By the rude bridge that arched the flood,
Their flag to April's breeze unfurled,
Here once the embattled farmers stood,
And fired the shot heard round the world.¹

Since its 1975 invasion of the ex-Portuguese colony of East Timor,² the Indonesian government has been involved in a low-intensity conflict with the East Timorese Liberation Front, Fretilin. In a struggle characterized by occasional ambushes of government patrols and reprisals, the likelihood of escalation beyond this little-known, little-cared about backwater seemed a remote possibility.³ Beginning in early 1997, however, Indonesians operating Internet websites noticed seemingly arbitrary intrusions into file servers followed by the appearance of statements in support of East Timorese independence.⁴ Primary targets appeared to be the Indonesian Armed Forces (“ABRI”), government ministries, the National Institute of Sciences and state-run universities. While no permanent damage resulted from these attacks, the ABRI launched what were described as “counter operations in the war of propaganda on the Internet”⁵ and attacked the intruders Internet homepages. These “counter operations” were not directed against Indonesian citizens under the jurisdiction of the Indonesian government but against a group of hackers in Portugal.⁶ Intrusions were subsequently reported at the ABRI and Department of Foreign Affairs websites, the government computer system, the Indonesian Institute of Studies, and the Surabaya Institute of Technology.⁷

Beginning August 1, 1998, and continuing for the next 48 hours, the implications of acting against the Portuguese hackers became clear to the Indonesian authorities. The Portuguese hacker group “KaotiK Team”⁸ eventually defaced forty-five websites belonging to the government, Indonesian-based international organizations, private industry and Indonesian Internet service providers.⁹ KaotiK Team, a group dedicated to fighting for East Timorese liberation, pledged to continue operations until Indonesia’s occupation of East Timor ends.¹⁰ A new dimension of conflict had arrived in Indonesia and literally, the shot was heard around the world.

I. INTRODUCTION

The development of the Internet as a form of mass media has resulted in a debate among the federal government’s law enforcement, intelligence and defense communities concerning the extent of vulnerability of the National Informa-

¹ See RALPH WALDO EMERSON, CONCORD HYMN (sung at the completion of the Concord, Massachusetts monument, July 4, 1837).
³ See id. at 448.
⁶ See id.
⁷ See id.
⁸ See Kaotik Team (visited Nov. 4, 1998) <http://www.complex-x.net/kaotik/intro.html> (describing the goals of KaotiK Team and its attack on forty-five Indonesian web sites).
¹⁰ See Kaotik Protest Conditions In East Timor, ANTONLINE (August 2, 1998) <http://www.antionline.com/SpecialReports/KaotiK/>; see also KaotiK Team (visited Nov. 4, 1998) <http://www.complex-x.net/kaotik/intro.html> (stating Kaotik Team’s goals and self-proclaimed capabilities).
tion Infrastructure ("NII") to an incident such as the August 1998 attack on Indonesian websites. In response to these concerns, the Acquisition and Technology Policy Center of the RAND Corporation's National Defense Research Institute, in conjunction with the National Defense University, conducted a study for the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence in early 1995. The study and its results, constituted one of the first gatherings of defense, intelligence, law enforcement, academia and industry personnel to identify emerging topics specifically related to the vulnerability of the NII.

The object of the study was to assess the decision making process during a major hypothetical "information warfare" attack launched against the United States during a crisis in the Persian Gulf region. Based upon the RAND Corporation's projected trends in the world's geopolitical balance of power, the exercise's scenario was based upon a fictitious split between members of the Organization of Petroleum Exporting Countries ("OPEC") over levels of oil production. Simultaneous with the study's fictitious disruption in relations, simulated infrastructure breakdowns occurred in Saudi Arabia, Egypt, and the United States. Reports that the banking system of the United Kingdom was compromised by hacking resulted in a sharp drop in worldwide stock markets as investors feared that fund transfer systems were compromised were also added to the simulation's fact pattern. This drop, combined with massive increases in the price of oil, resulted in a looming worldwide economic collapse. In addition, a successful disinformation campaign led to media reports that the United States government was on the brink of an aggressive and unprovoked war in the Persian Gulf Region. Evidence was presented to the participants suggesting that

---


12 The Acquisition and Technology Policy Center of the RAND Corporation's National Defense Research Institute is a federally funded research and development center. See RAND Corporation (visited Nov. 11, 1998) <http://www.rand.org>. Its primary role is to improve public policy through independent research and analysis. See id.

13 The mission of the National Defense University is to serve as the post-graduate center for military education for the armed forces and to provide research to support national security objectives. See National Defense University (visited Nov. 11, 1998) <http://www.ndu.edu>.


15 See Report of the President's Commission on Critical Infrastructure Protection: Critical Foundations - Protecting America's Infrastructures B-3 (1997) (hereinafter PCCIP REPORT) (defining vulnerability as a characteristic of a critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat).

16 See Molander, supra note 14, at 8-9 (stating that participants represented industry, academia, the analytic and research communities, the intelligence community, national security policy-makers, and the military services at the levels of Chief Executive Officer, Two- and Four-star military officers and assistant secretary-level civilian employees in the U.S. government).

17 The RAND Corporation described the hypothetical fact pattern for a Persian Gulf Major Regional Contingency-Type Crisis as:

Iran seeks hegemony over the Persian Gulf region (circa 2000) by the overthrow of the Saudi Kingdom through a coup by dissidents in Saudi Arabia. A major military crisis develops in the region with a decision by the United States to deploy forces as a deterrent maneuver. Iran and its Saudi domestic 'ally' conduct information warfare attacks on the Saudi government and the U.S. government.

See id. at 6.

18 See id. at 64. (stating that during a May 4, 2000, OPEC meeting in Caracas, Iran, Iraq, Libya and Algeria promote a major cutback in production with a goal of driving the price to at least $60 (FY-95 dollars) a barrel); see generally DANIEL YERGIN, THE PRIZE: THE Epic Quest for Oil, Money and Power 519-27 (1991) (describing OPEC membership and goals).

19 See Molander, supra note 14, at 64-65 (describing a loss of power in Cairo for several hours; massive failures in the public switched telephone network in Northern California and Oregon; a mass-dialing attack on Fort Lewis, Washington; a malfunction leading to a large explosion and fire at the largest Arabian-American Oil Company refinery near Dhahran, Saudi Arabia; and a high-speed train collision in Maryland).

20 See id. at 66, 74, 78 (describing malfunctions at automatic tellers in Georgia and wild fluctuations at the Chicago Commodity Exchange bring widespread suspicion that "the Exchange was being subjected to a powerful form of electronic manipulation by parties unknown").

21 See id. at 78 (stating that at the close of the spot oil market the price for crude oil topped $100 a barrel).

22 See id. at 79 (describing the initiation of a information warfare campaign by the 'Action Arm of the Committee for Planetary Peace' with a call for widespread civil disobedience to thwart an Administration that had, "lost touch with domestic and international reality").
these incidents were the result of coordinated attacks on critical NII components in support of a coup attempt in Saudi Arabia backed by Iran.

The study's participants found that American and Allied military responses to the Persian Gulf situation were sharply degraded in effectiveness by the loss of critical NII support overseas and massive civil disobedience in the United States. The exercise highlighted the serious vulnerability of the NII to organized attacks, thereby undermining the United States' ability to protect vital national interests and its allies. The participants determined that any such attack on the NII would hinder the ability of the United States to act decisively in the event of a similar crisis in the future. Their findings emphasized the need for changes in planning against threats to the NII, especially regarding the development of information warfare capabilities by organizations or foreign nations in the future. In particular, the report suggested that current assumptions of secure communications in the United States were misplaced because of the increasing reliance upon Internet-based infrastructures for planning, logistics and research and development.

Since the RAND study's publication, the federal government has launched several initiatives to address the report's conclusions. This Comment defines the elements that are critical to the NII and how they are vulnerable to disruption through computer-based means. Next, this Comment evaluates the federal government's efforts at addressing NII vulnerabilities, the findings of the President's Commission on Critical Infrastructure Protection ("PCCIP") and the measures taken in response to the PCCIP Report by Presidential Decision Directives 62 and 63. Additionally, this Comment analyzes the current statutes relevant to NII protection and the jurisdictional mandates of selected government agencies implicated by such statutes. Finally, this Comment analyzes possible alternatives for protecting the NII based upon past government experience and the PCCIP report.

