USAWC STRATEGY RESEARCH PROJECT

ASYMMETRICAL THREATS AND HOMELAND SECURITY POLICY: IS AMERICA READY FOR AN ATTACK ON ITS TELECOMMUNICATIONS NETWORKS?

by

Colonel Edric A. Kirkman
United States Army

Dr. James E. Gordon
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council of Higher Education Accreditation.

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

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
18 MAR 2005		**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Asymmetrical Threats and Homeland Security Policy Is America Ready for an Attack on its Telecommunications Networks?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Edric Kirkman**	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**38**	

ABSTRACT

AUTHOR: Colonel Edric A. Kirkman

TITLE: Asymmetrical Threats and Homeland Security Policy: Is America Ready For An Attack On Its Telecommunications Networks?

FORMAT: Strategy Research Project

DATE: 18 March 2005 PAGES: 38 CLASSIFICATION: Unclassified

With the expenditure in excess of $17 billion spent on Homeland Defense since 11 September 2001, is the U.S. critical infrastructure truly secure? The asymmetrical threat is ever mounting and has significantly increased against the U.S. Perhaps the U.S. is experiencing the quiet before the storm. Given that no other country or nation-state on earth can match our armed forces, common sense drives sophisticated enemies such as Osama bin Laden and others to attack through means other than force on force. The U.S. leadership has identified 13 critical infrastructures and four Key Asset areas. Critical infrastructures range from telecommunications, economics … electrical power to transportation systems. I propose to take a critical look at the nation's readiness of telecommunications networks against terrorist attacks since the establishment of the Office of Homeland Security. This study will review the nation's posture, including national policy, plan procedures, vulnerabilities, and it will make recommendations, where, necessary regarding critical telecommunications infrastructures. The premise of this study is that the U.S. is significantly deficient in its ability to protect against such attacks.

TABLE OF CONTENTS

ABSTRACT iii

ACKNOWLEDGEMENTS vii

LIST OF TABLES ix

ASYMMETRICAL THREATS AND HOMELAND SECURITY POLICY: IS AMERICA READY FOR AN ATTACK ON ITS TELECOMMUNICATIONS NETWORKS? 1

SCOPE 1

BACKGROUND 2

CURRENT POLICY 2

STRATEGIC APPRAISAL 3

CYBERSECURITY FOR CRITICAL INFRASTRUCTURE 4

CONTROL SYSTEMS 7

CONTROL SYSTEMS AT INCREASING RISK 7

FACTORS CONTRIBUTING TO ESCALATION OF RISK 7

COMMERCIAL SATELLITE SECURITY SHOULD BE MORE FULLY ADDRESSED 9

COMMERCIAL SATELLITE SYSTEMS ARE VULNERABLE TO A RANGE OF THREATS 11

SECURITY TECHNIQUES AVAILABLE FOR SATELLITE COMMUNICATIONS 11

CONSTRUCT FOR ACHIEVING TELECOMMUNICATIONS CRITICAL INFRASTRUCTURE PROTECTION 12

BUSH ADMINISTRATION CONSTRUCT 14

NATIONAL TELECOMMUNICATIONS ADVISORY COMMITTEE 16

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL (NIAC) 16

SCIENCE AND TECHNOLOGY 17

ACHIEVING NATIONAL OBJECTIVES? 18

RECOMMENDATIONS 20

CONCLUSIONS 20

ENDNOTES 23

BIBLIOGRAPHY 27

ACKNOWLEDGEMENTS

There are many people that I would like to thank for their assistance and support during my research. First, I would like to acknowledge and thank Dr. James E. Gordon for his guidance, suggestions, and assistance in the writing and editing of this study. I would also like to personally thank Dr. James Hanlon and Lieutenant Colonel Bobby Smith for their insights and advice. Finally, I want to thank my wife, Anita, and our two sons, Lamar and Alonzo, for their patience and support.

LIST OF TABLES

TABLE 1. THREAT TO CRITICAL INFRASTRUCTURES 5
TABLE 2 RISE IN CYBER ATTACKS 6
TABLE 3. SECURITY TECHNIQUES TO ADDRESS UNINTENTIONAL & INTENTIONAL THREATS.....12

ASYMMETRICAL THREATS AND HOMELAND SECURITY POLICY: IS AMERICA READY FOR AN ATTACK ON ITS TELECOMMUNICATIONS NETWORKS?

> The U.S. government has no more important mission than protecting the homeland from future terrorist attacks.[1]
>
> - President George W. Bush (July 2002)

With expenditures in excess of $17 billion spent on homeland security since September 11, 2001, (9/11) are the U.S. critical infrastructures now secure from terrorist attack? The asymmetrical threat is constantly mounting and has significantly increased against the U.S. All indications are that terrorists will continue to attack by any means necessary in an attempt to disrupt and destroy the American way of life. Terrorists have demonstrated a history of attacks on America as evidenced by attacks beginning as early as "September 16, 1920, when anarchists exploded a horse cart filled with dynamite near the intersections on Wall and Broad Streets, taking 40 lives and wounding about 300 others."[2] Similar attacks continued with the 1993 truck bombings of the World Trade Center, of U.S. embassies in Tanzania and Kenya in 1998, and of the USS Cole in Yemen in 2000.[3] Since no other country or nation-state can match the U.S. armed forces, sophisticated enemies such as Osama Bin Laden and others have inevitably chosen to attack through means other than force-on-force. Total adherence to the Homeland Security Policy has become vital for success in repelling attacks and sustaining the American way of life. This paper examines the Homeland Security Policy and state of readiness with respect to the protection of Telecommunications, one of the most significant of 13 critical infrastructures identified by the U.S. leadership in The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets. The 13 critical sectors consist of agriculture and food, water, government, public health, emergency services, the defense industrial base, information and telecommunications, energy, transportation, banking and finance, postal and shipping, and chemicals and hazardous materials.[4]

SCOPE

This paper is bounded by the following overarching documents that are linked and significantly impact critical infrastructures protection: the National Strategy for Homeland Security; this base document establishes areas identified as critical infrastructure sectors among other key aspects of homeland security giving a general concept for homeland security; the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets; this particular document provides greater granularity on the strategy required to physically protect critical infrastructures. Lastly, the National Strategy to Secure Cyberspace; this document is

germane to the question in the topic of this paper because telecommunications include electronic software and inherently utilizes cyberspace. Within the context of this paper, the working definition of critical infrastructure means, "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[5]

