NATIONAL DEFENSE UNIVERSITY

NATIONAL WAR COLLEGE

America's National Critical Infrastructure Assurance Plan:

Can Compromise Win in an Uncompromising World?

Stephen J. Werner / Class of 2000
Course 5603
Seminar M

Faculty Seminar Leader:
Mr. Hugh De Santis

Faculty Advisor:
Colonel Gene Powell

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2000	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
America's National Critical Infrastructure Assurance Plan: Can Compromise Win in an Uncompromising World?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University National War College Washington, DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**14**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

"We are at the dawn of a new century. Now is the moment to be farsighted as we chart a path into the new millennium."

— President William J. Clinton, "A National Security Strategy for a New Century," May 1997

"We must judge our national security strategy by its success in meeting the fundamental purposes set out in the preamble to the Constitution: '...provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity...' "

— "A National Security Strategy for a New Century," October 1998

The United States' Constitution was generated with considerable difference of opinion as to how the U.S. government ought to be organized, and was the product of significant compromise.[1] The Constitution established a federal government of separate institutions sharing powers—a system of checks and balances that throughout U.S. history, has fostered tension among these branches of government. Yet, in order to effect policy for U.S. national interests, this form of government has also required a mix of cooperation and compromise among the branches. The National Critical Infrastructure Assurance Plan[2] is likewise the product of significant coordination and compromise among the branches of government, as well as numerous industry players and the American people.

---

[1] Collier, Christopher, and James L. Collier, *Decision In Philadelphia: The Constitutional Convention of 1787*, (New York, NY: Ballantine Books, 1986): x.

[2] The National Critical Infrastructure Assurance Plan is a requirement of Presidential Decision Directive 63 (Protecting America's Critical Infrastructures), and will be published in two parts. Part I, the National Plan for Information Systems Protection, will be published in January 2000. Part II, the Critical Physical Infrastructure Protection Program, will be published at a time to be determined.

This paper is but one chapter in a larger effort to analyze the effectiveness of the U.S. government's policies on Critical Infrastructure Protection (CIP)[3]. Using a practitioner's framework for decision making, I will describe the contextual elements, institutional equities, and spirit of compromise that led to Presidential Decision Directive 63 (PDD-63) and the National Critical Infrastructure Protection Plan.

Background—in the context of U.S. National Security Strategy

Protecting U.S. critical infrastructures has long been a subject of government concern. Dams, bridges, tunnels, power plants, and other important physical structures have been specially protected for more than 50 years.[4] Moreover, the Senate has frequently conducted hearings to explore the security status of various U.S. national physical infrastructures. In 1995, precipitated by the Oklahoma City bombing, President Clinton issued PDD-39. This directive was geared toward preventing domestic terrorism, and directed the Attorney General to lead a government-wide effort to re-examine the adequacy of our infrastructure protection.[5] The Attorney General's review highlighted vulnerabilities of America's physical infrastructures and significant gaps in protection of our cyber infrastructure: critical information systems and computer networks.

In a separate initiative, the National Security Advisor led an interagency working group (including DOD, DOJ, and DCI) to examine critical infrastructure vulnerabilities. Strong testimony to the Senate Committee on Government Affairs by former Deputy Attorney General Jamie Gorelick, and statements by Senators Levin, Leahy, and Kyl

---

[3] Critical Infrastructures include electrical power systems, telecommunications, gas/oil storage and transportation, banking and finance, water supply systems, transportation and emergency services, and, as appended by the PCCIP, government services.

[4] President, *Defending America's Cyberspace: National Plan for Information Systems Protection (Draft Version 1.0); An Invitation to a Dialogue*, (10 November 1999): xvi.