II. THE NATIONAL INFORMATION INFRASTRUCTURE AND ITS VULNERABILITIES

A. Critical Infrastructures

Information infrastructures consist of networks of computers, data storage and generating equipment, administrators and the interconne-

---

23 See id. at 66 (stating that the Iranian Ambassador to the UN is overheard to state that the United States was highly vulnerable to attacks by states and others who had mastered contemporary computer and telecommunications technology).
24 See id. at 74, 76. (describing the mobilization of six Iranian armored and mechanized divisions and coup attempts in Dhahran and Mecca, Saudi Arabia).
25 See id. at 77 (stating that the Secretary of Defense is informed by the Chairman, Joint Chiefs of Staff that a information warfare attack was then underway at almost every military base in the United States and Europe involved in the deployment to the Persian Gulf).
26 See id. at 77 (describing hypothetical efforts by the Coast Guard and local police to break up a flotilla of boats attempting to "blockade" the sealift ship U.S.S. Bob Hope from sailing to the Persian Gulf from Savannah, Georgia).
27 See id. at 41-42 (describing the findings of the study's participants).
28 See id.
29 See Todd A. Morth, Note, Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter, 30 CASE. W. RES. J. INT'L L. 567, 571 (1998) (defining information warfare as "a state activity which has an incapacitating effect on the ability of the owners of any information network to use or manage that network. This includes, but is not limited to, telecommunications, electrical power systems, gas and oil storage, transportation, banking and finance, military forces, and emergency services"); see also Robert G. Hanseman, The Realities and Legalities of Information Warfare, 42 A.F. L. REV. 173, 176 (1998) (stating the U.S. Air Force's definition of information warfare in the context of offensive and defensive operations).
30 At the conclusion of the exercise, the RAND study provided four major recommendations for addressing shortcomings in the protection of the NII. First, participants agreed that there should be a focal office within the federal government for detecting and monitoring threats to the NII at the level of the Office of the President because of the need for coordination of a large number of organizations at the federal, state and local levels of government and in private industry. Second, the federal government should embark on a risk assessment to identify potential areas of risk to the NII and develop methods to counter those threats due to the dynamic and constantly evolving environment of cyberspace threats and vulnerabilities. Third, the government's role in defending and protecting against threats to the NII must be well defined. The primary role advocated was maintenance of critical NII systems, promoting policies among private industry to reduce vulnerability and improving recovery capabilities in the event of attack. Fourth, the vulnerability of the NII needs to be addressed as a national security concern rather than simply a public policy issue because of the high probability that the sources of disruption would in many cases originate from overseas sources. See Molander, supra note 14, at xvii-xxi.
31 See Henry H. Perrett Jr., Law and the Information Superhighway §1.2 (1996) (defining the types of computers comprising information infrastructures as "clients" with which users interact directly and "servers" which store and
tions between these components. In support of these building blocks of information infrastructures are public switched telephone networks ("PSTN"), satellite communications networks, private networks and the Internet. Through the creation of such information infrastructures, large amounts of data can be transferred to several locations simultaneously, increasing the ability of all users to communicate more efficiently. Beginning in the early 1990's, the rapid commercialization of the Internet resulted in the expansion of the use of such infrastructures and eventually, the creation of the NII.

Today, many major industries, particularly those in the telecommunications and energy areas, have utilized the NII to accelerate the quality, quantity and efficiency of the services which they provide. Technological advances facilitated by the NII have yielded improved services at lower costs, opened up new markets for goods and services and accelerated the flow of new ideas. As a result, however, the dependence on these technologies has increased and eliminated the redundancy which gave their predecessors resilience should failure occur. A large portion of the NII depends upon the use of the public switched telephone network and the Internet for the transfer of information. This network depends on electricity, computer operated systems, telephone lines, and fiber optic cables to facilitate communications. The increasing demand by public and private organizations for information also ensures that the number of access points will rapidly increase with time. The fundamental issue facing the government today is how to effectively maintain the NII while preventing individuals or organizations which seek to disrupt these activities from penetrating critical components of infrastructure.

This increasing dependence on information infrastructures is not merely a private sector phenomenon. The NII is integral to the operation of practically all vital defense and public service functions performed at every level of government. Specifically, five areas were identified by the PCCIP as "critical" components of the NII. These areas are telecommunications, transportation, vital human services, energy, and banking and finance. Significant disruption in any of these areas is of primary concern when discussing the threats to the NII today.

B. Threats to the NII's Critical Components

Traditionally, threats to the stability of government infrastructures have arisen in the form of physical attacks against key sites by terrorist groups or through actions by foreign nations stated that NII dependence has grown because: "Organizations have harnessed information technology to accelerate their delivery of goods and services, tighten the efficiency of their processes, and shed excess inventory and unused reserve capacity. Many businesses are so tightly balanced in their 'just-in-time' processes that recovery from even a minor disruption would prove difficult." See id.

Cyber Attack: Is the Nation At Risk?, Hearing Before the Senate Comm. on Governmental Affairs, 105th Cong. (June 24, 1998), (Testimony of George J. Talent, Director, Central Intelligence Agency) (stating "...we have staked our way of life on the use of information. We rely more and more on computer networks for the flow of essential information...reliability breeds dependence - and dependence produces vulnerabilities. ...Disruptions in information-based technologies can range from being a serious nuisance...to potentially disastrous.").

See Rattray, supra note 11, at 83 (stating that the vast majority of transactions and information flows "rely on the vulnerable public switched network for transmission by landline, microwave or satellite means").

See The National Information Infrastructure: Agenda for Action, 58 Fed. Reg. 49,025 (1993) (stating that the government has a duty to ensure that all Americans have access to the resources and job potential of the Information Age).


See id. at B-3 (describing physical security as action "taken for the purpose of restricting or limiting unauthor-
which threaten national interests. Today, while these conventional forms of action continue to occur, \[43\] new types of "threats" have arisen in conjunction with increased reliance on the NII. These threats include foreign and domestic entities (e.g., an individual, organization or nation) possessing both the capability\[44\] to exploit a weakness in a critical infrastructure\[45\] and the malicious intent\[46\] of debilitating defense or economic security.\[47\] Such entities initiate attacks\[48\] with the goal of destroying,\[49\] incapacitating\[50\] or debilitating\[51\] NII systems to accomplish the tasks assigned to them. Due to the diverse nature of the components of the NII, the individual characteristics that make them vulnerable to attack should be explored.

1. Telecommunications

The expansion of the information and communications infrastructure in the United States has led to radical changes in the way government and economy communicate. This critical infrastructure includes the PSTN, the Internet and the millions of computers for personal, commercial and governmental use. Prior to the widespread introduction of cellular service in the 1980’s,\[52\] the landline telephone system provided virtually all telecommunications service.\[53\] This system of fiber optic and copper cables comprises the backbone of the telecommunications infrastructure.\[54\] The PSTN is primarily operated by software-driven switching systems which automatically connect and disconnect users at all points of the system.\[55\] The Internet relies upon the PSTN to facilitate data transport between remote users by breaking messages into small packets of data.\[56\] This data is sent from relay point to relay point over different paths to its destination where it is reassembled upon arrival.\[57\] The lack of direct connection leaves the system vulnerable at intermediate points.\[58\]

Threats to the telecommunications infrastructure can come from physical or cyberspace\[59\] attacks at many points in the process.\[60\] Physical attacks, the traditional threat to the telecommunications infrastructure, specifically, reducing the probability that a threat will succeed in exploiting critical infrastructure vulnerabilities including protection against direct physical attacks, e.g. through use of conventional or unconventional weapons.".


\[44\] See PCCIP Report, supra note 15, at B-1 (describing capability as "the ability of a suitability organized, trained, and equipped entity to access, penetrate, or alter government or privately owned information or communications systems and/or to disrupt, deny or destroy part of a critical infrastructure").

\[45\] See id. at B-1 (defining critical infrastructures as "infrastructures which are so vital that their incapacitation or destruction would have a debilitation effect on defense or economic security").

\[46\] See id. at B-3 (describing intent as "demonstrating a deliberate series of actions with the objective of debilitating defense or economic security by destroying or incapacitating a critical infrastructure").

\[47\] See id. at B-2 (describing economic security as "the confidence that the nation’s goods and services can successfully compete in global markets while maintaining or boosting real incomes of its citizens").