BACKGROUND

Homeland security has been a significant challenge for the U.S. government, but the attacks on 9/11 demonstrated the extent of the U.S. vulnerability to terrorist threats. As a result, the U.S. declared a global war on terrorism, followed by combat operations in Afghanistan and Iraq along with other offensive and defensive actions. The current Bush administration developed and published the nation's first comprehensive National Strategy for Homeland Security, followed by the National Strategy for The Physical Protection of Critical Infrastructures and Key Assets. The administration initiated the "most extensive reorganization of the federal government in the past fifty years"[6] by proposing the Homeland Security Department. Subsequently, Congress passed the Homeland Security Act of 2002, thereby consolidating 22 federal agencies into the Department of Homeland Security. Prior to this effort, there was no single federal organization responsible for homeland security; thus, creating a fragmented effort to protect telecommunications infrastructures at best. The Department of Homeland Security became operational in March 2003.[7] The administration also created U.S. Northern Command (NORTHCOM) as a single military command to centralize military responsibility for the defense of the United States. Previously, the North American Aerospace Defense Command was the only major military command primarily missioned to defend only the air sovereignty of the U.S. Despite these laudable initiatives, much work remains. In the wake of 9/11, the U.S. found itself without coherent policy, clear objectives, adequate strategic concepts, and sufficient national power to effectively thwart terrorist attacks. The Bush administration immediately charted a path to rectify this situation and harness the nation's resources to prevent or at least minimize the impact of potential terrorist attacks upon America.

CURRENT POLICY

President Bush articulated our post-9/11 national strategy and issued Homeland Security Presidential Directive –7, subject: "Critical Infrastructure Identification, Prioritization, and Protection." "As a Nation, we are committed to protecting our critical infrastructures and key assets from acts of terrorism that would: Impair the federal government's ability to perform

essential national security missions and ensure the general public's health and safety; undermine state and local government capacities to maintain order and to deliver minimum essential public services; damage the private sector's capability to ensure the orderly functioning of the economy and the delivery of essential services; and undermine the public's morale and confidence in our national economic and political institutions."[8] This policy supports the protection of national interests. Essential to the implementation of this policy is a clear statement of the national objectives.

STRATEGIC APPRAISAL

According to the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, the *national objectives* include: "[1] identifying and assuring the protection of those infrastructures and assets that we deem most critical in terms of national-level public health and safety, governance, economic and national security, and public confidence consequences; [2] providing timely warning and assuring the protection of those infrastructures and assets that face a specific, imminent threat; [3] and assuring the protection of other infrastructures and assets that may become terrorist targets over time by pursuing specific initiatives and enabling a collaborative environment in which federal, state, and local governments and the private sector can better protect the infrastructures and assets they control."[9]

With respect to the virtual aspect of critical telecommunications infrastructures, the strategic objectives articulated in the National Strategy to Secure Cyberspace are of equal importance. The three strategic objectives are to: 1) prevent cyber attacks on America's critical infrastructures; 2) reduce national vulnerability to cyber attacks; and 3) minimize damage and recovery time from cyber attacks that do occur.[10]

Unlike historical approaches to national security, when security was considered primarily a responsibility of the federal government through our military strength and foreign policy along with other instruments of national power, homeland security and infrastructure protection have become fundamentally different since 9/11. Homeland security has prompted a major paradigm shift of national cooperation, calling for a shared responsibility with local governments and the private sector to achieve assured homeland security mission success. In many cases, the private sector will provide the frontline defense because private assets may receive first attacks. The federal government cannot provide total security alone.[11] The telecommunications sector is made up of a vast and significantly dispersed conglomeration of critical assets that provide voice and data services. This sector is continuously evolving due to rapid technological advances. Telecommunications infrastructures are subject to physical and cyber attacks; both

the government and private industry are continuously challenged to counter these threats. The Public Switched Telecommunications Network (PSTN) consists of over 20,000 switches and over two billion miles of cable with huge numbers of critical intersections within the infrastructure.[12] The PSTN is the backbone of the infrastructure; its cellular, microwave, and satellite technologies provide extensive gateways for users to connect to the network. Connections to this infrastructure include the Internet.

The Telecommunications Act of 1996 prompted companies to open the PSTN service to competition. This Act had immediate positive and negative consequences as network infrastructures became more fragmented while providing less expensive service to customers. The Telecommunications Act also caused the PSTN and the Internet to become more software-driven and increased remote management of network infrastructures. An overall benefit gained from the open competition is a more robust and redundant network. But currently there is no single source with a complete layout of the PSTN and the Internet, which makes it very difficult at this time for the Department of Homeland Security to map comprehensive diagrams needed to define appropriate thresholds for security. [13] It is very difficult to determine when a comprehensive mapping will exist. Given that 85% of the telecommunications infrastructure is owned by the private sector and only 15% by the federal government, many companies are reluctant to share proprietary information and locations of critical communications nodes without a compelling business case for doing so.[14]

CYBERSECURITY FOR CRITICAL INFRASTRUCTURE

Protecting the nation's telecommunications infrastructure is a formidable challenge. It is important to note that physical security and cyber security are intertwined and both are required to have overall security against numerous threats and vulnerabilities. Table 1 depicts threats that cannot be taken lightly.[15] Since the terrorist attacks of 9/11, warnings of the potential for terrorist cyber attacks against critical infrastructures have also increased. According to the Department of Defense, there is a rise in cyber attacks as depicted in table 2.[16] Cyber-attacks by Al Qaeda are feared. Reports by the Federal Bureau of Investigation (FBI) indicate terrorists are at the threshold of using the Internet as a tool for bloodshed.[17]

> The event I fear most is a physical attack in conjunction with a successful cyber-attack on the responders' 911 system or the power grid," Ronald Dick, director of the FBI's National Infrastructure Protection Center, told a closed gathering of corporate security executives hosted by Infraguard in Niagara Falls.[18]

Threat	Description
Criminal groups	International corporate spies and organized crime organizations pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to ire or develop hacker talent.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency (CIA), the large majority of hackers do not have the requisite tradecraft to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Hacktivists	Hacktivism refers to politically motivate attacks on publicly accessible Web pages or e-mail servers. These group and individuals overload e-mail servers and hack into Web sites to send a political message. Most international hacktivist groups appear bent on propaganda rather than damage to critical infrastructures.
Insider threat	The disgruntled organization insider is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors.
National governments and foreign intelligence services	Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of U.S. interests. According to the CIA, only government-sponsored programs are developing capabilities with the prospect of causing widespread, long-duration damage to U.S. critical infrastructures.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. However, traditional terrorist adversaries of the United States are less developed in their computer network capabilities than other adversaries. Terrorists likely pose a limited cyber threat. The CIA believes terrorists will stay focused on traditional attack methods, but it anticipates growing cyber threats as a more technically competent generation enters the ranks.
Virus writers	Virus writers are posing and increasingly serious threat. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore Zip worm, the CIH (Chemobyl) Virus, Nimda, Code Red, Slammer, and Blaster.

