

**STRATEGY
RESEARCH
PROJECT**

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

**IMPLEMENTING THE NATIONAL SECURITY STRATEGY OF
CRITICAL INFRASTRUCTURE PROTECTION**

BY

**LIEUTENANT COLONEL GREGORY M. WILLIAMITIS
United States Army**

**DISTRIBUTION STATEMENT A:
Approved for Public Release.
Distribution is Unlimited.**

USAWC CLASS OF 2000



U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5051

20000526 110

USAWC STRATEGY RESEARCH PROJECT

**IMPLEMENTING THE NATIONAL SECURITY STRATEGY OF CRITICAL
INFRASTRUCTURE PROTECTION**

by

LTC Gregory M. Williamitis
United States Army

Douglas C. Lovelace Jr.
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

ABSTRACT

AUTHOR: LTC Gregory M. Williamitis

TITLE: Implementing the National Security Strategy of Critical Infrastructure Protection
FORMAT: Strategy Research Project

DATE: 31 March 2000

PAGES: 22

CLASSIFICATION: Unclassified

Presidential Decision Directive (PDD) 63 provides detailed guidance for the protection of America's critical infrastructures of energy, banking, transportation, human services and telecommunications as viewed in the context of the Information Age. Does PDD 63 provide the necessary framework and resources to create a viable defense of these essential services or does it simply acknowledge there is a challenge that must be addressed? This report examines the National Security Strategy concerning PDD 63 and analyzes the challenges of implementing its complex strategy in a cooperative environment between the federal government and the private sector. The complexities of relating this directive to PDD 62 (Combating Terrorism) and PDD 56 (Interagency Cooperation) are explored in order to enhance the ways and means of implementing a cohesive strategy of infrastructure protection. The paper develops the emerging threats to this nation's infrastructure and identifies government, private sector and military implications. The paper further examines policy, doctrine and strategy for implementing critical infrastructure protection.

TABLE OF CONTENTS

ABSTRACT	III
IMPLEMENTING THE NATIONAL SECURITY STRATEGY OF CRITICAL INFRASTRUCTURE PROTECTION	1
NATIONAL SECURITY STRATEGY	2
PDD 63 CRITICAL INFRASTRUCTURE PROTECTION POLICY REVIEW	3
PDD 62 COMBATING TERRORISM	6
PDD/NSC 56 MANAGING COMPLEX CONTINGENCY OPERATIONS	6
ENHANCING THE EFFORT	7
THE EMERGING THREAT	8
POLICY, STRATEGY AND DOCTRINE	10
ENCRYPTION	11
CONCLUSION	12
ENDNOTES	13
BIBLIOGRAPHY	15

IMPLEMENTING THE NATIONAL SECURITY STRATEGY OF CRITICAL INFRASTRUCTURE PROTECTION

Because so many key components of our society are operated by the private sector, we must create a genuine public/private partnership to protect America in the 21st century. Together, we can find and reduce the vulnerabilities to attack in all critical sectors. We will launch a comprehensive plan to detect, deter, and defend against attacks on our critical infrastructures, our power systems, water supplies, police, fire, and medical services, air traffic control, financial services, telephone systems, and computer networks.

President William J. Clinton

In light of these imperatives President Clinton ordered the strengthening of the nation's defenses against emerging unconventional threats to the United States: terrorist acts, use of weapons of mass destruction, assaults on our critical infrastructures and cyber-attacks. Presidential Decision Directives (PDD) 62 and 63 were issued to establish priorities and responsibilities.

PDD 62 Combating Terrorism, highlights the growing threat of unconventional attacks against the United States and details a new and more systematic approach to fighting terrorism by bringing a program management approach to U.S. counter-terrorism efforts.

PDD-63 Critical Infrastructure Protection, calls for a national effort to assure the security of the increasingly vulnerable and interconnected infrastructures of the United States and stresses the critical importance of cooperation between the government and the private sector by linking designated agencies with private sector representatives.

A third related directive, PDD 56 Managing Complex Contingency Operations, directs the establishment of appropriate interagency working groups to assist in policy development, planning, and execution of complex contingency operations. It also calls for all U.S. Government agencies to institutionalize lessons learned from previous experiences to continually improve the planning and management of complex contingency operations.