\[48\] See id. at B-1 (describing an attack as "a discrete malicious action of debilitatng intent inflicted by one entity upon another. A threat might attack a critical infrastructure to destroy or incapacitate it").

\[49\] See id. at B-1. (defining destruction as "a condition when the ability of a critical infrastructure to provide its customers an expected level of products and services is negated. Typically a permanent condition. An infrastructure is considered destroyed when its level of performance is zero.").

\[50\] See id. at B-2. (defining incapacitation as "an abnormal condition when the level of products and services a critical infrastructure provides its customers is reduced. While typically a temporary condition, an infrastructure is considered incapacitated when the duration of reduced performance causes a debilitating impact").

\[51\] See id. at B-1 (defining debilitated as "a condition of defense or economic security characterized by ineffectualness").


\[54\] See generally, supra note 52, at 143-48.

\[55\] See id. at 185-86 (describing the operation of the Internet through the use of different sites to send parts of a single message or packet of data).

\[56\] See id.


\[58\] See Reno, 117 S.Ct. at 2334-35 (1997) (stating that "cyberspace" consists of methods that transmit text, sound, pictures and video images via e-mail, chat rooms and sites on the World Wide Web that, while located in no particular location, can be accessed by anyone with access to the Internet with anonymity).

\[59\] See generally PCCIP Report, supra note 15, at A-4-A-7 (discussing vulnerabilities to the NII in the areas of PSTN switching, transport of data, signalling between intermediate data transfer points, and control and management of data).
cations system and beyond the scope of this work. Deliberate attacks designed to steal, modify or destroy data have increasingly emerged as threats to the viability of the systems as it presently exists. Insiders constitute the largest known source of security threat to the telecommunications systems using cyberspace methods of attack. However, equally troublesome to the telecommunications industry is the threat of well organized outside attacks by national intelligence organizations, military information warfare units, criminals, and industrial competitors. Attacks may come in the form of destruction, alteration, remote unauthorized control or the shut down communications systems. This situation is intensified by deregulation of the telecommunications industry, resulting in the expansion of access points, increasing reliance upon automated systems to reduce costs and easier access to sensitive data and functions comprise the backbone of the system. With network elements increasingly reliant upon each other, attacks simultaneously targeting multiple sites and functions are highly difficult to defend against, particularly if they coincide with physical destruction of supporting systems in the telecommunications infrastructure.

2. Transportation

The transportation infrastructure in the United States consists of the vast network of highways, railroads, pipelines, ports and inland waterways, ... we are not alone in developing information warfare weapons. Other nations are not only watching our actions, but developing their own doctrines and contingencies as well. Americans may take some comfort from our current lead in advanced computer chip production, but other nations are close behind... Other countries can take advantage of much of the information revolution that the United States has invested heavily in, without bearing any of the costs.


See Andretta, supra note 53, at 223-24 (stating that the private sector will continue to be responsible for leading future development of the NII through competitive environments and that hundreds of companies of all sizes must strive to satisfy the vast and varying array of consumer wants and needs).


See In re: Implementation of Local Competition provisions in The Telecommunications Act of 1996, First Report and Order 11 F.C.C.R. 15499 (1996) (stating that the three principal goals of the 1996 Act are the opening of local exchange and local access markets to competition, promoting increased competition in all telecommunications markets and preserving universal service during the transition to open competition).

See id.

See Stone, supra note 52, at 188-89 (describing the development of the World Wide Web and the increased accessibility to information which has resulted from its widespread use).

See Adams, supra note 67, at 189-90.
airports, and air traffic control systems which the nation relies upon to facilitate the efficient movement of goods, services and people on both domestic and international routes.\(^74\) Assurance of the continued viability of this system is critical to the continued health of the economy and national security, particularly in the areas of air traffic control,\(^75\) ports and waterway safety,\(^76\) and the Global Positioning System.\(^77\) These elements of the transportation system, previously reliant primarily on non-electronic methods of operation, have become increasingly dependent on computer-controlled systems.\(^78\) The continued consolidation of the transportation industry in sectors such as air transport, railroads, seaborne transport and trucking has reduced the number of routes used by the transportation industry through the consolidation of distribution centers, compounding redundancy deficiencies in the event of failure of a critical component.\(^79\) The increasing congestion at selected points in the transportation system also results in pressure on government systems, particularly those connected to the air traffic control system.\(^80\) Additionally, there is a marked absence of security assurance against attacks on the NII systems upon which the transportation infrastructure depends.\(^81\) This congestion and lack of security, combined with a general lack of awareness sharply limits the government's ability to counter even a limited NII disruption in the transportation industry.

3. Vital Human Services

Vital human services provided by government entities consist of three critical NII components: (1) water supply;\(^82\) (2) emergency services;\(^83\) and (3) government services.\(^84\) Unlike other NII components, the majority of these services are maintained at the state and local levels and are primarily concerned with basic human needs and safety.\(^85\) This highly decentralized system of controls raises the possibility that failures would be localized to a specific geographical area should they

\(^74\) Transportation is defined by the PCCIP as

A critical infrastructure characterized by the physical distribution system critical to supporting the national security and economic well-being of this nation, including the national airspace system, airlines and aircraft, and airports; roads and highways, trucking and personal vehicles; ports and waterways and the vessels operating thereon; mass transit, both rail and bus; pipelines, including gas, petroleum, and other hazardous materials; freight and long haul passenger rail; and delivery services.

See PCCIP REPORT, supra note 67, at B-3.

\(^75\) See GENERAL ACCOUNTING OFFICE, AIR TRAFFIC CONTROL: WEAK COMPUTER SECURITY PRACTICES JEPORDIZE FLIGHT SAFETY, Rep. No. GAO/AIMD-98-155, at 2 (1998) (hereinafter "Rep. No. GAO/AIMD-98-155") (describing the ineffectiveness of Federal Aviation Administration security for information systems and stating that it was in violation of its own policy during a review conducted for the FAA's Office of Civil Aviation in October, 1996 because it had performed the necessary analysis to determine threats, vulnerabilities and safeguards for only 3 of 90 operational air traffic control computer systems, less than four percent).

\(^76\) See generally KEEPING ALL CHANNELS OPEN, THE ECONOMIST, Sept. 12-18, 1998, at 28-29 (describing the missions of the U.S. Coast Guard and its roles in law enforcement and administrative law).

\(^77\) See Global Positioning System (visited Nov. 11, 1998) <http://www.msl.jpl.nasa.gov/Programs/gps.html> (describing the operation of the 24 satellites which make up this navigation system).

\(^78\) See PCCIP Report, supra note, 15 at A-12 (1997).

\(^79\) See id.

\(^80\) Attention must be paid to air traffic control systems when discussing NII security. This federally run system is currently undergoing modernization, resulting in increased reliance on the exchange of information from remotely located parts of the system. See id. Current systems are primarily self contained, based upon voice communications and physical handoffs of aircraft between communications centers avoid problems connected with disruption if the NII. See id. Future plans, however, call for the Global Positioning System of satellites to become the nation's sole radionavigation system by 2010, leading to exclusive reliance on a satellite-based system to control air traffic. This reliance raises the potential for disruptions at a single point in the air traffic control system to effect the entire system. See Ed Hazelwood, Air Traffic Control Outlook: FAA Considers Backup for GPS, 148:5 AVIATION WEEK & SPACE TECH. 58 (1998).

\(^81\) See Rep. No. GAO/AIMD-98-155, supra note 75, at 11

See PCCIP Report supra note 15, at B-4 (defining water supply systems as "a critical infrastructure characterized by the sources of water, reservoirs and holding facilities, aqueducts and other transport systems, the pipelines, the cooling systems and other delivery mechanisms that provide for domestic and industrial applications, including systems for dealing with water runoff, waste water, and fire-fighting.").

\(^82\) See id. (defining emergency services as "critical infrastructure characterized by medical, police, fire, and rescue systems and personnel that are called upon when an individual or community is responding to emergencies. These services are typically provided at [the county or metropolitan area] level. In addition, state and Federal response plans define emergency support functions to assist in response and recovery").

\(^83\) See id. at B-2 (defining government services as "sufficient capabilities at the Federal, state and local levels of government are required to meet the needs for essential services to the public").

