders, as directed."

The IO Roadmap developed in response to DPF 04 was approved by Defense Secretary Rumsfeld October 30, 2003. It concluded that DoD must "fight the net" by improving CNA capability [15]. It recommended STRATCOM as the combatant command responsible for centralized IO planning, integration and analysis. Also, it specified that all the military services, including the Special Operations Command must organize, train and equip personnel for assignment to STRATCOM. Finally, it recommended that IO become "a dedicated military occupation specialty or career field" by designating service and joint IO billets.

Currently, the six IO core competencies are not universally defined, understood or applied. However, even if they were defined, each service would develop IO specialists that would meet its specific requirements. Also, the IO specialist communities within the services are relatively isolated. This results in a lack of knowledge for command-level IO planners and a gap between combatant command needs and what is provided by the services.

Entry-level IO personnel have limited, if any, experience in the discipline and require significant on-the-job training [15]. Unfortunately, none of the military services are mandated by Title 10 law to provide resources for IO training. Therefore, STRATCOM can request IO personnel from the services, but the services are not required by applicable law to expend their resources to train the IO personnel. For these reasons, the IO career force is progressing slower than desired.

3.3 U.S. Air Force Authority

On December 8, 2005, the Secretary of the Air Force and the Chief of Staff of the Air Force released a new mission statement that added cyberspace to the Air Force's core responsibilities. When asked why the Air Force was taking the lead for cyberspace, the Air Force Secretary stated that "the Air Force is a natural leader in the cyber world and we thought it would be best to recognize that talent" [9]. This statement may be true, but it does not recognize the lack of IO direction in the other services and the need for one service to take the lead in organizing, training and equipping an IO force. If IO is to become a new warfighting domain on par with land, sea and air, then the personnel and equipment ought to come from a single service. This follows from the service structure set forth by the Goldwater-Nichols Act of 1986. Also, when multiple services are responsible for the same mission, different techniques, tactics,

procedures and equipment are developed that not interoperable. Numerous instances of these interoperability problems were encountered during the military efforts in Vietnam, Grenada, Panama and Iraq [18].

The Air Force has taken charge of the cyberspace domain without Title 10 authority or executive directive. In a September 6, 2006 memorandum to all the major Air Force commands, the Air Force Secretary and the Chief of Staff ordered the creation of a new operational command with the sole purpose of organizing, training and equipping cyberspace forces for combatant commanders and STRATCOM. The 8th Air Force created a provisional Cyberspace Command in September 2007. On par with the Air Combat Command and Space Command, this new major command is scheduled for permanency by October 1, 2008. But only time will tell if the Air Force's authority over the cyber realm will, in fact, endure.

4. Conclusions

Legal and policy issues related to cyberspace operations are still not completely clear. However, what is clear is that military and civilian organizations must be afforded the resources commensurate with the importance of critical infrastructure protection. The strategic importance of offensive cyberspace operations cannot be overstated. The U.S. Department of Defense has recognized cyberspace as a domain for attack and maneuver and has begun to integrate it into wartime planning. Humankind is on the cusp of a new method of warfare and only time will reveal its viability.

References

[1] BBC News, On this Day (11 June 1976): Mercenaries trial begins in Angola, London, United Kingdom, (news.bbc.co.uk/onthisday/hi/dates/stories/june/11/newsid_2510000/2510947.stm).

[2] G. Bush, Executive Order 13228: Establishing the Office of Homeland Security and the Homeland Security Council, The White House, Washington, DC (fas.org/irp/offdocs/eo/eo-13228.htm), October 8, 2001.

[3] G. Bush, Executive Order 13231: Critical Infrastructure Protection in the Information Age, The White House, Washington, DC (fas.org/irp/offdocs/eo/eo-13231.htm), October 16, 2001.

[4] G. Bush, Homeland Security Presidential Directive (HSPD) 7, The White House, Washington, DC (www.whitehouse.gov/news/releases/2003/12/20031217-5.html), December 17, 2003.

[5] J. Cartwright, Statement of General James E. Cartwright, Commander, United States Strategic Command on the United States Strategic Command, House Armed Services Committee, U.S. House of Representatives, Washington, DC (armedservices.house.gov/pdfs/FC032107/Cartwright_Testimony032007.pdf), March 21, 2007.

[6] W. Clinton, Executive Order 13010: Critical Infrastructure Protection, The White House, Washington, DC (www.fas.org/irp/offdocs/eo13010.htm), July 15, 1996.

[7] W. Clinton, Presidential Decision Directive 63, The White House, Washington, DC (fas.org/irp/offdocs/pdd/pdd-63.htm), May 22, 1998.

[8] G. England, DoD Directive 3020.40, Defense Critical Infrastructure Program, Department of Defense, Washington, DC (www.dtic.mil/whs/directives/corres/pdf/302040p.pdf), August 19, 2005.

[9] M. Gettle, Air Force releases new mission statement, Air Force Link, U.S. Air Force, Washington, DC (www.af.mil/news/story.asp?storyID=123013440), December 8, 2005.

[10] J. Moteff and P. Parfomak, Critical Infrastructure and Key Assets: Definition and Identification, Congressional Research Service, The Library of Congress, Washington, DC (www.fas.org/sgp/crs/RL32631.pdf), 2004.

[11] Office of Homeland Security, National Strategy for Homeland Security, The White House, Washington, DC (www.whitehouse.gov/homeland/book/nat_strat_hls.pdf), 2002.

[12] Office of the United Nations High Commissioner for Human Rights, Protocol additional to the Geneva Conventions of 12 August 1949 and relating to the protection of victims of international armed conflicts (Protocol I), Geneva, Switzerland (www.unhchr.ch/html/menu3/b/93.htm), June 8, 1977.

[13] President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, The White House, Washington, DC (chnm.gmu.edu/cipdigitalarchive/files/5_CriticalFoundationsPCCIP.pdf), 1997.

[14] President's Critical Infrastructure Protection Board, The National Strategy to Secure Cyberspace, The White House, Washington, DC (www.whitehouse.gov/pcipb/cyberspace_strategy.pdf), 2003.

[15] D. Rumsfeld, Information Operations Roadmap (declassfied in 2006), Department of Defense, Washington, DC (www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf), 2003.

[16] Sandia National Laboratories, Information Design Assurance Red Team (IDART), Albuquerque, New Mexico (www.idart.sandia.gov).

[17] U.S. Congress (107th Congress), Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Public Law 107-56, Government Printing Office, Washington, DC (frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf), October 26, 2001.

[18] WGBH Educational Foundation, Frontline: Rumsfeld's War: The Military's Struggles and Evolution, Boston, Massachusetts (www.pbs.org/wgbh/pages/frontline/shows/pentagon/etc/cronagon.html), 2004.