The juxtaposition and complexity of these three directives requires tremendous coordination of priorities and resources. Several areas requiring critical analysis become readily apparent as the concurrent strategies of these directives are effected. Does PDD 63 provide the necessary framework and resources to create a viable defense of the essential services composing the nation's infrastructure or does it simply acknowledge there is a challenge that must be addressed? Are the three directives capable of bringing about complementary action in a coherent manner and is the command and control of such an overwhelming undertaking possible? Can the public and private sector cooperate to achieve strategic imperatives or will legislation be required? Can government remain relevant in the face of rapid technological advances or will the private sector outpace government efforts? Does the required intelligence structure exist to identify and deter the threat or will America have to rely on addressing the vulnerabilities through risk management in lieu of risk avoidance?

The scope of this project is specifically to examine the United States National Security Strategy concerning PDD 63 and analyze the challenges of implementing its complex imperatives in a cooperative environment between the federal government and the private sector. The complexities of relating this directive to PDD 62 (Combating Terrorism) and PDD 56 (Interagency Cooperation) are explored in order to understand the ways and means of implementing a coordinated strategy of infrastructure protection. The paper addresses the emerging threats to this nation's infrastructure and identifies government, private sector and military implications. The paper further examines policy, doctrine and strategy for implementation of counter proliferation, deterrence, consequence management, and intelligence collection.

NATIONAL SECURITY STRATEGY

As stated in the October 1999 National Security Strategy (NSS) our national security and our economic prosperity rest on a foundation of critical infrastructures, including telecommunications, energy banking and finance, transportation, water systems and emergency services. These infrastructures are vulnerable to computer generated and physical attacks. More than any other nation America is dependent on cyberspace. We know that other governments and terrorist groups are creating sophisticated, well-organized capabilities to launch cyber attacks against critical American information networks and the infrastructures that depend on them. To enhance our ability to protect these critical infrastructures President Clinton issued PDD 63 in May 1998 and directed that a plan for defending critical infrastructures be in effect by May 2001 and fully operational by December 2003.¹

The key infrastructures identified by the policy are defined as but not limited to transportation, oil and gas production and storage, water supply, emergency services, government services, electrical power, and telecommunications (information and communications). A review of these major systems reveals that there is common dependence on them among all levels of government and the private sector on a national and even global scale. The private sector interface presents one of the biggest challenges to the implementation of PDD 63, since the majority of the infrastructure and evolving technology resides in the private sector. These systems are widely dispersed, difficult to defend from physical attack and vulnerable to cyber intrusion from anyone with means, motive and intent. Threats to these systems include nation states, terrorists (foreign and domestic), drug cartels, individuals (malicious or mischievous) and even multinational corporations. Complicating the challenge is the international aspect or globalization of the private sector. The private sector's competitive drive and profit motive will not necessarily coincide with national security interests.

Because of these threats PDD 63 certainly has overwhelming relevancy to national security and its implementation is long overdue. Global trends outlined in Joint Doctrine indicate an increase in mass communication and economic interdependence, proliferation of information technology and equal access to that information by all players no matter how small. Military-specific trends describe advanced technology weapons. Microbiology and biotechnology breakthroughs and information dominance are

rapidly becoming realities of joint operations.² Without viable systems capable of detecting and assessing the threat we are vulnerable to a cyber "Pearl Harbor" at any time.

The 1999 NSS clearly addresses the national values concerning infrastructure protection by establishing three core objectives; enhancing American security, bolstering our economy, and promoting democracy and human rights abroad. Additionally the NSS articulates the vital interests of providing physical security of our territory and that of our allies, ensuring the safety of our citizens, the economic well-being of our society and protecting our critical infrastructures from paralyzing attack.³

PDD 63 CRITICAL INFRASTRUCTURE PROTECTION POLICY REVIEW

PDD 63 directs that it shall be the policy of the United States to assure the availability and continuity of the critical infrastructures on which our economic security, defense, and standard of living depend. These critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. The infrastructures will be defended by whatever means necessary, including the full range of business, legal, law enforcement, military, and social tools available.⁴ As a result of advances in information technology and the necessity of improved efficiency, these infrastructures have become increasingly automated and inter-linked. These advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities requires flexible, responsive, real time approaches that span both the public and private sectors, and protect both domestic and international security.

Adherence to the following three imperatives established by PDD 63 is essential to achieving the strategic end of reducing these vulnerabilities and protecting the infrastructure from intentional attack. In this context the strategic end is defined as the objectives the nation wants to accomplish using the means available (resources) and the ways (possible modes) of employing means to achieve these ends.