\(^84\) See id. at A-44 (describing the differences between vital human services infrastructures and other critical infrastructures).
However, a loss of confidence in the government's ability to maintain these systems in times of crisis and the possible interstate effects of failure necessitates their inclusion in the NII as critical infrastructures.\textsuperscript{87}

4. \textbf{Energy}

All information infrastructures depend on the availability of energy to operate. Of particular concern when discussing energy and the NII is the vulnerability of electric power systems,\textsuperscript{88} oil and gas refining and transmission facilities.\textsuperscript{89} Many private entities providing energy services are attempting to minimize costs and increase efficiency through the increased use of automation.\textsuperscript{90} Compromising these control systems could lead to widespread disruption of services and physical destruction of equipment vital to recovery efforts. An effective method to facilitate such a breakdown is to alter or disrupt the information and control systems used to operate major components of the systems.\textsuperscript{91} Currently, there is little awareness within private industry on information security and the consequences of a compromise in security of operating systems.\textsuperscript{92} This results in the use of NII based systems to control various aspects of the energy production process from raw materials production to power generation and refining processes.\textsuperscript{93} The increased use of industry-wide systems for coordination of supplies, the centralization of previously dispersed control systems and dependence on the use of the PSTN raise the possibility that the breakdown of one system due to attack could disrupt service throughout the entire energy distribution infrastructure.\textsuperscript{94}

5. \textbf{Banking and Finance}

Banking and finance infrastructures\textsuperscript{95} of concern to the NII include banks, financial service companies, payment systems, investment companies and securities and commodities exchanges.\textsuperscript{96} The banking and financial sector is the most secure component of the critical NII because theft prevention mechanisms and systems for recording transactions ensure its reliability and provide redundancy in the event of unauthorized access.\textsuperscript{97} At the operational level, however, reliance on non-U.S. information infrastructures for international fund transfers and securities trading, as well as dependence on the telecommunications and energy industries to facilitate all financial transfers create vulnerabilities because they allow access to the NII by parties which may not observe the same standards of security as those located in the United States.\textsuperscript{98}

Furthermore, a reluctance to share information dealing with cyber attacks and protection methods exists within the industry and between government increased use of technology by the energy industry to maximize efficiency).

\begin{itemize}
  \item See id.
  \item See PCCIP Report, supra note 15, at A-14-A-53 (demonstrating that emergency services rely heavily on computer controlled PSTN systems for dispatch of appropriate first responders, coordination, incident containment and the emergency 911 system. This results in the possibility that emergency services could be future targets of outside groups or individuals purposely or indirectly while attacking another part of the NII).
  \item See PCCIP Report, supra note 15, at B-2 (defining electrical power systems as "a critical infrastructure characterized by generation stations, transmission and distribution networks that create and supply electricity to end-users so that end-users achieve and maintain normal functionality, including the transportation and storage of fuel essential to that system").
  \item See id. (defining gas and oil production, storage and transportation as "a critical infrastructure characterized by the production and holding facilities for natural gas, crude and refined petroleum, and petroleum-derived fuels, the refining and processing facilities for these fuels and the pipelines, ships, trucks, and rail systems that transport these commodities from their source to systems that are dependent upon gas and oil in one of their useful forms").
  \item See Karl Rabago, Information Technology: It's Not Just Business Anymore, 134 FORT. 23, 24-25 (1996) (describing the
\end{itemize}
ment authorities because of the fear that public confidence will undermined. Reporting is generally compartmentalized and few trusted methods exist for sharing the kinds of information needed to make an overall assessment of what the result of a coordinated attack would be.

III. INFRASTRUCTURE PROTECTION INITIATIVES AND ORGANIZATIONS

A. National Security Directive No. 42

One of the earliest unclassified documents describing preparations to protect the NII by the defense and intelligence communities is National Security Directive No. 42 ("NSD 42"). This document, dated July 5, 1990, "National Policy for the Security of National Security Telecommunications and Information Systems," established the initial objectives, policies, and organizational structures to prevent the compromise of secure national security systems and disseminate information to affected government agencies. Specifically, NSD 42 created the National Security Telecommunications and Information Systems Security Committee ("NTISSC"), an inter-agency policy coordinating committee to oversee implementation and coordination of various activities associated with NII protection.

At the operational level, the NTISSC oversees all activities utilizing the NII which affect national security. These roles include: (1) development of specific operating policies, procedures, guidelines and priorities for implementation of NSD 42; (2) presentation of an annual report to the Executive branch on the status of national security information systems; (3) control of the release of cryptography technology to foreign governments or international organizations; and (4) the maintenance of a national system for promulgating operational policies, instructions and guidance pursuant to the goals of NSD 42.

The Assistant Secretary of Defense for Command Control, Communications and Intelligence ("ASDCCI"), directly subordinate to the Secretary of Defense, is chairperson of the NTISSC and conducts liaison activities with the intelligence community through the National Security Council.

The Department of Defense seized an early role in NII protection activities after it found itself the target of many of the original unauthorized entry attempts. The creation of NTISSC provided a forum for discussion of policy issues relating to communications and intelligence and is composed of a voting representatives from the Secretaries of State, Treasury, Defense, Transportation, Energy, the Office of Management and Budget, the Assistant to the President for National Security Affairs, the Central Intelligence Agency, the Joint Chiefs of Staff and each of the armed services, the Federal Bureau of Investigation; the Federal Emergency Management Agency, the General Services Administration, National Security Agency, the National Communications System, the Defense Intelligence Agency and the Attorney General.

99 The PCCIP Report defines trust as that:
3. bestowed by citizens based on demonstrations and expectations of 1) Their government's ability to provide for their common defense and economic security and behave consistent with the interests of society; and 2) Their critical infrastructures' ability to provide products and services at expected levels and to behave consistent with their customers' best interests.

See PCCIP Report, supra note 11, at B-3
100 See id. at A-40.
102 See id. (stating that the directive establishes initial objectives of policies, and an organizational structure to guide the conduct of activities to secure national security systems from exploitation; establishes a mechanism for policy development and dissemination; and assigns responsibilities for implementation through insuring full participation and cooperation among the various existing centers of technical expertise throughout the Executive branch, while recognizing the special requirements for protection of intelligence sources and methods).
103 The NTISSC was established to consider technical matters and develop policies, procedures, guidelines, instructions and standards as necessary to implement provisions of NSD 42. See id. at §5(a). The Committee is chaired by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence and is composed of a voting representatives from the Secretaries of State, Treasury, Defense, Transportation, Energy, the Office of Management and Budget, the Assistant to the President for National Security Affairs, the Central Intelligence Agency, the Joint Chiefs of Staff and each of the armed services, the Federal Bureau of Investigation; the Federal Emergency Management Agency, the General Services Administration, National Security Agency, the National Communications System, the Defense Intelligence Agency and the Attorney General.
104 See id.
105 See id. at §5(b)(1).
106 See id. at §5(b)(3).
107 See id. at §5(b)(4).
108 See id. at §5(b)(5).
109 See generally id. at §5(d) (stating that the Committee has a permanent secretariat composed of personnel of the National Security Agency and other personnel from Executive departments and agencies as requested by the Chairman).
110 See Robert G. Hanseman, The Realities and Legality of Information Warfare, 42 A.F. L. Rev. 179, 192-93. (stating that the Defense Information Systems Agency has estimated that Defense department Computers were attacked at least 250,000 times in 1995, that these attacks were successful 65% of the time, and the number of attacks has been doubling each year). The Defense Information Infrastructure ("DII") is "the web of communications networks, computers, software, databases, applications, weapon system interfaces, data, security services, and other services that meet the information processing and transport needs of Department of De-
systems that process classified information or information involving intelligence activities, national security and critical military or intelligence missions. Concern over the increasing vulnerability of the overall NII resulted in the ASD C'I commissioning of the RAND study detailed above. While this office is primarily concerned with defense related portions of the NII, the appearance of an expanded threat to the NII due to increased reliance on information systems, called for a government-wide assessment of what should be done to assess the situation.

B. Executive Orders No. 12,864 and No. 13,010

Outside of the Department of Defense, the Clinton Administration established of the National Telecommunications and Information Administration ("NTIA") at the Commerce Department to coordinate non-National Security related aspects of NII policy. This organization, and an advisory council consisting of thirty-seven members of the public and private sectors, was given a mandate to create NII policy. Unlike NTISSC's emphasis on security, this initiative encouraged job creation, economic growth, increased productivity and improved quality of life through utilization of the NII. The NTIA sought to connect industry, residences, schools, health care facilities and government agencies through high-speed links in the NII.