Source GAO analysis based on data from the FBI, CIA, and CERT/CC

TABLE 1. THREAT TO CRITICAL INFRASTRUCTURES

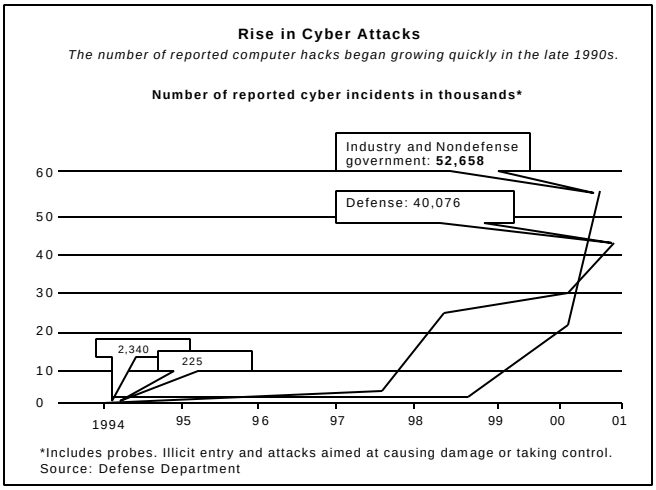


TABLE 2 RISE IN CYBER ATTACKS

Until recently, some experts considered terrorist cyber attacks as a slim possibility and of limited chance.

> Regarded until recently as remote, the risks of cyber-terrorism now command urgent White House attention. Discovery of one acute vulnerability—in a data transmission standard known as ASN.1, short for Abstract Syntax Notification—rushed government experts to the Oval Office on Feb. 7 to brief President Bush. The security flaw, according to a subsequent written assessment by the FBI, could have been exploited to bring down telephone networks and halt "all control information exchanged between ground and aircraft flight control systems."[19]

Evidence found on an Al Qaeda laptop in Afghanistan indicates Al Qaeda had access to "cracking" tools used to search out networked computers, find security deficiencies and exploit them to gain entry…[20]

> According to the National Security Agency (NSA), foreign governments already have or are developing computer attack capabilities, and potential adversaries are developing a body of knowledge about U.S. systems and methods to attack these systems. The National Infrastructure Protection Center (NIPC) reported in January 2002 that a computer belonging to an individual who had indirect links to Osama bin Laden contained computer programs that indicated that the individual was interested in the structural engineering of dams and other water-retaining structures. The NIPC report also stated that U.S. law enforcement and intelligence agencies had received indications that Al Qaeda members had sought information about control systems from multiple Web sites, specifically on water supply and wastewater management practices in the United States and abroad.[21]

One may ask why is this a major concern? It is a major concern because of the challenges that the U.S. has in a lack of secure control systems regarding its vast telecommunications infrastructures that are networked via the Internet.

CONTROL SYSTEMS

Control systems are computer-based systems that are used in many infrastructures and industries to monitor and control sensitive processes and physical functions. Such systems are used to automatically reroute heavy call or data traffic within the telecommunications arena. Control systems are typically used to collect sensor measurements and operational data from the field, process and display the information, and relay control commands to local or remote equipment. Examples may include the opening and closing of circuit breakers and setting thresholds to prevent shutdowns.[22]

There are two main types of control systems. First, distributed control systems usually used within a processing or generating plant or a small area. Second, supervisory control and data acquisition systems normally used for large, geographically dispersed distribution operations.

CONTROL SYSTEMS AT INCREASING RISK

Both types of systems are increasingly more at risk according to a U.S. Government General Accounting Report "…there has been a growing recognition that control systems are now vulnerable to cyber attacks from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and other malicious intruders." [23] In 2002, the National Research Council identified the potential for attack on control systems as an item of urgent attention. Also in 2002, "security experts reported that 70% of energy and power companies experienced at least one severe cyber attack."[24] As result, President Bush "demonstrated a concern about threat of organized cyber attacks capable of causing debilitating disruption to the Nation's critical infrastructures, economy, or national security, noting that disruption of these systems can have significant consequences for public health and safety and emphasized that the protection of control systems has become "a national priority."[25]

FACTORS CONTRIBUTING TO ESCALATION OF RISK

Many factors have contributed to the increase of risk to control systems. Four major factors include (1) the adoption of standardized technology with known vulnerabilities, (2) the connectivity of control systems to other networks, (3) insecure remote connections, and (4) the widespread availability of technical information about control systems.[26]

Previously many vendors utilized proprietary hardware, software, and network protocols which made it hard to understand the operation of control systems and more challenging for one to compromise control systems. In an effort to ease understanding of operation, "to reduce cost, improve performance and to standardize control systems, some companies have begun to adopt standardized technologies such as Microsoft's Windows, Unix-like operating systems, and common networking protocols used by the Internet for positive measures. These widely used technologies have commonly known vulnerabilities."[27] Ironically, sophisticated and effective exploitation tools are readily available to the public and easy to use.

Telecommunications infrastructures and cyber infrastructures are intertwined and as such, control systems are connected inherently to other networks often via integrated enterprise networks. This increased connectivity provides redundancy, but at the same time potentially creates further security vulnerabilities in control systems.

Unsecured remote connections exacerbate vulnerabilities in many control systems. Various organizations within the private sector often leave access links for dial-up modems to equipment and control information open for diagnostic, maintenance, and examination of system status.[28] Needless to say, these types of situations not protected with authentication or encryption increase risk and provide opportunity for potential terrorists and hackers to take control of telecommunications systems. In some cases these control systems are connected via leased lines and pass through commercial telecommunications elements or via wireless connections that further increase risk of compromise.

Perhaps one of the most dangerous risk factors is that much of the information about infrastructures and control systems is publicly available on the Internet. Terrorists or hackers would never have to leave their respective safe havens or homes to potentially wreak havoc on America's critical infrastructures.

"The availability of this infrastructure and vulnerability data was demonstrated last year by a George Mason University graduate student who, in his dissertation, reported that he had mapped every business and industrial sector in the American economy to the fiber-optic network that connects them, using material that was available publicly on the Internet—and not classified."[29]

Unfortunately, vulnerabilities exist in the United States telecommunications networks in spite of protective measures taken and are subject to exploitation by potential terrorists or hackers that may seek to disrupt the nation's economy and military command and control capabilities. Even the Department of Defense has experienced significant compromise by network intruders and is evidenced by an Israeli teenager attack in 1998 that utilized the name

"Analyzer". He was identified as Ehud Tenebaum and reported to have penetrated 400 military computer networks.[30]

Commercial satellites are another critical aspect of the telecommunications infrastructure that are not included as part of the national critical infrastructure protection strategy.