[5] President, *U.S. Policy on Counterterrorism: Presidential Decision Directive 39*, (24 January 1997).

further highlighted grave concerns with America's critical infrastructure protection capabilities. These events culminated in Executive Order 13010—issued in July 1996—which created the President's Commission on Critical Infrastructure Protection (PCCIP). The PCCIP was chartered to assess the scope and nature of the threats, identify legal and policy issues, recommend a comprehensive national policy and implementation strategy, and propose any necessary statutory or regulatory changes.[6]

The PCCIP consisted of representatives and experts from the various infrastructures' industries, as well as from corresponding departments of government. The Commissioners spent 15 months on the problem, and on 20 October 1997, released their report. The PCCIP concluded that our nation is so dependent on our infrastructures that we must view them through a national security lens. They are essential to the nation's security, economic health, and social well being.[7] Further, the PCCIP found the Americans' collective dependence on the information and communications infrastructure makes obvious the very real and growing cyber dimension associated with infrastructure assurance. The various infrastructure systems are becoming more interconnected via telecommunication networks and, with the advent of SCADA[8] systems, increasingly dependent on networked cyberspace for command and control. With these ever-increasing interdependencies come significantly heightened system vulnerabilities and the concomitant dangers to U.S. national security. In a statement to the Senate Committee on the Judiciary, Senator Patrick J. Leahy reiterated conclusions of the PCCIP Report:

---

[6] President, Executive Order 13010: Critical Infrastructure Protection, (15 July 1996): 1-2.
[7] U.S. President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures,* (Washington D.C.: GPO, 20 October 1997): vii.
[8] SCADA – Supervisory Control And Data Acquisition. SCADA systems employ remote sites to effect infrastructure system control; control commands and data pass to and from the remote site via telecommunications links. Without strong security measures, SCADA systems are particularly vulnerable to cyber attack.

> "[A] significant threat to the American way of life is posed by well-focused attacks on the computers and computer networks that support telecommunications, transportation, water supply, banking, electrical power and other critical infrastructure systems. A successful physical or cyber-attack that damaged any single one of these systems would wreak havoc on our national economy or even jeopardize our national defense."[9]

There are numerous adversaries in the world with the desire and a developing and inexpensive means to attack the U.S. critical infrastructures and our way of life.

Overall, the PCCIP report was widely criticized as not answering the original charter. The Attorney General commented strongly that the Commission left several foundational questions unanswered, yet made strident funding and organizational recommendations. It seemed that the core of the Commission's charter was wrapped and reissued in the form of its final recommendations. For example, a common recommendation to an observed problem was to assign some other agency or department to further study the problem. The PCCIP also called for development and adoption of industry-wide security standards. This was widely rejected by industry because of the legal implications—lawsuits may arise and insurance rates might climb for those companies who will not or cannot follow the industry standards.

Following the PCCIP Report, on 22 May 1998, President Clinton issued both PDD-62 (Combating Terrorism) and PDD-63 (Protecting America's Critical Infrastructures). PDD-62 was issued to create a more systematic approach to fighting the terrorist threat of the next century. It also established the Office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism.[10]

---

[9] Congress, Senate, Subcommittee on Technology, Terrorism, and Government Information, of the Committee on the Judiciary, *The Nation At Risk: Report of the President's Commission on Critical Infrastructure Protection,* 105th Cong., 1st sess., 5 November 1997, 17.
[10] U.S. President, *Combating Terrorism: Presidential Decision Directive 62*, (22 May 1998): 2.

In a parallel effort, the Secretary of Defense chartered the U.S. Commission on National Security/21st Century (USCNS/21) to analyze the nature of future threats to the United States. In its Phase I Report, the Commission declared that a terrorist attack on the American homeland and upon our critical infrastructures with the potential loss of a significant number of American lives was likely to occur within the next 25 years.[11]

On yet another front, the Department of Defense chartered the Critical Infrastructure Protection Working Group (CIPWG) to identify national issues while concurrently working departmental issues. The CIPWG's concern for DOD equities spawned another organization, the Critical Asset Assurance Program (CAAP). Meanwhile, in the private sector, the banking industry was starting to stand up their own information-sharing network (with limited participation), and Carnegie-Mellon University had developed a Computer Emergency Response Team concept that was very well organized.

The effect of all these efforts, which are not even the complete list, is the conduct of a rather large group of organizations and initiatives, without much coherency, with very little cross-community cooperation, and subsequently, with hamstrung effectiveness.