The NTIA was established with the recognition that major parts of the NII would be developed by the private sector, with the government complementing these efforts. These roles were specifically outlined in both Executive Order 12,864, establishing the advisory council for NTIA and a supplementary Federal Register notice entitled "The National Information Infrastructure: Agenda for Action."

The initiative recognized

---

117 The Advisory Council was to advise the Secretary of Commerce on matters related to the development of the NII. These issues included:
(1) the appropriate roles of the private and public sectors in developing the NII; (2) a vision for the evolution of the NII and its public and commercial applications; (3) the impact of current and proposed regulatory regimes on the evolution of the NII; (4) national strategies for maximizing the benefits of the NII, as measured by job creation, economic growth, increased productivity, and enhanced quality of life; (5) national strategies for developing and demonstrating applications in areas such as electronic commerce, agile manufacturing, lifelong learning, health care, government services and civic networking; (6) national security, emergency preparedness, system security, and network protection implications; (7) national strategies for maximizing interconnection and interoperability of communications networks; (8) international issues associated with the NII; (9) universal access; and (10) privacy, security and copyright issues.
See Executive Order No. 12,864, 58 Fed. Reg. 48,773 at §2(b) (hereinafter "Exec. Order No. 12,864").
118 See generally Connecting the Nation, supra note 114, at 16-17 (1996) (discussing the programs initiated by NTIA to assist increased Internet connection).
119 See Exec. Order No. 12,864, supra note 118.
120 See Connecting the Nation, supra note 119, at 2 (emphasizing NTIA's role in connecting public institutions and the underprivileged, while encouraging public-private investments).
121 See Connecting the Nation, supra note 119, at §1.
that these initiatives would aid the ability of U.S. firms to compete in the global economy while eliminating the constraints which had previously limited growth.\textsuperscript{125} Additionally, expanded use of the NII would improve access to government services and aid in the Administration’s Reinventing Government initiatives.\textsuperscript{124}

Increasing accessibility to the NII was not the only issue confronting the agency. Early concerns about privacy rights,\textsuperscript{125} intellectual property\textsuperscript{126} and NII security\textsuperscript{127} were identified as priority missions to be addressed. Reliability, another matter incorporated into NTIA’s mandate, was addressed in cooperation with the Federal Communication Commission’s Network Reliability Council\textsuperscript{128} and the NTISSC.\textsuperscript{129} In this role, NTIA was able to encourage the rapid expansion of the NII throughout the early and mid-1990’s, resulting in the NII in place today.

NTIA’s work and the effects of private industry initiatives in utilizing the NII for the operation of many critical infrastructures raised concerns about NII security.\textsuperscript{130} When the NTIA policy statement was released, the primary threat to the NII was impediments to growth due to the lack of digital and high capacity access services in the PSTN.\textsuperscript{131} By 1995, when RAND and NTISSC staged the information warfare exercise described earlier,\textsuperscript{132} vulnerabilities in the security of the NII became apparent. Along with these vulnerabilities came the realization that individuals began exploiting the expanded access to the NII for their own purposes.\textsuperscript{133} While none of these unauthorized entries resulted in more than nominal damage to any one part of the NII, it became clear that much more needed to be done to keep the NII secure.\textsuperscript{134}

These concerns resulted in Executive Order No. 13,010.\textsuperscript{135} Promulgated on July 15, 1996, this Order established the PCCIP to evaluate the potential threats then existing to the critical components of the NII.\textsuperscript{136} Threats were divided into two categories: physical and cyber. Physical threats included those using conventional or unconventional weapons to damage components of the NII, while the “cyber” threats were described as those emanating from the use of electronic, radio-frequency or computer-based attacks on the information or communications components that control critical infrastructures.\textsuperscript{137} In addition, the PCCIP for the first time brought together members from defense, intelligence, commerce, law

\begin{footnotesize}
\begin{enumerate}
\item See id. (stating that limits on growth of industry previously imposed by geographical location have been eliminated because of increased ability to communicate utilizing the NII).
\item See id. at 49,029.
\item See generally id. at 49,030 (demonstrating the necessary balance between the private sector’s need for access to secure communications while utilizing the NII and the preservation of the ability of government agencies to investigate illegal activities); see also id. at 49,029 (mandating that NITA review encryption technologies to protect the privacy of citizens utilizing the NII).
\item See Exec. Order No. 12,864, supra note 118, at §2(b)(10).
\item See id. at §2(b)(6).
\item The Federal Communications Commission’s Network Reliability and Interoperability Council (“the Council”) was chartered in 1996 by the Telecommunications Act of 1996 to study network reliability, interconnection, emerging technologies and essential communications during emergencies. See Pub.L. No. 104-104, 110 Stat. 56, 47 U.S.C. §256 (Coordination for interconnectivity). The Council’s work builds upon that completed by its predecessor, the Network Reliability Council, first organized by the FCC in 1992, to study causes of service outages and develop recommendations based upon its findings. The Council is composed of 35 CEO-level representatives of telecommunications carriers, manufacturers, state regulators and consumers. See generally Network Reliability and Interoperability Council, Office of Engineering and Technology, Federal Communications Commission, NRIC Network Interoperability: The Key to
\item See id. (stating that limits on growth of industry previously imposed by geographical location have been eliminated because of increased ability to communicate utilizing the NII).
\item See NSD 42, supra note 108.
\item See Molander, supra note 14, at 1-8.
\item See 58 Fed. Reg. at 49,029 (stating the need for modernization of the telecommunications infrastructure to accommodate increased use by public and private actors).
\item See supra note 12.
\item See id.
\item See id.; see also PCCIP Report, supra note 15, at 18.
\end{enumerate}
\end{footnotesize}
enforcement and private industry to discuss NII protection policy.\textsuperscript{138} Previous efforts to define and shape the NII had been divided exclusively into civilian and military areas.\textsuperscript{139} Increased commonality between uses of the NII and shared dependence on its attributes prompted a change in policy and increased cooperation at all levels by the summer of 1995.\textsuperscript{140}

The PCCIP was charged with the mission of defining issues important to NII protection\textsuperscript{141} and consulting with areas of the public and private sectors interested in NII assurance issues.\textsuperscript{142} The group would also assume a lead role in the coordination of actions of infrastructure protection\textsuperscript{143} efforts during its policy development phase. Because of need to increase coordination between the then existing infrastructure protection efforts (centered in the NTISSC and NTIA), Executive Order 13,010 created the Infrastructure Protection Task Force ("IPTF") within the Federal Bureau of Investigation\textsuperscript{144} and overseen by PC-CIP.\textsuperscript{145}

The IPTF's interim coordination mission prior to the final PCCIP report was to provide, facilitate and coordinate the provision of expert guidance to critical infrastructures within the NII to halt or confine an attack while working to restore any services affected.\textsuperscript{146} Also, the IPTF was provided that authority to facilitate any criminal investigation resulting from attacks on the NII and have the ability to call upon other executive branch agencies for support should the need arisen.\textsuperscript{147} This structure remained in place until the PCCIP released its findings and recommendations in October 1997.

C. The PCCIP Report

On October 13, 1997, the PCCIP presented its findings to the Clinton Administration.\textsuperscript{148} While the Commission found no evidence that an attack on the NII's critical components was imminent, it did find that there was widespread capability to exploit present weaknesses in the NII and that the threat posed by these weaknesses was intensifying.\textsuperscript{149} Its recommendations emphasized cooperation between infrastructure owners and operators, both inside and outside of the government.\textsuperscript{150} Because of the magnitude of the threat and its evolving nature this responsibility and the effects on the NII were deemed to be shared by all groups utilizing the NII.\textsuperscript{151}

The findings in the PCCIP report noted that one of the primary features of protection against infrastructure threats to the United States, that of geography, has become less relevant.\textsuperscript{152} Due to the ease with which computer messages can cross international boundaries through the use of the Internet, concepts such as early warning, jurisdictional boundaries and time to assess adversary's
actions had decreased in both scope and relevance. Simulated attacks carried out during the PCCIP’s analysis of the potential for disruption of the NII revealed vulnerabilities with the potential to cripple the continued function of the U.S. government in times of crisis. As a result of global integration, the report stated that the operations of U.S. infrastructures extended well beyond the ability of any single entity to protect them. New points of entry had been established to the critical infrastructure of the U.S., providing avenues of attack to adversaries abroad as well as those located domestically.