COMMERCIAL SATELLITE SECURITY SHOULD BE MORE FULLY ADDRESSED

To date, the satellite industry has not been included as part of the national effort when it comes to securing critical telecommunications infrastructure and there are no plans to include it.[31] In my opinion, this is clearly an error given the increased reliance on satellite communications to support commercial industry, military operations, and other private sector requirements. According to the General Accounting Office, in an August 2002 report, the federal agencies and other federal customers only account for approximately 10% of the commercial satellite industry customers and do not dominate this market. [32] As such, the federal customers have not influenced security techniques utilized in the commercial satellite industry.

The federal government does not control any significant commercial satellite assets, but reduces its risk by encrypting its data transmissions and by securing the few system components it controls. Given that the U.S. Armed Forces are transforming and inherently relying increasingly upon the use of commercial satellite services to augment government satellites for critical services such as global positioning, navigation, weather, imaging, and meteorological support, security for this infrastructure should be incorporated into the national strategy or at least officially added to the existing telecommunications sector. In many cases, some of the services cited above are only available via commercial satellite industry. Government relies heavily on the use of commercial satellites.

> For example, the Department of Defense (DOD) typically relies on commercial satellites to fulfill its communications and information transmission requirements for non-mission-critical data and to augment its military satellite capabilities. The importance of commercial satellites for DOD is evident during times of conflict: according to a DOD study, commercial communications satellites were used in 45 percent of all communications between the United States and the Persian Gulf region during Desert Shield/Desert Storm.[33]

The reliance on commercial satellite percentage grew well beyond 45% in Operation Iraqi Freedom. To date, the actual level of usage is classified.

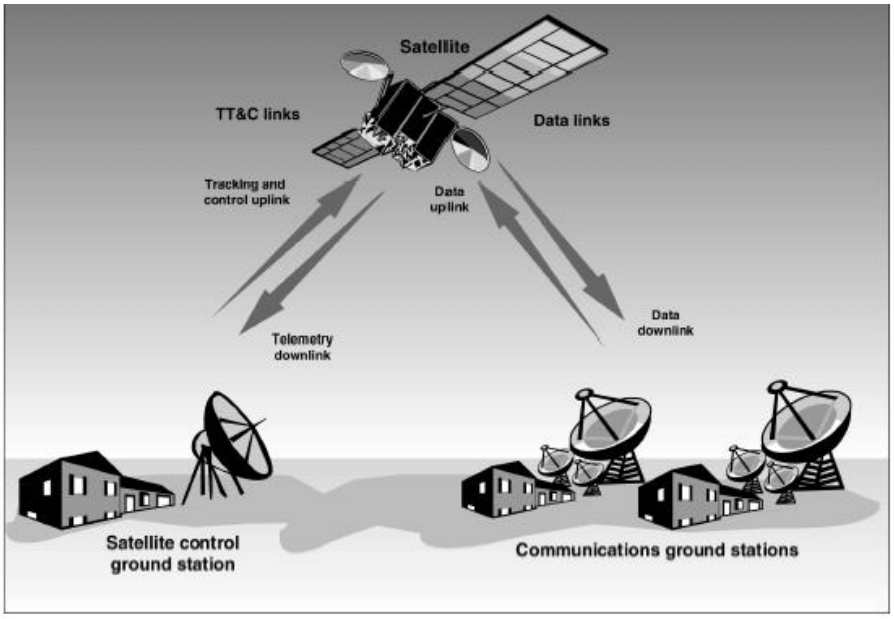
The commercial satellite industry not only impacts national security, but also economic security. "The commercial satellite industry is also a critical component of the worldwide and

national economy: the industry generated $85 billion in revenue in 2000. Accordingly, disruption of satellite services, whether intentionally or not, can have a major adverse economic impact."[34]

To better comprehend the potential security risk associated with commercial satellite systems, one needs an understanding of the key components of the system.

Satellite systems primarily consists of the following key components: (1) ground stations, (2) tracking and control links (normally referred to as tracking, telemetry, and control), and data links, and satellites.

Transmission links between the two types of ground stations are commonly referred to according to respective functions: tracking, telemetry and control (TT&C) and data links. TT&C links facilitate the exchange of critical commands and status information between ground stations and the satellite as depicted in figure 1.[35] Data links (also shown in figure 1) provides the exchange of communications, imaging data and navigation between ground stations and satellites. The last major component, the satellite, contains the payload and a bus. The term bus refers to the metal casing that houses the payload. The payload consists of the actual



Source: GAO analysis.

FIGURE 1. KEY COMPONENTS OF SATELLITE SYSTEM

equipment utilized within the satellite to perform its function; cameras for photographing clouds, transponders for communications of radio or television signal etc. The bus carries the payload of equipment to provide electrical power and fuel the propulsion of the entire satellite.[36]

COMMERCIAL SATELLITE SYSTEMS ARE VULNERABLE TO A RANGE OF THREATS

Commercial satellite systems are vulnerable to two major categories of threats Unintentional and Intentional. For the purposes of this paper, the focus will be on the intentional threats to commercial satellites. The types of threats include three subcategories: 1) Ground-based, 2) Space-based (anti-satellite), and Interference and Content-Oriented.

Ground-based stations and data links along with supporting communications networks are all vulnerable to cyber attacks. Such attacks may include physical destruction of ground stations and sabotage; space-based threats may involve interceptors (space mines, directed energy—electromagnetic pulse, laser energy); interference and content-oriented threats encompass cyber attacks: "jamming and the use of malicious software [computer viruses], denial of service, unauthorized monitoring and disclosure of sensitive information (data interception), injection of fake signals or traffic ("spoofing"), and unauthorized modification or deliberate corruption of network information, services, and databases."[37]

SECURITY TECHNIQUES AVAILABLE FOR SATELLITE COMMUNICATIONS

There are security techniques available for protecting satellite systems. For example, encryption of TT&C and data links can be done easily. Usually only the uplink is encrypted. The application of physical and cyber controls at the ground stations significantly enhances the security posture of telecommunications networks. Table 3 contains a list of security techniques available to address unintentional and intentional threats.[38] The use of these controls varies across the government and private sector in protecting satellite systems. Commercial satellite service providers may use some of these protective measures to meet security requirements. The military normally utilizes very "stringent techniques to protect their satellites than do civilian agencies or the private sector."[39] Encryption is a must for military systems.

In spite of the various security techniques available, commercial satellite systems transmitting non-national security information are not required to have encryption. There is no policy that security is required for these links. According to the General Accounting Office report, satellite owners and operators included in the review stated that, "they protect tracking and control uplinks with encryption."[40] Ironically, in the same report, National Security Agency (NSA) officials stated that not all commercial providers TT&C uplinks are encrypted. Most commercial satellite systems are designed for "open access" meaning that a transmitted signal

is broadcast universally and unprotected. However, the NSA requires approved U.S. cryptographies on TT&C and data links for U.S. space systems transmitting national security information. These are but a few of the challenges and deficiencies facing the administration and private sector to ensure security of the telecommunications infrastructures.