PDD-63 became the strongest directive to date to try to formulate a coordinated and cooperative system for providing CIP. PDD-63 identified critical infrastructure protection as a national security priority, instituted a national commitment to create a viable CIP capability within five years, established the Critical Infrastructure Assurance Office (to coordinate government CIP efforts), directed the development of a national CIP plan, and

---

[11] U.S. Commission on National Security in the 21st Century, *New World Coming: American Security in the 21st Century; Supporting Research and Analysis; Phase I Report on the Emerging Global Security Environment for the First Quarter of the 21st Century*, (http://www.nssg.gov, 15 September 1999): 139.

called for establishment of a public-private partnership to accomplish its goals.[12] It also directed the development of a National Critical Infrastructure Assurance Plan, to serve as a coherent plan of action for CIP. The first part of this two-part plan addresses the information infrastructure, and is due for publication in January 2000.

Controlling Authorities

Deciding where and how to proceed on this CIP problem requires consideration and integration of several controlling authorities: Constitutional constraints, domestic and international law, existing policies, precedent and conventions, and public support.

Per the U.S. Constitution, the federal government shall provide for the common defense, and as specified in Article IV, Section 4, shall protect each state against invasion.[13] Counterbalancing the Constitutional authority to protect American national security interests is the moral imperative to protect U.S. citizens from intrusive government interference. Detection of potential CIP attacks requires viable intelligence activity, which may violate certain rights to privacy and civil liberties. Amendment IV protects US citizens from illegal search, and as such protects each citizen's right to privacy:

> "The right to be left alone—the most comprehensive of rights, and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[14]

Further, this right to privacy extends beyond U.S. citizenry. Per Article 12 of the United Nations Universal Declaration of Human Rights, "No one shall be subjected to arbitrary

---

[12] Hunker, Jeffrey A., statement before the House National Security Committee, Military Procurement Subcommittee, Military Research & Development Subcommittee: On *Protecting America's Critical Infrastructures: Presidential Decision Directive 63*, (11 June 1998): 8-9.

[13] Collier, Christopher, and James L. Collier, *Decision In Philadelphia: The Constitutional Convention of 1787*, (New York, NY: Ballantine Books, 1986): 375, 385.

interference with his privacy."[15] The "arbitrary" qualification logically invokes the requirement for adjudged probable cause to justify surveillance.

With respect to existing policies, there is little in the way of substantive policy that addresses the growing threat to critical information infrastructures. The cyber technologies have grown too rapidly for policy to keep up.[16] While the PCCIP acknowledges the growing cyber vulnerabilities and calls for a government-industry partnership to address these emerging threats, there remains a dearth of policy to resolve the CIP issues. In a Senate Hearing on CIP, Subcommittee Chairman Senator Kyl states:

> "Many have pointed out the need for government-industry partnership, which I endorse. But it must be a carefully articulated partnership, which will enable industry to know what it is being asked to do and why. To call for more cooperation in a policy vacuum is meaningless and useless."[17]

In any case, the PCCIP Report has called for sharpened CIP focus from the executive as well as from the owners and operators of the critical infrastructures.

Additionally, the United States' encryption policy lacks some coherency. The U.S. intelligence community maintains the stance that encryption technology should be deliberately controlled and kept to a level that they can monitor for the sake of keeping tabs on the criminal element. However, the criminals have already shown a propensity to break the law, and the more complex encryption algorithms can already be relatively easily procured, albeit illegally. The U.S. encryption policy has an adverse impact exclusively on

---

[14] Justice Louis Brandeis in *Olmstead v. U.S.* (1928).
[15] Right to Privacy Forum; http://www.rightoprivacy.com/.
[16] This is a classic example of William F. Ogburn's theory of culture lag, which refers to the differential in the speed at which different elements of society react to significant changes and can create significant social problems. Culture lag presents significant implications for policy makers. The purpose of policy is to effect some change, to achieve some desired state within some specific community at an earlier time than might otherwise naturally occur. Policy makers must look beyond the near-term and consider the wider potential for change that any policy brings. [Bates, Benjamin, in *Telecommunication Policy and Cultural Lag*, from http://excellent.com.utk.edu/%7Ebates/hkej7.htm, (August 1992).]

the law-abiding segment, by precluding them from using the best tools available to secure their information systems.