The growing irrelevance of geography and traditional methods of response to criminal or terrorist attacks were not the only factors considered when examining the vulnerability of the NII. Of particular significance to the PCCIP was that in the past 15 years, the number of software control specialists with the ability to disrupt the NII has grown from only a few individuals to well over a million worldwide. Additionally, the case of availability of the programs which enable those individuals to conduct unauthorized entries into critical control systems of the NII has spurred attempts by laypersons to achieve today what could be achieved only by a skilled professional 10 years ago. The PCCIP found that while the introduction of technology based upon the NII produced better services at lower cost by both government and industry, dependence on the continued reliability and existence of the NII was higher the ever. Processes used were efficient but lacked the redundant characteristics that non-NII systems have in case of failure.

In response to the issues raised by its survey of the NII, the PCCIP findings reflected the fact that it would disregard the infrastructure protection approaches used during the Cold War by the federal government. Compartimentalization of information and the availability of long periods of time to analyze potential threats were deemed to be obsolete for the NII protection mission. The findings contained in the report regarding security from cyber threats stated that (1) information sharing is the most immediate need; (2) responsibility is shared among owners and operators and government; (3) NII protection requires integrated capabilities of diverse federal agencies and special means for coordinating federal response to ensure these capabilities are melded together effectively; (4) the challenge is one of adapting to a changing culture; (5) the federal government has important roles in the new infrastructure protection alliance with industry and state and local governments; (6) the existing legal framework is imperfectly attuned to deal with cyber threats; and (7) research and development are not presently adequate to support infrastructure protection.

D. Presidential Decision Directives 62 and 63

A comprehensive response by the Clinton Administration to the PCCIP Report was issued on May 22, 1998 during the commencement address at the U.S. Naval Academy in Annapolis, Maryland. During the address, President Clinton unveiled the contents of Presidential Decision Di-

---

153 See id.
154 During the summer of 1997, the Department of Defense ran an exercise named “Eligible Receiver” to test the ability of the U.S. military and political structure to withstand a cyber-based attack. See James Adams, The Next World War, 187-90 (1998). The attacks focused on the NII, the military and the political leadership. The exercise utilized personnel outside of the U.S. government who had no knowledge regarding government-run NII systems. See id. In all cases, the hackers were able to gain access to vital NII systems and seriously disrupt the ability of the U.S. government to function during a crisis. See id.; see also Cyber-Invaders Leave U.S. on Brink of Darkness, Deutsche Presse-Agentur, April 16, 1998, at 12.
155 See PCCIP Report, supra note 11, at 47-48.
156 See Connecting the Nation, supra note 115.
rectives 62\textsuperscript{171} and 63\textsuperscript{172} ("PDD 62" and "PDD 63"), aimed at combating unconventional threats to the critical infrastructures of the United States.\textsuperscript{173} Based upon the recommendations of the PCCIP, these two policy statements are the foundation of the federal government's objective of protecting the NII.\textsuperscript{174}

In order to deal with the overall threat of terrorist attacks against the United States, PDD 62 discusses the missions and authorities of various government agencies regarding counter-terrorist programs currently underway.\textsuperscript{175} The goal of the directive is to limit the opportunities available for attack through increased prevention activities and create mechanisms for incident response and recovery to conventional or unconventional attacks.\textsuperscript{176} The importance of this new initiative to NII protection is found in the establishment of the Office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism ("National Coordinator") within the National Security Council.\textsuperscript{177} The role of the National Coordinator will be to oversee the implementation of policies\textsuperscript{178} in areas such as counter-terrorism, protection of critical infrastructure, preparedness and response management in the event of the use of a weapon of mass destruction\textsuperscript{179} in the United States.

As opposed to PDD 62's coverage of a wide variety of threats, PDD 63 directly describes the Clinton Administration's policy for critical NII protection. It declares that the United States shall create an initial capability to protect the NII from disruption by the year 2000 and that by 2002 this capability will be transformed into an effective defense.\textsuperscript{180} This critical infrastructure protection capability is to be designed to prevent disruption of the federal government's ability to provide for national security and general health and public safety, ensure that state and local governments are able to maintain minimum services while also ensuring the continued availability of privately owned parts of the critical NII.

To achieve these declared goals, PDD 63 established a four part organizational structure. First, each part of the NII will be assigned to a "Lead Agency" responsible for working with private parties to develop and implement a vulnerability awareness and education program.\textsuperscript{181} "Lead Agencies for Special Functions" are designated to

\textsuperscript{171} See id.
\textsuperscript{172} See also, 18 U.S.C. §2332a(c)(2) (B)-(C) (1994) (defining the term "weapon of mass destruction" as "any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors; or any weapon involving a disease organism; or any weapon that is designed to release radiation or radioactivity at a level dangerous to human life").
\textsuperscript{173} See White Paper on Critical Infrastructure Protection, supra note 172. PDD 63 states that:
\textsuperscript{174} No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from the day the President signed Presidential Decision Directive 63 the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of: the federal Government to perform essential national security missions and to ensure the general public health and safety; state and local governments to maintain order and deliver minimum essential public services; the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.
\textsuperscript{175} See id.
\textsuperscript{176} For each information sector that could be a target for significant cyber or physical attacks, a single U.S. government department is designated to serve as Lead Agency for Sector Liaison regarding NII issues. Together, the Lead Agency and the private sector counterparts are to develop and implement a Vulnerability Awareness and Education Program for their sector. See id.


coordinate activities relating to NII protection for special functions which are performed exclusively by the federal government, such as national defense and intelligence.\(^{182}\) Representatives of Lead Agencies and Lead Agencies for Special Functions meet on a regular basis under the auspices of a Critical Infrastructure Coordination Group ("CICG"), chaired by the National Coordinator.\(^{183}\) Finally, a National Infrastructure Assurance Council was established.\(^{184}\) This advisory council consists of representatives of major infrastructure providers, state and local representatives who are to advise the CICG on matters affecting non-federal infrastructures.\(^{185}\)

Outside of the advisory and coordination tasks described, PDD 63 imminently authorized the Federal Bureau of Investigation ("FBI") to create a National Infrastructure Protection Center\(^{186}\) ("NIPC") to provide warning of an imminent attack on the NII, building upon the work of the IPTF.\(^{187}\) For the first time, efforts to protect the NII have been given the ability to bring together all parts of the civilian and military resources available in a single organization. With elements responsible for warning, analysis, computer investigation, coordinating emergency response, training and application of technical tools, it has a much broader mandate to accomplish the NII protection mission than either NTISSC or NITA.\(^{188}\)

IV. PROBLEMS WITH THE CURRENT STATE OF JURISDICTIONAL AND INTERAGENCY EFFECTIVENESS IN PROTECTING THE NII

A. Current Law

The current state of the law regarding protection of the NII is defined by the Computer Fraud and Abuse Act of 1984 (the "Act"),\(^{189}\) as amended by the National Information Infrastructure Protection Act of 1996.\(^{190}\) Congress' amendment bypassed the traditional methods of attempting to adapt existing laws to newly emerging offenses involving NII protection.\(^{191}\) Additionally, because the NII encompasses more than federally-owned systems, statutory construction had to encompass unauthorized access to non-federal government computer systems.\(^{192}\)

The need to defend against newly emerging threats affecting NII resulted in the addition of Section 1030, entitled "Fraud and related activity in connection with computers."\(^{193}\) Statutory offenses occur whenever intentional unauthorized access takes place for the purpose of obtaining financial data,\(^{194}\) classified government information, comprehensive analyses and law enforcement investigation and response and includes elements responsible for warning, analysis, computer investigation, coordinating emergency response, training, outreach and development and application of technical tools. See id.

\(^{182}\) Certain functions, such as national defense and foreign affairs, related to critical infrastructure protection are chiefly performed by the Federal Government. See id. For each of these special functions, there shall be a Lead Agency for Special Function which will be responsible for coordinating all of the activities of the United States Government in that area. See id.

\(^{183}\) The Sector Liaison Officials and Functional Coordinators of the Lead Agencies, as well as representatives from other relevant departments and agencies, including the National Economic Council, will meet to coordinate the implementation of this directive under the auspices of a Critical Infrastructure Coordination Group, chaired by the National Coordinator. See id.