Satellite system Components	Security techniques available	Type of threat addressed
TT&C and data links	Encryption	Cyber attacks
	High-power radio frequency (RF) Uplink	Jamming
	Spread spectrum	Jamming
	Unique digital interface	Cyber attacks, jamming
Satellites	Hardening	Space environment, interceptors, directed-energy weapons
	Redundancy	Sabotage, space objects, interceptors, directed-energy weapons
Ground stations	Physical and logical security controls	Physical destruction, sabotage, cyber attacks, jamming, power outages
	Hardening	Natural occurrences, physical destruction, cyber attacks, jamming
	Redundancy	Natural occurrences, physical destruction, sabotage, power outages

Source: GAO Analysis.

TABLE 3. SECURITY TECHNIQUES TO ADDRESS UNINTENTIONAL & INTENTIONAL THREATS

CONSTRUCT FOR ACHIEVING TELECOMMUNICATIONS CRITICAL INFRASTRUCTURE PROTECTION

Given the vastness of the telecommunications infrastructures, a conceptual construct for defending America's critical telecommunications infrastructures may include actions taken in five major aspects: 1) preventing an attack, 2) thwarting an attack, 3) limiting damage during a successful attack, 4) reconstituting after an attack, and 5) improving defensive posture.[41]

There are perhaps three ways to prevent attacks. The first would be to deter terrorists and hackers by demonstrating the capability to levy punishment should an unauthorized entity violate network integrity. Of course this implies that the U.S. would have the means to identify the location of the attacker and bring him or her to justice. Because cyber space involves international connectivity, "deterring criminal action requires special levels of international legal machinery, to include common definitions of what constitutes a crime, standards for collection of forensic evidence and extradition agreements."[42]

The second is to prevent attacks through the establishment of cyber attacks as violations of federal law and as unacceptable behavior in the international community. This would require the development of federal laws and the creation of formal arms control agreements. Additionally, it implies that the U.S. has the means to enforce sanctions on violators.

The third way to prevent attacks involves pre-emption. To pre-empt terrorists or hackers means that the capability of the overall system has to be such that there is an extremely high level of national surveillance and means to readily and accurately identify changes from normality and respond before the intruder recognizes what is occurring. Indications are that the U.S. telecommunications infrastructures do not possess that capability in an integrated manner at the national level.

Thwarting attacks is perhaps the most effective means at present. There are numerous ways of defending systems against cyber-attack. To be most effective, there must be a comprehensive effort at all levels, local through national regarding the employment of defensive action. Some of the ways to thwart attacks include requiring authorization to enter systems, frequent checks on the integrity of critical software, monitoring and recording the use of systems to detect unauthorized activities, and developing policies and enforcing governance. Employ the use of automated security software such as firewalls, etc. Owners of systems can employ compartmentalizing procedures for the most sensitive aspects of critical infrastructure access. Lastly, owners can determine and apply common security standards and capitalize on industry best practices.

Limiting damage during a successful cyber attack is paramount. The main idea is the development of a "management" system that would enable leaders from the national to the local levels (state, county, city, town) to take swift appropriate action to minimize the damage of terrorists and or hackers. First, it implies that a capability for a technical audit is applicable to determine the level of damage; thus, prompting authorities on what steps to implement. Upon recognizing the attack, information would have to be provided to higher headquarters (in this case to the Department of Homeland Security) for analysis and for situational awareness and assessment. Inherent in limiting damage of a successful cyber attack is the preexistence or pre-established response option at local organizations and governments to the national level.

Such response options may include "calling for the re-authentication of all users or those currently undertaking critical functions or accessing critical information, putting critical transactions in quarantine until they can be more thoroughly scrutinized, backing up system status, providing real-time warning to other systems and collecting larger amounts of forensic evidence.'"[43] Some other options may include "defensive measures such as automatic tracing

at the packet [means tracking every small portion of the attacker's message back to its point of origin], message or session level, blocking traffic from or to an attacker's location and instituting legal actions to search and seize attacking computers."[44] Of course if the attacker is out side of the U.S., international law and formal arms control agreements would apply on a case-by-case basis. Damage control can also involve preplanned redundancy and the establishment of priorities to transfer telecommunications traffic load to dynamically reconfigured routes or paths. Not only is it necessary to limit the damage of a successful attack, it is of equal importance to reconstitute after an attack.

Reconstituting after an attack is normally the action taken to recover from the most urgent threats. Reconstituting usually occurs in two phases short and long term. Short-term includes immediately assessing the damage and implementing a recovery plan. Systems are restored from back-ups and made operational where possible.

Long-term reconstitution may involve the construction of physical facilities and the development of loss information impacting operations. It is very important that such long lead items and critical information be identified before hand where possible to expedite the recovery process. Managing this type of risk is vital for survival of the critical telecommunications infrastructures because it is so interdependent with virtually every aspect of American life, economically to recreationally.

Improving the defensive posture must be examined from a management perspective of learning from past lessons and experiences. One needs to identify exploitable flaws and design telecommunications systems defensively.[45] This involves protection of the system's defensive capabilities. One such example is to be very cautious of what information is made public and posted on the Internet. After conducting appropriate analysis of forensic data from attacks, distribute it to appropriate levels for all to strengthen the posture of the telecommunications infrastructure as applicable. In view of a construct for achieving critical infrastructure protection and some of the shortcomings of the telecommunications industry, one may ask what action the Bush administration is taking to protect the U.S. critical telecommunications infrastructures.

BUSH ADMINISTRATION CONSTRUCT

In a broad sense, the construct chosen by the administration appears to be well on the way to making a significant difference in the protective posture of the nation's critical infrastructures.

The president's Executive Order 13231 of October 16, 2001, "Critical Infrastructure in the Information Age," has further established the policy and approach to critical infrastructure

protection. Because of this document, several entities have been strengthened and in some cases established to facilitate the formidable task of protecting the critical telecommunications infrastructures among others.

One such entity created is the President's Critical Infrastructure Protection Board (CIPB). This particular board was established to coordinate government actions taken by the executive branch departments and agencies for certain critical infrastructures. The board consists of 25 member representatives of the executive branch department and agencies. The CIPB has an awesome challenge that appears to cover the gamut regarding infrastructures.