- Ensure the Federal Government's ability to perform essential national security missions and provide for the general public health and safety;
- Enable state and local governments to maintain order and to deliver minimum essential public services;
- Ensure the private sector's ability to continue the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

The President's Commission on Critical Infrastructure Protection recommends the following actions as the ways to begin building the required protection.⁵

- Promote a partnership between government and infrastructure owners/operators beginning with increased sharing of information relating to infrastructure threats, vulnerabilities and interdependencies;
- Ensure infrastructure owner/operators and state and local governments are sufficiently informed and supported to accomplish their roles;
- Establish national structures that will facilitate effective partnership between federal, state and local governments, and infrastructure owners/operators;
- Elevate national awareness of infrastructure threat, vulnerability, and interdependency assurance issues through education and other appropriate programs;
- Demonstrate government leadership with information security programs and related programs;
- Sponsor legislation to increase effectiveness of federal assurance and protection efforts;
- Promote increased research and development for infrastructure protection and increase investment for needed improvements.

The federal government has applied the following method to achieve the ways of this strategy. For each of the major sectors of the economy that are vulnerable to infrastructure attack, the Federal Government will appoint from a designated Lead Agency a senior officer of that agency as the Sector Liaison Official to work with the private sector. Sector Liaison Officials, after discussions and coordination with private sector entities of their infrastructure sector will identify a private sector counterpart (Sector Coordinator) to represent their sector. Together these two individuals and the departments and corporations they represent shall contribute to a National Infrastructure Assurance Plan. During the preparation of these plans, the National Coordinator in conjunction with the Lead Agency Sector Liaison Officials and a representative from the National Economic Council, shall ensure their overall coordination and the integration of the various sectorized plans, with a focus on interdependencies.⁶ As of this writing the first sector to achieve this architecture is the financial services sector under the Department of Treasury.

To execute these directives the Federal Bureau of Investigation expanded the National Infrastructure Protection Center (NIPC).⁷ This organization now serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC includes representatives from the FBI, and the United States Secret Service, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, the intelligence community and lead agencies. It is linked electronically to the rest of the Federal Government, including other warning and operations centers, as well as private sector sharing and analysis centers. The mission of the NIPC is both a national security and law enforcement effort to detect, deter, assess, warn of, respond to, and investigate computer intrusions and unlawful acts both physical and "cyber," that threaten or target our critical infrastructures.⁸

Several complimentary agencies have been tasked to assist the NIPC with the execution of its responsibilities. The Critical Infrastructure Assurance Office (CIAO) is tasked with managing the interagency expert review process; forming a public-private partnerships; promoting private-sector led information sharing channels; developing a federal intrusion detection system; and drafting of an inter-agency national plan which incorporates the many aspects of the critical infrastructure protection agenda.⁹ The Information Sharing and Analysis Center (ISAC) consults with owner/operators of infrastructures to encourage information sharing and the development of an analysis center. The Information Infrastructure Task Force (IITF) is working together with the private sector to develop comprehensive technology, telecommunications, and information policies and promote applications that best meet the needs of the agencies and the country. By helping build consensus on difficult policy issues, the IITF will enable agencies to make and implement policy more quickly and effectively.

The implementation of these actions are an evolving process that will require considerably more time to measure effectiveness; however, the Center for International Security and Arms Control (CISAC) recommends the following nine areas of consideration to enhance implementation of PDD63.¹⁰

- A discussion of the time available for coordinating public and private initiatives.
- The need for priorities, in view of the very large number of recommendations.
- An expanded discussion of the nature of the proposed public-private partnership, taking greater account of the incentives driving suggested private sector participants.
- Broadening the base of the public sector partners beyond that of the executive branch organizations to include state and local regulators, international organizations, and other sovereign states.
- The degree of which infrastructure systems are robust and the degree to which they are susceptible to cascading and catastrophic failure.
- The working of the market in providing enhanced security through private investments of infrastructure operators, product vendors, and system integrators.
- The relationship between public and private R&D investments.
- The relationship between infrastructure assurance and the administration's encryption policy.
- What costs will be incurred in protecting the nation's infrastructure and who should pay them.

The CISAC paper goes on to recommend eight additional areas where the Presidents Commission's proposal should be modified. The most important of which is to confine the initial actions to the telecommunications and the electrical power infrastructures until assessment of threats and vulnerabilities can be validated. Considering the magnitude of effort required to implement these directives and the high probability of redundant initiatives between government agencies it is imperative to consider the complimentary portions of PDD 62 and PDD 56.