Similar to the lack of policy on CIP, there is also little precedent to deal with protecting critical infrastructures, especially in the information realm. While there is some legal basis for enforcing physical protection of critical infrastructures, the rapid emergence of the cyber threat has left all branches and agencies of the federal government far behind. While the FBI has set up the National Infrastructure Protection Center (NIPC), this entity is tasked to detect and track computer intrusions/attacks. The priority for U.S. CIP should be to develop a defense in depth, to prevent, or at least significantly blunt the effects of a cyber attack on American critical infrastructures.

At the state and local levels, the vulnerabilities of our critical infrastructures seem widely recognized, but the threat is only minimally addressed. For example, states and municipalities nationwide have mobilized Y2K crisis watch centers to address potential problems with the critical infrastructures—whether brought on by Y2K anomalies or terrorist cyberattacks. Unfortunately, many of these centers will quickly disband after the New Year with little thought of quick reconstitution capability, even though the many potential threats to critical infrastructures remain.

Finally, public support is mixed. Most agree that the U.S. government should provide for the common defense, but blanch at the perception that in providing for cyber security, the government would trample citizens' rights to privacy. Further, many either don't recognize the extent of the threat, or believe that this is a problem that the private sector should solve unilaterally. In business circles, there is fear that if the government

---

[17] Congress, Senate, Subcommittee on Technology, Terrorism, and Government Information, of the Committee on the Judiciary, *The Nation At Risk: Report of the President's Commission on Critical*

serves as the clearinghouse for monitoring industry vulnerabilities, the Freedom of Information Act (FOIA) may permit release of industry-sensitive information. In other words, no company would want to share its vulnerabilities with any agency if there was the possibility that such information could leak out and damage that company's credibility. There is also the risk of losing competitive edge through the release of proprietary information.

The Decision-Makers and Other Participants

The Executive Branch has taken the lead for the government in protecting critical infrastructures. This is largely due to the organization of the Executive Branch, which contains the various departments and agencies that are directly influenced by policy on CIP. The President serves as the focal point for such policy, and is also responsible for coordinating agreements with foreign countries. The President has also stated the position, both in PDD-63 and in the National Plan for Critical Information Systems Protection, that the CIP solution exists absolutely in a cooperative arrangement between government and the private sector. Further, the government will rely on such cooperative solutions and not on government regulations or enforced industry standards.[18]

The Legislative Branch will also have a significant role in the CIP program. Inasmuch as the Executive Branch needs to cooperate with the private sector, the Executive and Legislative Branches need to work together for CIP. Legislation may be required to add caveats to the FOIA, in order to address propriety and competitive concerns, and encourage industry partners to share information on critical infrastructure

---

Infrastructure Protection, 105th Cong., 1st sess., 5 November 1997, 6.

[18] President, *Defending America's Cyberspace: National Plan for Information Systems Protection (Draft Version 1.0); An Invitation to a Dialogue*, (10 November 1999): iv-v.

attacks. Further, legislation is already in process concerning encryption policy, and obviously, some compromise will be required to effect rational encryption policy. Finally, Congress will be called upon by the President to continue to fund the CIP program and to increase funding for research and development of network defense technologies. President Clinton, in his National Plan for Information Systems Protection, has requested an annual budget allocation of $1.5B for administration of the plan, of which $750M is earmarked for research and development.[19] The Critical Infrastructure Assurance Office anticipates that Congress may balk at the high price tag for CIP. It will be incumbent upon the President to communicate effectively the scope of the threat, if he hopes to elicit any compromise and cooperation from Congress.

Cooperation between the executive, legislative, and judicial branches will be required to address the subject of tracking through cyber space and apprehending cyber-criminals. This issue must address rules of surveillance and problems of jurisdiction that arise as the cybercrook transits several jurisdictional zones while engaged in an attack within the cybersphere, and must be carefully handled to ensure protection of citizens' civil liberties. Note that the capture of a cyber criminal is secondary to the primary objective: assuring a solid defense of our information systems from even an initial attack.