> The CIPB functions through ten standing committees responsible for: private sector and state and local government outreach; the security of executive branch information systems; national security systems; incident response coordination; research and development; national security and emergency preparedness communications; physical security; infrastructure interdependencies; international affairs; and the financial and banking information infrastructure.[46]

The CIPB is responsible for developing a national plan or plans for protecting the critical infrastructures. CIPB works in coordination with the Homeland Security Department and makes recommendations to the Office of Management and Budget (OMB) regarding the executive branch budget that pertains to protection of critical infrastructure. One may ask, what is the significance of this action? This action is important because it tracks the impact or lack of, in support of the national policy to the level required to affect change. Additionally, this board is authorized to ask various federal department and agencies to include in respective budgets, requests to OMB funding for research and projects concerning infrastructure protection.

As result of the administration's action, the President has published a strategic plan that addresses key issues and establishes five priorities along with major initiatives. The five priorities are: "a national cyberspace security response system; a national cyberspace security threat and vulnerability reduction program; a national cyberspace security awareness and training program securing government cyberspace; and national security and international cyberspace security cooperation."[47] The Department of Homeland Security has the primary responsibility for implementing this strategic plan. This plan was developed with significant input from owners and operators of the nation's critical infrastructure sectors. To fully implement this plan, the national government is aided by two very important advisory groups, the president's National Security Telecommunications Advisory Committee (NSTAC) and the National Infrastructure Advisory Council (NIAC).

NATIONAL TELECOMMUNICATIONS ADVISORY COMMITTEE

"Composed of up to 30 industry chief executives representing the major communications and network service providers and information technology, finance, and aerospace companies, the NSTAC provides industry-based advice and expertise to the President on issues and problems related to implementing national security and emergency preparedness (NS/EP) communications policy."[48] Such advice is paramount if the level of protection for critical telecommunications infrastructures is to be achieved, since much of it is owned by the private sector. In short the NSTAC is primarily concerned with the security and continuity of systems necessary for national security and emergency preparedness. Hopefully, the advice provided to the president corresponds to the five aspects of the defensive construct mentioned earlier.

NATIONAL INFRASTRUCTURE ADVISORY COUNCIL (NIAC)

This is the second advisory group and its focus is on the security of information systems of critical infrastructures supporting the national economy. Specifically, it focuses on entities such as banking and finance, energy, transport, manufacturing and emergency government services. This particular council is comprised of members from academia, the private sector and local and state governments.[49]

In addition to the boards and committees, the federal government has the Critical Infrastructure Assurance Office (CIAO), which has the full time responsibility for critical infrastructure protection. This office coordinates national policy planning and various initiatives with the private sector and assists government agencies in analyzing respective infrastructure dependencies and interdependencies. The CIAO plays a vital and active role in increasing awareness throughout the industry sectors; "to influence corporate information assurance policy; to promote market solutions for more robust cyber-security; to identify and address statutory and regulatory issues that potentially discourage or undermine business initiatives; and to assist voluntary efforts at enhancing critical infrastructure assurance."[50] The CIAO is further supported in its efforts by the National Infrastructure Protection Center (NIPC).

The NIPC serves as focal point for critical infrastructure threat assessments, and vulnerability and law-enforcement investigation and response. The NIPC seems to be the first organization within the administration construct that tangibly acts with respect to activity within the telecommunications arena.

> Its mission is to detect, deter, assess, warn and investigate unlawful acts involving computer and information technologies and unlawful acts both physical and cyber, that threaten or target critical infrastructures; manage computer intrusion investigations; support law enforcement, counter-terrorism and foreign counter-intelligence missions related to cyber crimes and intrusion; support

> national security authorities when unlawful acts go beyond crime and are foreign-sponsored attacks on US interests; and coordinate training for cyber-investigations and infrastructure protection government and the private sector.[51]

The administration's construct of the various boards, committees, federal organizations, voluntary public-private partnerships between government and private sector is the approach taken verses regulatory to implement the national strategy for protection of critical infrastructures. The intent is that private sector cooperation on assessing threats and sharing information on the reduction of vulnerabilities and on the establishment of best security practices will result in more secure systems.[52] It is at this point that the administration's construct falls short in achieving implementation of the national strategy. To avoid imposing costs, the construct favors voluntary public-private partnerships. This may seem like a good approach but, as mentioned earlier, many of the companies comprising portions of the telecommunications infrastructures will not invest funding over current market operations to further enhance protection without a compelling business case to do so or use of regulations or mandates to some degree. Thus, this will inherently perpetuate a disparity of technology and varying degree of security protection. Also, there is no stated standard as a minimum that must be met to ensure a baseline level of security for the telecommunications infrastructures. Of the 12 remaining critical infrastructures identified in the national strategy, all rely heavily upon the use of telecommunications to function properly. However, there are certain agencies that are working to enhance the protection of telecommunications such as the Defense Information System Agency (DISA).

DISA "provides the capstone capabilities for the entire department such as DoD Computer Emergency Response Team, the DoD wide anti-virus license, the DoD public key infrastructure (PKI), and accreditation and certification process, policy, and implementation."[53] DISA also has the primary responsibility as the command, control and communications critical infrastructure protection defense sector lead component. DISA operates a global and regional network operations and security centers to perform essential network operations on a continuous basis to ensure telecommunications infrastructures support the president through combatant commander levels.[54] Even in light of DISA's work, much of DoD information flow depends on commercial telecommunications infrastructures and in many cases the protection of these infrastructures are outside the authority and responsibility of the Department of Defense.[55]

SCIENCE AND TECHNOLOGY

Increasing the use of available cyber security technologies perhaps will make the telecommunications infrastructures more secure. Some experts believe that technologies

available are not being utilized to the maximum extent possible, mainly due to costs. Obviously, this means the funding for such capabilities must be resolved. Additionally, computer network experts state that more needs to be done to increase security awareness of system administrators and users to include enhancing information sharing to facilitate a better understanding of security vulnerabilities.[56]

Perhaps the greatest benefit at this time is the redundancy within the infrastructures to ensure that no single point of failure will disable other networks.

Many tools—including physical security, antivirus software, and anti-intrusion detection devices—are used to prevent or minimize the impact of rogue actors and terrorist attacks on telecommunications infrastructures. These tools alone are not enough. While the attack of 9/11 did not directly target the telecommunications sector, it did cause extensive collateral damage. As a whole, the telecommunications infrastructure exhibited resiliency due to the redundancy within the networks throughout 9/11 and its aftermath.[57]

ACHIEVING NATIONAL OBJECTIVES?

To achieve the national objectives for securing our telecommunications networks, we should first consider relevant strategic concepts available to the government and the private sector. Meeting these objectives requires the integrated, coordinated support of federal departments and agencies, state and local governments, and private-sector asset owners.[58] Secondly, it requires a clear understanding of the terms "critical infrastructure" to assure a unity of effort. The Draft National Infrastructure Protection Plan offers a good working definition: "critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[59] Thirdly, the government must develop incentives that will motivate businesses and other private citizens to invest capital over and above basic network operations to further enhance infrastructure security. The private sector must be convinced to see expenditures as investments and not as cost. Fourthly, the government must continue to work the effort via the advisory council for the private sector to share information to complete a comprehensive mapping of the critical telecommunications infrastructures and to reduce vulnerabilities across the spectrum. The Patriot Act certainly enhanced the conditions for information gathering in general, but it is not the answer in total.