PDD 62 COMBATING TERRORISM

PDD 62 creates a systematic approach to fighting the terrorist threat of the next century. It reinforces the missions of the many U.S. agencies charged with roles in defeating terrorism and codifies and clarifies their activities in the wide range of U.S. counter-terrorism programs. The directive addresses every activity from apprehension and prosecution of terrorists to increasing transportation security, enhancing response capabilities and protecting the computer-based systems that lie at the heart of America's economy. The Directive is intended to achieve the goal of ensuring that America meets the threat of terrorism in the 21st century with the same rigor that military threats have been addressed in this century. To achieve this new level of integration in the fight against terror, PDD 62 also relies on the Office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. The National Coordinator oversees a broad variety of relevant policies and programs including such areas as counter-terrorism, protection of critical infrastructure, preparedness and consequence management for weapons of mass destruction. The National Coordinator works within the National Security Council, reports to the President through the Assistant to the President for National Security Affairs and produces an annual Security Preparedness Report. The National Coordinator also provides advice regarding budgets for counter-terror programs and leads in the development of guidelines that might be needed for crisis management.¹¹ All of the responsibilities directed by both PDD 62 and PDD 63 clearly require extensive interagency cooperation between government and non-government organizations. PDD 56 Managing Complex Contingency Operations addresses the method that orchestrates these activities.

PDD/NSC 56 MANAGING COMPLEX CONTINGENCY OPERATIONS

The intent of PDD/NSC 56 is to establish management practices to achieve unity of effort among U.S. Government agencies and international organizations engaged in "complex contingency operations" loosely defined as peace operations.¹² Unless otherwise directed, the PDD does not apply to domestic disaster relief or to relatively routine or small-scale operations, nor to military operations conducted in defense of U.S. citizens, territory, or property, including counter-terrorism and hostage-rescue operations and international armed conflict. The PDD does direct preparedness to manage the humanitarian, economic and political consequences of a technological crisis where chemical, biological, and/or radiological hazards may be present. The occurrence of any one of these dimensions could significantly increase the sensitivity and complexity of any U.S. response to a technological crisis. In many complex emergencies the appropriate U.S. government response will require the involvement of only non-military assets. The need for complex contingency operations is likely to recur in future years, demanding varying degrees of U.S. involvement. PDD 56 calls for all U.S. Government agencies to institutionalize what has been learned from recent experiences and to continue the process of improving the planning and

management of complex contingency operations. The PDD is designed to ensure that the lessons learned, including proven planning processes and implementation mechanisms, will be incorporated into the interagency process on a regular basis.

ENHANCING THE EFFORT

Coordinating the efforts of PDD 63 and PDD 62 strengthens the nation's defenses against emerging unconventional threats to the United States: terrorist acts, use of weapons of mass destruction, assaults on our critical infrastructures and cyber-attacks. PDD 62 highlights the growing threat of unconventional attacks against the United States and details a systematic program management approach to fighting terrorism. The directive also establishes the office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism which oversees a broad variety of relevant policies and programs including areas such as counter-terrorism, protection of critical infrastructure, preparedness and consequence management for weapons of mass destruction.

The Critical Infrastructure Protection directive PDD 63 calls for a national effort to assure the security of the increasingly vulnerable and interconnected infrastructures of the United States. The directive requires immediate federal government action including risk assessment and planning to reduce exposure to attack. It stresses the critical importance of cooperation between the government and the private sector by linking designated agencies with private sector representatives.

Applying the PDD 56 framework to management of domestic disaster relief and military operations conducted in defense of U.S. citizens, territory, or property, including counter-terrorism would enhance this combined effort. Since PDD 56 does direct the management of humanitarian, economic and political consequences of a technological crisis where chemical, biological, and/or radiological hazards may be present. The inclusion of support to critical infrastructure protection and consequence management through contingency planning would be a natural extension of the interagency process.

There are two additional shortcomings contained in PDD 63 that require critical analysis and cannot be corrected with simple coordination between policy's and agencies. Both of these issues could be the thesis for future projects of this nature. First the complete lack of horizontal integration between the sectors will lead to a stovepipe relationship during the planning and execution of any contingency. And second there is no compelling reason for the private sector to either become completely involved in the process or even trust that the government will be capable of providing early warning of attacks or protection of corporate secrets. Since private sector interests have not been incorporated on a global scale and legislation has not mandated participation or established disincentives, the door is open for selective noncompliance in areas that might create the backdoor required for an adversary to execute an attack.