\(^{184}\) See id. (stating that the National Infrastructure Assurance Council is to meet periodically to enhance the partnership of the public and private sectors in protecting critical infrastructures and will provide reports to the President).

\(^{185}\) See id.

\(^{186}\) The NIPC includes elements from the FBI, US Secret Service, and other organizations experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, the intelligence community and Lead Agencies. The NIPC is linked electronically to the rest of the federal government, including other warning and operations centers, as well as any private sector sharing and analysis centers. See id. The NIPC's mission is to include providing timely warnings of international threats.

\(^{187}\) See Exec. Ord. No. 13,010, supra note 156, at §7 (stating that the NIPC consists of members from the Federal Bureau of Investigation, the Secret Service, the Department of Defense, the Central Intelligence Agency, the National Security Agency, and the Lead Agencies).

\(^{188}\) See NSD 42, supra note 101 (describing the NTISSC's primary goal of protecting the DII); see CONNECTING THE NATION, supra note 114, (describing NTIA's mandate to increase access to the NII, as opposed to increasing its security).


\(^{192}\) See generally Jo-Ann M. Adams, Comment, Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet, 12 SANTA CLARA COMPUTER & HIGH TECH. L.J. 403, 419-20 (1996) (describing the need for more elaborate government regulation of the uses of the Internet).


tion\textsuperscript{195} or any information from "any protected computer involved in interstate or foreign communication."\textsuperscript{196} Unauthorized access to a computer system that affects its use by the federal government, even if that system is owned by another entity, is also addressed.\textsuperscript{197} By using the phrase "protected computer"\textsuperscript{198} to describe non-federally owned computer systems that are involved in interstate commerce or affect the operation of federally owned computer systems, the statute goes further than previous NII-related statutes.\textsuperscript{199} This language was added by the National Information Infrastructure Protection Act of 1996 to protect any computer involved in Internet-related activities.\textsuperscript{200} Jurisdiction under the statute is thus always federal because of subject matter jurisdiction, eliminating problems associated with the application of state laws which may provide deficiencies in scope or are lacking in specificity to computer based crimes.\textsuperscript{201} The National Information Infrastructure Protection Act of 1996 thus closes many significant gaps in previous statutes which served to hinder NII protection.

The statute also applies to acts committed by persons who obtain authorized access or exceed their authorized authority to access NII systems.\textsuperscript{202} It criminalizes the transmission or insertion of a program or command into a protected computer with the intent to cause damage.\textsuperscript{203} Additionally, the use of such a command or program to defraud another party is a violation, regardless of whether damage is done to the system.\textsuperscript{204}

Access issues such as those addressed by the Act and its amendment in 1996 reflect the Second Circuit's decision in \textit{United States v. Morris}.\textsuperscript{205} In \textit{Morris}, the defendant, a doctrinal candidate at Cornell University, released a virus into the NII which eventually affected numerous installations, including military sites.\textsuperscript{206} The defendant argued that the Act was inapplicable because he had access to the system and was therefore outside the scope of the statute.\textsuperscript{207} The Second Circuit rejected this statutory construction, finding that the legislative history of the Act showed that Congress did not intend to differentiate between unauthorized access and access that exceeds authority.\textsuperscript{208} However, in its application of this construction, the Court in \textit{Morris} noted that the defense was not entirely without merit because there had been no firm statement by Congress on the subject.\textsuperscript{209} This ambiguity was remedied by the National Information Infrastructure Protection Act of 1996.\textsuperscript{210}

In addition to the National Information Infrastructure Protection Act, other federal laws exist which enforcement officials can invoke to protect the NII. The National Stolen Property Act,\textsuperscript{211} and the Electronic Communications Privacy Act,\textsuperscript{212} are useful tools in this area of law enforcement. The National Stolen Property Act prohibits the transportation in interstate commerce of goods worth more than $5,000 which have been stolen or fraudulently obtained.\textsuperscript{213} The use of this statute in protecting the NII relates to cases involving fraudulent transfer of funds or goods obtained through manipulation of a computer system.\textsuperscript{214} The Electronic Communications Privacy Act, passed in 1986, created prohibitions regarding

\textsuperscript{198} See 18 U.S.C. §1030(e)(2)(A)-(B) (stating that as used in this section the term protected computer refers to "a computer exclusively for use of a financial institution or the U.S. Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the U.S. Government and the conduct constituting the offense affects that use by or for the financial institution or the Government or which is used in interstate, foreign commerce or communication").
\textsuperscript{199} See Dillon, \textit{supra} note 191, at 508-09.
\textsuperscript{200} See id.
\textsuperscript{201} See generally Gwenn M. Kalow, Note, \textit{From the Internet to Court: Exercising Jurisdiction Over World Wide Web Communications}, 65 Fordham L. Rev. 2241, 2253-56 (1997) (discussing personal jurisdiction analyses relevant to the Internet).
\textsuperscript{202} See 18 U.S.C. §1030 (a)(5).
\textsuperscript{205} 928 F.2d 504 (2nd Cir. 1991).
\textsuperscript{206} See id. at 505-6.
\textsuperscript{207} See id. at 508-10.
\textsuperscript{208} See id. at 511.
\textsuperscript{209} See id.
\textsuperscript{210} 18 U.S.C. §1030(a)(5)(A). (allowing for criminal penalties for whoever, having knowingly accessed a computer without authorization or exceeding authorized access knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage to a protected computer shall be guilty of a felony).
\textsuperscript{213} See 18 U.S.C. §2314 (describing application of the National Stolen Property Act to fraudulent transfer of funds or goods obtained through manipulation of a computer system).
\textsuperscript{214} See id.
the interception of wire and electronic communications and can be interpreted to extend to e-mail and Internet communications transmitted over the PSTN. Both statutes therefore enhance the effectiveness of the National Information Infrastructure Protection Act because prosecutors are provided additional tools to assist them in NII protection roles.

B. Federal Agency Jurisdiction

In evaluating the federal government’s ability to prosecute acts which disrupt the security of the NII, it is necessary to examine the ability of individual federal agencies to exercise jurisdiction. The creation of numerous advisory committees, task forces and public-private commissions complicates the examination of agency roles in NII protection. An obvious choice for enforcement of statutes relating to the NII is the Department of Justice (“DOJ”), however, there are many other organizations that possess resources and responsibilities mandated by statute, Executive Order or simply institutional experience with information infrastructures. Foremost among these organizations is the Department of Defense (“DOD”).

The DOD has accumulated vast experience in dealing with intruders into its information infrastructure because of its elaborate security precautions and the sheer size of its system. This ability, however, is circumscribed by the limitations placed upon the armed forces through statutes providing that they not be used as posse comitatus. As a result, the DOD is forced to act in a supporting role regarding NII protection. Other organizations with the capability to assist in preventing attacks on the NII, such as the Central Intelligence Agency and the National Security Council are barred from domestic operations and are unable to act independently of the DOJ in preventing such activities. This is true even if the individual responsible is later found to be located in a foreign country. While limiting the activities of the armed forces and intelligence agencies in law enforcement area is a sound national policy, it does not equate with the roles that these organizations have been given with regard to the NII.

Prior to the promulgation of PDD 62 and 63, the lines between law enforcement and national security functions in the NII was clearly drawn. The Commerce Department’s NTIA organization conducted liaisons with private owners and operators within the NII, while the NTISSC coordinated military and intelligence efforts. Adoption of the PCCIP’s recommendations blurred these two areas of NII protection. The result was the creation of an organization which, while operationally located within the DOJ, contains military and intelligence personnel and utilizes them in a law enforcement capacity, namely, investigating intrusions into civilian NII systems and reporting to a member of the National Security Council. Furthermore, some of the designated Lead Agencies, such as the Department of Energy and the Department of State, have little or no capability of their own to conduct effective computer-based NII protection due to a lack of institutional knowledge of the subject. The significance of this action was to create an organization that is not as effective as its predecessors because it concentrates on inter-agency participation rather than working with the owners and operators to respond quickly and effectively to threats to the NII.