Numerous entities in the private sector will play a very large role in the solution to this CIP problem. The cooperation of the private companies within each sector is essential to viable analyses of the threats to their specific infrastructures. Moreover, the cooperation of the private sector with the government—who will have the unique capability and legal authority to provide intelligence support to and analysis of the CIP problem. Compromise

[19] President, *Defending America's Cyberspace: National Plan for Information Systems Protection (Draft Version 1.0); An Invitation to a Dialogue*, (10 November 1999): iii, 119, 136.

on both sides is essential, in order for government to provide the essential CIP services while assuring protection of individual privacy and civil liberties, and for the private sector to share the information essential to good threat analysis.

Action Required

Technological and economic progress provides tremendous benefits to society, but also causes friction and conflict. As societies grow and interact, violence becomes increasingly a method of human reaction. The threat to American infrastructures and the American way of life is very real. The capacity for devastating violent action has devolved from the State entities to the individual—technology has made it so. Attacks to our networks and critical infrastructures are becoming more and more common, in the form of terrorism and information warfare. Limited forms of conflict no longer mean limited aims; this shift in the paradigm of conflict indicates that the issue can no longer be left to the State to maintain threat awareness, plan for, or defend against. It is an issue that has become the responsibility of all people.[20] Clearly, an effective CIP program will require cooperation and a certain level of compromise among all the players—all branches of government, the private sector, and the American people. The threat is real, and the threat demands it.

[20] 7Pillars Partners, *Infrastructural Warfare: Why Should You Be Aware?* From http://www.7pillars.com/know.html.

SELECTED BIBLIOGRAPHY

Bates, Benjamin. *Telecommunication Policy and Cultural Lag*. From http:/excellent.com.utk.edu/%7Ebates/hkej7.htm, August 1992.

Collier, Christopher, and James L. Collier. *Decision In Philadelphia: The Constitutional Convention of 1787*. New York, NY: Ballantine Books, 1986.

Hunker, Jeffrey A. Statement before the House National Security Committee, Military Procurement Subcommittee, Military Research & Development Subcommittee: *Protecting American's Critical Infrastructures: Presidential Decision Directive 63*. 11 June 1998.

Right to Privacy Forum. From http://www.rightoprivacy.com/.

U.S. Commission on National Security in the 21st Century. *New World Coming: American Security in the 21st Century; Supporting Research and Analysis; Phase I Report on the Emerging Global Security Environment for the First Quarter of the 21st Century*. From http://www.nssg.gov, 15 September 1999.

U.S. Congress. Senate. Subcommittee on Technology, Terrorism, and Government Information, of the Committee on the Judiciary. *Critical Infrastructure Protection: Toward A New Policy Directive*. Serial No. J-105-88. 105th Cong., 2nd sess., 17 March 1998 and 10 June 1998.

U.S. Congress. Senate. Subcommittee on Technology, Terrorism, and Government Information, of the Committee on the Judiciary. *The Nation at Risk: Report of the President's Commission on Critical Infrastructure Protection*. Serial No. J-105-68. 105th Cong., 1st sess., 5 November 1997.

U.S. Department of Defense Critical Infrastructure Protection Office, OASD(C3I). Briefing on the *Critical Infrastructure Protection Plan*. 16 November 1999.

U.S. President. *A National Security Strategy for a New Century*. Washington D.C.: GPO, May 1997.

U.S. President. *A National Security Strategy for a New Century*. Washington D.C.: GPO, October 1998.

U.S. President. *Defending America's Cyberspace: National Plan for Information Systems Protection (Draft Version 1.0); An Invitation to a Dialogue*. 10 November 1999.

U.S. President. *Critical Infrastructure Protection: Executive Order 13010*. 15 July 1996.

U.S. President. *U.S. Policy on Counterterrorism: Presidential Decision Directive 39*. 24 January 1997.

U.S. President. *Combating Terrorism: Presidential Decision Directive 62.* 22 May 1998.

U.S. President. *Protecting America's Critical Infrastructures: Presidential Decision Directive 63.* 22 May 1998.

U.S. President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures.* Washington D.C.: GPO, 20 October 1997.