This noncompliance is demonstrated in recent denial of service attacks against several Internet commerce sites. With Treasury Department approval financial industry officials did not pass detailed

warnings to the FBI or other law enforcement agencies as alerts escalated February 8, 2000 from the first assault against the Yahoo! Web site on to eBay, Amazon.com, Buy.Com, CNN and others.¹³

The urgent alerts, by e-mail and pager, began fully four days before Yahoo! fell under electronic assault Feb. 8. They cautioned that dangerous attack software had been discovered and implanted on powerful computers nationwide. The messages ultimately identified specific Internet addresses of attacking machines. Participating banks were not allowed to share the warnings with government investigators under rules of an unusual \$1.5 million private security network created in recent months for the financial industry.

The Treasury Department said mandated disclosures might hamper banks and others from being forthcoming about attacks by rogue employees, software bugs, viruses or hackers. The industry said such guarantees helped ensure it was protected. "Everybody felt comfortable sharing information," said William Marlow, executive vice president for Global Integrity Corp., which runs the network. "The government wasn't involved, everything was anonymous. The private sector can help each other without additional regulation."

The banking industry's warning network, run from the secretive Financial Services Information Sharing and Analysis Center, is among the first of its kind. The center grew out of the president's orders for better protection from cyberattack for America's most important industries. Its member banks, and even its location, are closely guarded secrets. To encourage open participation by banks and other financial firms, the Treasury Department decided that information disclosed would not be turned over to federal regulators or law enforcement agencies. It worked well last week for banks, which enjoyed early warnings about pending attacks, but it also guaranteed the same warnings weren't widely distributed.

A unilateral decision like the one listed above in each service industry is certainly a boundary that any adversary could exploit. As the technology becomes more sophisticated new threats and methods of attack become even more diverse.

THE EMERGING THREAT

As pointed out in several U.S. Government policy and strategy documents, the United States possesses both the world's strongest military and its largest national economy. These two aspects of our power are mutually reinforcing and interdependent. They are also increasingly reliant upon the critical infrastructures and upon the cyber-based information systems described in PDD 63. Because of these strengths, future enemies, whether nations, groups or individuals, will certainly seek to attack the United States in non-traditional ways including attacks within the United States. The emerging threats can be classified into the following categories:

- Nation States - economic and military espionage, data mining, and information warfare.
- Hacker's - individuals satisfying a variety of personal agenda's from white-collar crime to service disruption and information corruption.
- Cult's - ideological organizations with no borders, no allegiance to nationality or concern for mainstream society.
- Paramilitary Organization's - an organized association of individuals with shared beliefs, training, political doctrine and access to arsenal's with plans for domestic terrorism against the federal government.
- Terrorists and Extremist Group's - international (state sponsored) systemic warfare to produce terror for political coercion.

- Organized Crime and Transnational Criminal's - a network of coordinated transnational sectors operated by regional crime societies.

Since our economy is increasingly reliant upon interdependent and cyber-supported infrastructures, non-traditional attacks on our infrastructure and information systems could be capable of significantly harm both our military power and our economy. Since the targets of attacks on our critical infrastructure would likely include facilities in the economy as well as those in the government, the elimination of potential vulnerability requires cooperation between the public and the private sector. Potential hostile actions against these vulnerabilities span the spectrum from inserting false data or harmful programs into information systems through stealing valuable data or programs, taking over control of a system's operation, manipulating the system's operation or performance, denying access, or physical destruction. Examples of potential future incidents are limited only by the attackers imagination and might include:

- Attacks on physical and functional infrastructures such as air traffic control systems, major regional power grids or financial institutions and international markets;
- Attacks on military or national security systems;
- Attacks on societal organizations and activities such as medical facilities or emergency services like regional 911 services or police and fire organizations.

The mechanisms for these attacks can range the spectrum from sophisticated embedded software programs to pipe bombs destroying physical locations or a combination of synchronized attacks. Attacks on infrastructure can be categorized as follows:

- Operations based attacks - exploitation of deficient security environments;
- User authentication based attacks - bypass or penetration of login or passwords;
- Software based attacks - exploiting software design flaws or using trap/back door access;
- Network based attacks - alteration of routing tables, password sniffing and the spoofing of addresses;
- Hardware based attacks - exploiting programmatic or logical flaws in hardware design;
- Physical attack - physical destruction of key nodes.