---

216 See Hanseman, supra note 29, at 192-93.
217 See Use of Army and Air Force as posse comitatus, 18 U.S.C. §1385 (1994) (stating that whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both); see also, Naval Instruction 5820.7 (1975) (Extending 18 U.S.C. §1385 to the use of the Navy and Marines as posse comitatus); see also BLACKS LAW DICTIONARY 1162 (6th ed. 1990) (defining posse comitatus as the entire population of a county above the age of fifteen, which the sheriff may summon in certain cases, as to aid him in keeping the peace, in pursuing and arresting felons, etc.).
218 See 50 U.S.C. §403(d)(3) (1994) (stating that the Central Intelligence Agency shall have no police, subpoena, law-enforcement powers, or internal security functions).
219 See id.
220 See Fact Sheet on PDD 62, supra note 173.
C. Proposed NII Protection Organization

The establishment of the CICG, the NIPC and a National Coordinator for NII protection is an important step in creating an awareness both inside and outside of government of the necessity of NII protection.222 Awareness, however, is only the first step in undertaking such an endeavor. A fundamental problem with the newly established framework is that in attempting to solve the dilemma of NII security, it creates new ones. Foremost among these is the decentralization of authority associated with the Lead Agencies concept. The CICG policy-making procedure requires the input of these agencies in formulating new policies and proposed legislation on the NII.223 This structure is therefore susceptible to the differing interests of its participants regarding methods to be employed, resources to be allocated, and to the individual agendas of each agency involved.

Additionally, private industry has been reluctant to become involved.224 PDD 63 calls for the establishment of an Information Sharing and Analysis Center ("ISAC") made up of private owners and operators of the NII.225 In theory, this coordination between the NIPC and the private sector is an excellent opportunity to create policy and provide a forum for participation associated with NII protection for groups outside the government. The reality is that not only is there a reluctance in the private sector for sharing information among competitors that may erode public confidence should a successful attack occur, the Lead Agencies associated with the ISAC have regulatory authority over the industries with which they are to cooperate.226 In establishing the ISAC concept, the Clinton Administration did not follow through on the PCCIP recommendation that some mechanism be put into place to safeguard proprietary information supplied by private owners and operators.227 Release of potentially damaging information to an industry affected by a breakdown in part of the NII could lead to calls for more stringent regulation or sanction from the very agency which is supposed to be cooperating with the affected industry.228

Regarding the role of the federal government, questions can be raised about the effectiveness of the CICG and NIPC regarding intelligence and dissemination of information. PDD 63 states that prior to the distribution of law enforcement and intelligence information the NIPC will "sanitize" the release to eliminate any sensitive national security data.229 Additionally, coordination between the National Coordinator and the NIPC is mandatory prior to the release of any public warnings of attacks by internationally based threats to

---

222 See PCCIP Report, supra note 11, at 24 (stating the importance of establishing mechanisms to protect the NII).
223 See White Paper on Critical Infrastructure Protection, supra note 172 (describing the membership of the Critical Infrastructure Coordination Group).
224 See The Role of Computer Security in Protecting U.S. Infrastructures: Hearing Before the House Comm. on Science, Subcommittee on Technology, 105th Cong., 28, 31 (1998) (statement of Russell B. Stevenson, General Counsel, CyberCash, Inc.) (stating that Congress should limit the role of government to (1) research and education aimed at enabling private actors to protect their interests more effectively and (2) identifying and addressing those weaknesses in the electronic infrastructure as a whole that cannot be effectively addressed by the private sector).
225 See White Paper on Critical Infrastructure Protection, supra note 172 (stating that in operating the Information Sharing and Analysis Center the National Coordinator shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center with the actual design and functions of the center and its relation to the NIPC determined by the private sector, in consultation with from the federal government).
226 See PCCIP Report, supra note 11, at 31-32 (discussing legal impediments to information sharing by the public sector with Lead Agencies).
227 The drafters of the PCCIP Report envisioned the creation of an environment that would allow the government and private sector to share information openly and voluntarily. See PCCIP Report, supra note 11, at 31. Success, according to the authors, depends on the ability to protect the NII as well as disseminate needed information regarding threats. See id. To accomplish this they proposed altering several legal provisions that discourage participation in areas such as antitrust, intellectual property and privacy. See id.
228 The PCCIP Report specifically mentions the need for assurances by the federal government that information provided by private organizations in any information sharing regime be given limited assurances that it will not be used against the providers. See id. at 31-33. Areas in which these assurances should be given according to report include antitrust, trust, liability, trade secrets and other confidential business information. See id. PDD 63 does not address these issues and therefore does not remove any of the previously existing impediments to information sharing which necessitated its promulgation. See id.
229 See White Paper on Critical Infrastructure Protection, supra note 172 (stating that prior to the release of information, the NIPC, in conjunction with the intelligence community, will sanitize information for inclusion into analyses and reports that it will provide federal, state and local agencies, owners and operators of critical infrastructures and to any private sector information sharing and analysis center).
the NII. There are two areas where these types of security measures fall short.

First, by limiting intelligence information to data deemed to be non-threatening to national security, the threat to the NII increases because incomplete information is disseminated. This incomplete information can create vulnerabilities because the affected portion of the NII may not either appreciate the magnitude of the threat or take incorrect precautions in response.

Second, the requirement of consultation with the National Coordinator may have the effect of slowing the process to the point of rendering a warning system ineffective. Information on the Internet can be generated in the United States, sent to an intermediate foreign destination, and then routed back to the United States attack the NII. There is no clear distinction between threats from within the United States and those originating from overseas, the capabilities and the will to act exist in both places. Because of the anonymity associated with the Internet, the sender of an attack on the NII can be anyone from a stereotypical terrorist organization in the Middle East, to a disgruntled computer programmer in Germany to a teenager in Basking Ridge, New Jersey. There is no readily ascertainable way to discover the true identity of an attacker until after a period of investigation, by which time the attack is over and the perpetrator may be reading about the results in the New York Times.

The DOJ is the only agency with the capabilities to effectively engage in both a law enforcement and investigatory role without becoming involved with regulatory oversight questions. Prior to the introduction of the restructuring associated with PDD 63, the FBI operated the IPTF using DOJ personnel with the PCCIP acting in an advisory role. This centralization of NII protection within one agency can serve to decrease inter-agency problems which may arise in the context of computer-based attacks because of confusion over which is to take the lead in responding. Furthermore, appropriations for NII protection can be assigned to one specific entity, resulting in a greater impact on operations. The Lead Agencies concept can also work within this structure. By assigning specialists to the FBI-based organization, the knowledge base necessary to understand the problems associated with private industry can be viewed from a technical, as opposed to a regulatory, perspective. Defense and intelligence organizations should also be represented, although only in an advisory capacity to share relevant and uncensored intelligence with FBI personnel. This change in mandate requires that the NTISSC should be designated the primary organization for parts of the NII involving national security computer systems on an equal status with the FBI organization. In this role, the permanent assignment of FBI personnel to operate in law enforcement roles should be contemplated to act upon information gathered by NTISSC when national security computer systems are involved.

The National Coordinator, the Clinton Administration's answer to the PCCIP's call for a coordinated NII protection policy, should be retained in its current role and given the task of coordination between the operational entities at the FBI and NTISSC and the National Security Counsel. This allows the Coordinator to formulate overall policy, freeing personnel directly involved with investigations and enforcement to play their role as protectors of the NII instead of being delegated the responsibility to meet with an ever-expanding number of advisory committees to debate future legislation.

See Morth, supra note 29, at 571 (discussing information warfare); see Rep. No. GAO/T-AIMD-96-108, supra note 133 at 2 (discussing the motivations of hackers).

See Reno, supra note 59, at 2334-35 (discussing the anonymity cyberspace).


See Exec. Ord. No. 13,010, supra note 135, at §7(a), (e) (describing the operation and roles of the IPTF).

See PCCIP Report, supra note 15, at 31-34.
V. CONCLUSION

The current structure of NII protection lacks the ability to overcome the possibility of jurisdictional and interagency based problems. The agencies with the best capabilities for detection and response to threats assigned to NII protection are unable to effectively respond due to institutional weaknesses in NII protection or, as in the case of the DOD, are likely barred by statute from doing so. The only proper solution is to return to the bifurcation between civilian and military NII protection that existed prior to PDD 62 and 63.

The NTISSC should work with the defense and intelligence related NII systems and the FBI should assume responsibility for all private and non-defense related government NII components while providing law enforcement capability to the NTISSC. The current laws in place are flexible enough to allow for effective NII protection today. However, without a clear organizational structure, the NII’s vulnerability will undoubtedly increase because of jurisdictional and interagency disputes.