To date, instruments of national power are not fully adequate to achieve the objectives of the homeland security policy. These instruments are problematic in that the federal government

cannot meet these objectives alone, since 85% of the infrastructure is owned by the private sector.[60] These instruments are usually focused outward to foreign nation states and international affairs. The traditional instruments of national power—diplomacy, informational, military, and economic (DIME)—do not easily or readily provide the means to assure homeland security.

Diplomacy should be utilized to coordinate with allied efforts to further implement physical and software protection measures for respective networks, acknowledging the impact of telecommunications on globalization of economies. Likewise, diplomacy should be used to deter adversaries from launching malicious computer viruses such as the “Melissa” virus, which caused more than $80 million in damages.[61]

The informational instrument of power, using the media certainly can assist in making the private sector aware of the potential security hazards. It can serve to advocate that positive action being taken as well as to inform allies that the U.S. is taking every possible measure to secure telecommunications networks, physically and virtually.

Clearly, the military resources of NORTHCOM can be used to protect the U.S. borders and selected telecommunications facilities. Currently, NORTHCOM is a military headquarters with approximately 500 personnel. Military forces have not yet been assigned and will be on an on-call basis. Currently, this limited resource does not protect telecommunications from cyber attacks. NORTHCOM will operate in support of civil authorities and not as a direct monitor or defender of telecommunications assets own by the private sector.

The economic instrument of power has traditionally been used as an element with foreign nation states. It is now time to look internal to the U.S. The federal government must find a legitimate way to reward or motivate the private sector to invest above the basic operating costs in security measures.

The federal government must make good use of the Government Network Security Information Exchanges, the Network Reliability and Interoperability Council of the Federal Communications Commission (FCC), and DISA to help prevent and mitigate the impact of terrorist attacks. Each of these organizations play a major role in helping to define an appropriate threshold for security, expanding diverse-routing capability, and in assisting the Homeland Security Department coordinate with key allies and trading partners regarding global network standards for vital assured communications. Many of these organizations have already contributed significantly in the drafting of the National Infrastructure Protection Plan. Now that the U.S. has a draft plan, it has not motivated the private sector to properly fund and implement

it. Overall much work remains to achieve synergy and fully implement the national policy to achieve homeland security of critical telecommunications infrastructures.

RECOMMENDATIONS

The current policy with respect to protecting critical infrastructures, specifically telecommunications, appears to be adequate at the national level with the exception of the modification indicated below. The current policy should be modified to include some level of financial provisions to motivate the private sector to invest above the basic operating costs to enhance security. Telecommunications critical infrastructures are vital to the nation's economy, to the nation's ability to conduct command and control, and to early warning in the event of another terrorist attack. Without this provision, the telecommunications critical infrastructures will rely primarily on redundancy and the private sector to enhance 85% of the infrastructure.[62] Further, the policy should be modified to include the establishment of signal corps units to ensure major urban areas have connectivity between appropriate authorities and first responders in the event of a terrorist attack.[63] Maximum effort should be expended by the government, private sector, and academia to develop technological solutions to strengthen the security of control systems. Given the criticality and use of commercial satellite communications, the national strategy should be modified to include these assets as a part of the critical telecommunications infrastructures.

CONCLUSIONS

Current risks are excessive and very threatening if America does not fully embrace the current policy with the changes recommended above. To date, many positive actions have been taken to make America safer since 9/11. However, research reveals that there is far more work to be done to minimize or at least reduce the impact of terrorist attacks on critical telecommunications infrastructures. This policy has certainly moved the nation in the right direction. Perhaps President Ronald Reagan said it best: "If we lose freedom here in America, there is no place to escape. This is the last stand on Earth."[64] We cannot afford failure in this vital sector. The federal government must find a way to help fund the implementation of the National Infrastructure Protection Plan, despite only 15% of government ownership of the critical assets. To some degree, the nation is operating with an incomplete road map. Will America's critical telecommunications infrastructure be ready for an attack? The telecommunications critical infrastructures may be considered one of the nation's centers of gravity through which all power and movement flow to a large degree. Clearly, DISA serves to mitigate some risks in providing some emergency communications capability in support of the civilian and military

chain of command. However, DISA alone cannot embrace the vast number of customers currently supported by the critical telecommunications infrastructures. A national effort is required to effectively protect the critical telecommunications infrastructures.

WORD COUNT=7076

ENDNOTES

[1] George W. Bush, *National Strategy for Homeland Security* (Washington, D.C.: The White House, July 2002), iv.

[2] George W. Bush, *National Strategy for Combating Terrorism* (Washington, D.C.: The White House, February 2003), 5.

[3] Ibid., 5.

[4] George W. Bush, *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets* (Washington, D.C.: The White House, February 2003), 35.

[5] Department of Homeland Security, *Draft National Infrastructure Protection Plan,* (Washington, D.C.: U.S. Department of Homeland Security, 14 July 2004), 2.

[6] Bush, *National Strategy for Homeland Security*, vii.

[7] General Accounting Office, *Department of Homeland Security: Formidable Information and Technology Management Challenge Requires Institutional Approach* (Washington, D.C.: U.S. General Accounting Office, August 2004), 1.

[8] Bush, *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets*, 11.

[9] Ibid., vii.

[10] George W. Bush, *The National Strategy to Secure Cyberspace* (Washington, D.C.: The White House, February 2003), viii.

[11] Ibid., vii, 11.

[12] Bush, *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets*, 9, 47.

[13] Ibid., 49.

[14] Bush, *National Strategy for Homeland Security*, viii.

[15] General Accounting Office, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection* (Washington, D.C.: U.S. General Accounting Office, May 2004), 24.

[16] Barton Gellman, "Cyber-Attacks by Al Qaeda Feared", *Washington Post,* June 27, 2002, Section A, 1; available from <http://www.washingtonpost.com>; Internet; accessed 1 November 2004.

[17] Ibid.

[18] Ibid.

[19] Ibid.

[20] Ibid.

[21] General Accounting Office, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems* (Washington, D.C.: U.S. General Accounting Office, March 30, 2004), 7.

[22] Ibid., 8.

[23] Ibid., 11.

[24] Ibid., 12.

[25] Ibid.

[26] Ibid.

[27] Ibid.

[28] Ibid., 13.

[29] Ibid.

[30] James Glave, "Nabbed in Israel," *Wired* 18 March 1998, [journal on-line]; available from <www.wired.com/new/technology/0 ,1282,11016,00.html>; Internet; accessed 4 Jan 2005.