To succeed in defending against these threats the public-private sector partnership must be genuine, mutual and cooperative. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure the U.S. government must seek to avoid outcomes that increase government regulation or expand government mandates to the private sector. Increased mandates could be seen as surrendering to the threats potential without any actual attack. Legal Considerations must include the potential for defensive as well as offensive operations. And a detailed analysis of actions that are expressly prohibited by international law or convention must be conducted to allow for an international solution.

POLICY, STRATEGY AND DOCTRINE

Is the U.S. national security structure capable of the intellectual and doctrinal suppleness required to pursue an implicit set of concerns and issues using highly calculated, specific means, to achieve explicit, but coherent objectives?¹⁴

The answer to this question is an evolving process that will require years to answer. However, it is clear that to achieve the required infrastructure protection outlined in PDD 63 policymakers must take the next step beyond "we will do anything necessary to protect these systems" and publicly articulate the ways and means that will be employed to reach the ends. The infrastructures and their owners have been defined in a macro sense and the appropriate agencies have been resourced and tasked to begin work on identifying vulnerabilities and legislation required, but key aspects of the national policy are missing. These aspects include the intent and willingness of the nation to execute a national security strategy of deterrence, defensive and offensive operations. A clear articulation of the employment of information operations against a threat should be outlined in the same manner as we have addressed the use of weapons of mass destruction. There are clearly areas of overlapping responsibility and in domestic and international law enforcement as well as military security responsibilities. Addressing these conflicts now is the first step in precluding or rapidly resolving future incidents.

Policy concerning the use of "weapons of mass disruption" is required in order to provide a strong deterrence and allow for employment in a unilateral or international operation. A posture statement would provide a springboard for developing national military strategy, civil defense and even international negotiations to enact treaties much like the nonproliferation treaties for nuclear weapons. Clearly a statement of what actions the nation will consider constitutes a sufficient justification to retaliate against state sponsored international infrastructure attacks, and what agency will respond, much as we do with terrorism and the protection of U.S. citizens would demonstrate a determined resolve. Without this national level of effort the national security and military experts will remain far more comfortable addressing the technology and resource means than considering the higher level policy and strategic objectives.¹⁵

Therefore, a holistic approach to strategy development and implementation which addresses culture, politics, economics and security concerns and reflect a "national will" which allows for offensive and defensive measures and information dominance is a required milestone in the pursuit of the ends. The requirement for a holistic approach is further reinforced when the range of players includes the government, Department of Defense and the proliferation of international organizations, non-government organizations, and special interest organizations.¹⁶ With the expanding involvement of these non-

government organizations as actors on the world scene, the focus of infrastructure protection shifts rapidly from the tactical battlefield level to the strategic plane. This complicates an already difficult problem of protecting total information infrastructures and reinforces the urgent need for policy and doctrine on the use of weapons of mass disruption. Organizations such as Business Executives for National Security (BENS) offer a partial solution for these challenges. The goal of the BENS organization is to bring business leaders and government representatives together to devise technically and politically feasible solutions. The anticipated end result is to develop a package of vetted, actionable proposals for how the private and public sectors can work together to ensure national security against emerging threats in WMD and cyber terrorism.¹⁷

ENCRYPTION

Perhaps one of the thorniest questions the government must address is the question of encryption. This is a critical issue and should be resolved in policy and legislation in order to incorporate the position into international agreements and treaties. Currently case law describes export controls on encryption source code as an impermissible "prior restraint" on speech protected by the First Amendment.¹⁸ This limitation severely restricts government ability to limit the export of dual use technology and retain the codes in interest of national security.

The importance of the issue is highlighted in the recent actions taken by China. Beginning January 31, 1999, the Chinese government will require all foreign firms to register the type of software the firm uses for data transfer and encryption.¹⁹ According to the directive companies must name the employees using the encryption software, the location of the computers they use and their email address and telephone numbers. All of this is required to control the Internet in China to ban dissidents from using the infrastructure to spread information. The consequences of this requirement are readily apparent. Certainly the Chinese government will benefit from collecting all of this information.

On the other extreme of the spectrum is the challenge the National Security Agency (NSA) faces. The agency has become a victim of its own success in helping create digitally encrypted transmissions. The advances of encryption technology and the inaccessibility of fiber optic lines have made it impossible for the NSA to reliably eavesdrop the way it has been accustomed to in the past.²⁰ Nations throughout Europe, Asia and the third world are posturing to capitalize on secure methods of communication and data transfer. This dichotomy clearly depicts the freedoms a free society enjoys verses a closed system like China.

U.S. Government regulation in this area would be difficult, cumbersome, and viewed as intrusive. The attempt to dictate registration of encryption codes for national security might arguably provide the government with the ability to assist in the protection of critical infrastructure, however, conspiracy enthusiasts would present these actions as "Big Brother's" finest hour. The bureaucratic overhead required to monitor and securely control these codes would be massive, and the security of these codes

would be called into question when the source code is registered. These requirements would have the unwanted result of shifting responsibility from the owner/operators of the infrastructure to the government.

Because of these challenges the government should support the operator's efforts to protect their systems, act as a clearing house of information sharing for attacks on the system and provide policy to that end. Finally government policy should allow for negotiation of international agreements that prohibit foreign governments from controlling encryption data information.

CONCLUSION

The analysis presented here only begins to scratch the surface of the complicated solutions required to make infrastructure protection a reality. The concept of a coordinated effort to protect the nations critical infrastructures from both cyber and physical attack is long overdue. To accomplish this protection PDD 63 in concert with PDD 62 provide a framework to begin organizing the initial defense. As presented in this paper there are major areas still requiring extensive coordination and it is time to "get out of the box" and aggressively pursue this end.

The government has defined the problem and presented a proposed solution with PDD 63. This proposed solution has addressed certain areas in detail and left execution of the remaining details to the good intentions and goodwill of the private sector. Additionally all of the analysis of PDD 63 has been done by bureaucratic think tanks that apparently have only reviewed the work done by the Presidential Committee on Infrastructure Protection. There has not been a bottom up review or tear down analysis done to determine if all of those involved share common vital interests, possess the means to identify vulnerabilities and achieve risk avoidance or can participate in the ways of executing risk management.

The private sector will participate only in those parts of the program development that address their vital interests and provide value added to their operations. They may not be able to achieve the same level of protection the government desires or chose other methods of risk management to facilitate operations and avoid regulation. What is not addressed is the fact that the private sector has interests beyond national security and in most cases are global organizations in direct competition with the other corporations this policy relies on for implementation. Until the government bureaucracy acknowledges this situation and addresses these interests with legislation and incentives the government will be irrelevant to the development of a cohesive plan for protection.

WORD COUNT = 5303

ENDNOTES

¹ William J Clinton, A National Security Strategy for a New Century (Washington, D.C.: The White House, December 1999), 17.

² Joint Chiefs of Staff, Concept for Future Joint Operations: Expanding Joint Vision 2010. (Washington, D.C., Department of Defense, May 1997), 8-9.

³ Clinton, 1.

⁴ Robert T. Marsh, Critical Foundations Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection, October 1997, 24. (Washington, D.C.)

⁵ Marsh, 93-99.

⁶ White Paper, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (Washington, D.C., May 22, 1998) 2-3.

⁷ Ibid., 9-10.

⁸ "NIPC Mission," linked from National Infrastructure Protection Center at "Mission," available from <<http://www.fbi.gov/mpc/mission>>; Internet: accessed 27 February 2000.

⁹ "About the Critical Infrastructure Assurance Office," linked from Critical Infrastructure Assurance Office at "CIAO Home" available from <<http://www.ciao.gov>>; Internet accessed 8 January 2000.

¹⁰ CISAC Working Paper, Review and Analysis of the Report of the President's Commission on Critical Infrastructure Protection, Center for International Security and Arms Control, Stanford University (Stanford, CA, January 1998) viii.

¹¹ The White House, Presidential Decision Directive 62, Fact Sheet linked from Federation of American Scientists (FAS) at "Presidential Decision Directives", available from <http://www.fas.org/irp/offdocs/direct.htm>; Internet accessed 8 January 2000.

¹² White Paper, The Clinton Administration's Policy on Managing Complex Contingency Operations: PDD/NSC 56 (Washington D.C., May 1997).

¹³ Ted Bridis, "Banks Warned of Hacker Attacks." The Washington Post, 14 February 28, 2000.

¹⁴ John Arquilla and David Ronfeldt, eds, In Athena's Camp. (Washington, D.C.: RAND, 1997), 228

¹⁵ Ibid., 223.