[31] General Accounting Office, *Critical Infrastructure Protection*: Commercial Satellite Security Should Be More Fully Addressed (Washington, D.C.: U.S. General Accounting Office, August 2002), 3.

[32] Ibid., 1.

[33] Ibid.

[34] Ibid.

[35] Ibid., 8.

[36] Ibid., 9.

[37] Ibid., 12.

[38] Ibid., 20

[39] Ibid., 19.

[40] Ibid., 21.

[41] Stephen J. Lukasik, Seymour E. Goodman, and David W. Longhurst, *Protection Critical Infrastructures Against Cyber-Attack* (New York, Oxford Press, 2003), 16.

[42] Ibid., 17.

[43] Ibid., 19.

[44] Ibid., 20.

[45] Ibid., 21.

[46] Ibid., 60.

[47] Ibid.

[48] "National Security Telecommunications Advisory Committee (NSTAC)," available from http://www.ncs.gov/nstac/nstac.html; Internet; accessed 22 December 2004.

[49] Lukasik, 61.

[50] Ibid.

[51] Ibid.

[52] Ibid., 64.

[53] U.S. Army War College, *Information Operations Primer*, (Carlisle, PA: U.S. Army War College, December 2004), 73.

[54] Ibid., 72.

[55] Ibid., 25.

[56] General Accounting Office, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*, 105.

[57] Bush, *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets*, 48.

[58] Department of Homeland Security, iv.

[59] Ibid., 2.

[60] Ibid., vii.

[61] Robert J. Cleary, "Creator of Melissa Computer Virus Pleads Guilty to State and Federal Charges" 9 December 1999;; available from <http://www.usdoj.gov/criminal/cybercrime/melissa.htm>; Internet; accessed 11 October 2004.

[62] Department of Homeland Security, vii.

[63] The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States Executive Summary: (Washington, D.C. National Commission on Terrorist Attacks upon the United States, 2004), 397.

[64] Cox, Denny, “Patriotism Taking solace in the past,” Soundoff 15 November 2001; available from http://www.ftmeade.army.mil/SoundOFF/archives/SO2001/15Nov2001/html>; Internet; accessed 22 February 2005.

BIBLIOGRAPHY

Bush, George W. *Executive Order on Critical Infrastructures Protection* , Washington, D.C.: The White House, October 2001.

_____. Homeland Security Presidential Directive (HSPD-7). *Identifying, Prioritizing, and Protecting Critical Infrastructure*, Washington, D.C.: The White House, December 2003.

_____. Homeland Security Presidential Directive (HSPD-7). *Critical Infrastructure Identification, Prioritization, and Protection*, Washington, D.C.: The White House, December 2003.

_____. *National Strategy for Homeland Security*, Washington, D.C.: The White House, July 2002.

_____. *The National Security Strategy of the United States of America* . Washington, D.C.: The White House, September 2002.

_____. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington, D.C.: The White House, February 2003.

_____. *The National Strategy to Secure Cyberspace*, Washington, D.C.: The White House, February 2003.

Cable News Network (CNN). "Master Hacker 'Analyzer' Held in Israel." 18 March 1998. Available from <http://www.cnn.com/TECH/computing/9803/18/analyzer>. Internet. Accessed 4 January 2005.

Cox, Denny, "Patriotism Taking solace in the past," Soundoff 15 November 2001; available from http://www.ftmeade.army.mil/SoundOFF/archives/SO2001/15Nov2001/html>; Internet; accessed 22 February 2005.

Daalder, Ivo H., I.M. Destler, James M. Lindsay, Paul C. Light, Robert E. Litan, Michael E. Halon, Peter R. Orszag, and James B. Steinberg. *Assessing the Department of Homeland Security*. Washington, D.C.: The Brookings Institution, 2002.

Gellman, Barton. "Cyber-Attacks by Al Qaeda Feared." *Washington Post*, 27 June 2002, sec. A, p. 1. Available from <http://www.washingtonpost.com>. Internet. Accessed 1 November 2004.

Glave, James. "Nabbed In Israel." 18 March 1998. Available from <http://www.wired.com/news/technology/0 ,1282,11016,00.html>. Accessed 4 January 2005.

Hennessy, John L., David A. Patterson, and Herbert S. Lin. Information Technology for Counterterrorism. Washington, D.C.: The National Academies Press, 2003.

Isenberg, David, Less Talk, More Walk: Strengthening Homeland Security Now. Washington, D.C.: Center for Defense Information, 2002.

National Security Telecommunications Advisory Committee (NSTAC), Available from <http://www.ncs.gov/nstac/nstac.html>. Internet. Accessed 22 December 2004.

Robert J. Cleary, “Creator of “Melissa” Computer Virus Pleads Guilty to State and Federal Charges” 9 December 1999; available from http://www.usdoj.gov/crimianal/cybercrime/melissa.htm; Internet; accessed 11 October 2004.

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States Executive Summary: (Washington, D.C. National Commission on Terrorist Attacks upon the United States, 2004).

Tishuk, Brian S. “Testimony of Brian S. Tishuk before U.S. House Financial Service Committee on Protection Our Financial Infrastructure: Preparation and Vigilance.” 8 September 2004. Available from <http://www.financialservices.house.gov/media/pdf/090804bt.pdf>. Internet. Accessed 25 September 2004.

U.S. Army War College, *Information Operation Primer*, U.S. Army War College, Carlisle, PA. December 2004.

U.S. Department of Homeland Security, *Draft National Infrastructure Protection Plan*. Washington, D.C.: U.S. Department of Homeland Security, 14 July 2004.

_____. *Formidable Information and Technology Management Challenge Requires Institutional Approach*. Washington, D.C.: U.S. General Accounting Office, August 2004.

U.S. General Accounting Office. *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems.* Washington, D.C.: U.S. General Accounting Office, March 2002.

_____. *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*. Washington, D.C.: U.S. General Accounting Office, February 2003.

_____. *Critical Infrastructure Protection: Commercial Satellite Security Should Be More Fully Addressed*. Washington, D.C.: U.S. General Accounting Office, August 2002.

_____. *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*. Washington, D.C.: U.S. General Accounting Office, July 2004.

_____. *Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities*. Washington, D.C.: U.S. General Accounting Office, July 2001.

_____. *Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks*. Washington, D.C.: U.S. General Accounting Office, September 2001.

_____. *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*. Washington, D.C.: U.S. General Accounting Office, May 2004.

U.S. Library of Congress. Congressional Research Service. CRS Report for Congress prepared by Dana A. Shea. *Critical Infrastructure: Control Systems and the Terrorist Threat*. Washington, D.C.: Congressional Research Service, 14 July 2003