¹⁶ J.D. Schwartzstein, ed, The Information Revolution and National Security (Washington, D.C.: CSIS, 1996), 121.

¹⁷ "What Is BENS," linked from Business Executives for National Security, at <<http://www.bens.org>>; Internet accessed 6 March 2000.

¹⁸ Thomas Crocker, "Ninth Circuit Panel Rules on Encryption Export Controls in *Berstein v. U.S. DOJ et al.*" American Bar Association National Security Law Report. September 1999, Vol. 21, No. 5, p.7.

¹⁹ Matt Forney, "China to Issue New Rule on Software for Foreign Firms", The Wall Street Journal, 25 January 1999, sec. A, p. A10 and A13.

²⁰ Seymore Hersh, "Tech Advances Put American Intelligence At Serious risk; National Security Agency Playing Catch-up", The New Yorker, 6 December 1999.

BIBLIOGRAPHY

"About the Critical Infrastructure Assurance Office," linked from Critical Infrastructure Assurance Office at "CIAO Home" available from <http://www.ciao.gov>; Internet accessed 8 January 2000.

"NIPC Mission," linked from National Infrastructure Protection Center at "Mission," available from <http://www.fbi.gov/mpc/mission>; Internet: accessed 27 February 2000.

"What Is BENS," linked from Business Executives for National Security, available from <http://www.bens.org>; Internet accessed 6 March 2000.

Arquilla, John, and David Ronfeldt, eds. In Athena's Camp. Washington, D.C.: RAND, 1997.

Bridis, Ted. "Banks Warned of Hacker Attacks." The Washington Post, 14 February 28, 2000.

Campen, Alan D., Douglas H. Dearth, and R. Thomas Goodden, eds. Cyberwar: Security, Strategy, and Conflict in the Information Age. Fairfax, VA: AFCEA International Press, 1996.

Clinton, William J. A National Security Strategy for a New Century. Washington, D.C.: The White House, October 1998.

Concept for Future Joint Operations: Expanding Joint Vision 2010. Washington D.C.: Pentagon, May 1997.

Crocker, Thomas. "Ninth Circuit Panel Rules on Encryption Export Controls in *Berstein v. U.S. DOJ et al.*" American Bar Association National Security Law Report. September 1999, Vol. 21, No. 5.

Dunnigan James F. Digital Soldiers. New York, NY: St. Martin's Press, 1996.

Forney, Matt. "China to Issue New Rule on Software for Foreign Firms", The Wall Street Journal, 25 January 1999, sec. A, p. A10 and A13.

Hersh Seymore. "Tech Advances Put American Intelligence At Serious risk; National Security Agency Playing Catch-up", The New Yorker, 6 December 1999.

Joint Chiefs of Staff, Concept for Future Joint Operations: Expanding Joint Vision 2010. Washington, D.C.: Department of Defense, May 1997.

Kiplinger, Knight. World Boom Ahead. Washington D.C.: The Kiplinger Washington Editors, Inc., 1998.

Lukasik, Stephen J. Review and Analysis of the Report of the President's Commission on Critical Infrastructure Protection. Stanford, CA: Center for International Security and Arms Control, January 1998.

Marsh, Robert T. Critical Foundations Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection. Washington, D.C., October 1997.

Presidential Decision Directive 62. Fact Sheet linked from Federation of American Scientists (FAS) at "Presidential Decision Directives". Available from <http://www.fas.org/irp/offdocs/direct.htm>, Internet. Accessed 8 January 2000.

Schwartzstein, J.D., ed. The Information Revolution and National Military Security. Washington, D.C.: The Center for Strategic and International Studies, 1996.

Shalikashvili, John M. National Military Strategy of the United States of America. Washington, D.C.: Pentagon, 1997.

The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. Washington, D.C., May 22, 1998.

The Clinton Administration's Policy on Managing Complex Contingency Operations: PDD/NSC 56. Washington D.C., May 1997.

The White House, Presidential Decision Directive 62, Fact Sheet linked from Federation of American Scientists (FAS) at "Presidential Decision Directives", available from <http://www.fas.org/irp/offdocs/direct.htm>; Internet accessed 8 January 2000.

U.S. Department of the Army. Information Operations. FM 100-6. Washington D.C.: U.S. Department of the Army, August 1996.

Waltz, Edward. Information Warfare: Principles and Operations. Norwood ,MA: ARTECH House, Inc., 1998.