



**STRATEGY
RESEARCH
PROJECT**

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

CYBER TERRORISM: A THREAT TO NATIONAL SECURITY

BY

**COLONEL JOYCE E. ELLIOTT
United States Air Force Reserve**

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

USAWC CLASS OF 2002



U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

20020806 271

USAWC STRATEGY RESEARCH PROJECT

CYBERTERRORISM: A THREAT TO NATIONAL SECURITY

by

COLONEL JOYCE E ELLIOTT
USAFR

DR. STEVEN METZ
Project Advisor

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

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

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

ABSTRACT

AUTHOR: Colonel Joyce E Elliott

TITLE: CYBERTERRORISM: A THREAT TO NATIONAL SECURITY

FORMAT: Strategy Research Project

DATE: 09 April 2002

PAGES: 35

CLASSIFICATION: Unclassified

During the Cold War, the source and nature of threats to the United States were understood and planned for. Even after a surprise attack on Pearl Harbor in 1941, Americans assumed our island nation was secure from foreign threats. Until the 11 September attacks, Americans felt reasonably safe at home. Now it is painfully obvious that it does not take a superpower to threaten the American homeland. Terrorist groups have found ways to inflict many casualties and meet the social objectives of their terrorist campaigns. The incredible tools of the information age, while giving America a tremendous technical advantage, may also be exploited by America's adversaries. America is reexamining what it takes to defend its borders from enemies posed to attack. It must also reexamine what it takes to defend itself from a weapon that has no borders: attacks on our nation's critical information infrastructure. Defending American homeland against possible cyber attacks presents a new challenge for the United States. Consistent with the values and structures established by our Constitution, America must refine the roles and responsibilities we assign law enforcement, intelligence agencies and the military, so they can work together, in their own spheres, to provide for public safety and the nation's defense.

TABLE OF CONTENTS

ABSTRACTiii

ACKNOWLEDGEMENTS.....vii

CYBERTERRORISM: A THREAT TO NATIONAL SECURITY.....1

THE CYBER THREAT..... 1

THE TERRORIST THREAT4

THE HACKER TOOLS 7

THREATS TO AMERICA’S CRITICAL INFRASTRUCTURE 9

THREATS TO GOVERNMENT AGENCIES AND THE DEPARTMENT OF DEFENSE..... 10

THE NATIONAL RESPONSE TO THE THREAT 12

DEPARTMENT OF DEFENSE RESPONSE..... 12

FEDERAL AGENCIES RESPONSE..... 14

THE CIVILIAN RESPONSE TO THE THREAT 16

SUMMARY, CONCLUSION AND RECOMMENDATION 18

ENDNOTES21

BIBLIOGRAPHY.....25

ACKNOWLEDGEMENTS

Thank you Dixie, Gretel, Bess, Lou and Dave for your help and patience.

CYBERTERRORISM: A THREAT TO NATIONAL SECURITY

The United States has moved from an industrial to an information economy. Computers, faxes and electronic mail are indispensable throughout all segments of our society and constitute the "central nervous systems" of the US military. Weapon systems are increasingly sophisticated and rely on the same technologies that have made the civilian sector boom throughout the 90's. Unfortunately, such systems can be attacked and disabled with potentially catastrophic consequences.

The United States is the most reliant and dependent on information systems in the world. The great advantage the United States derives from this also presents the United States with unique vulnerabilities. The Nation is vulnerable to attacks on the critical information infrastructure. Computer based operations could provide adversaries with an asymmetric response to US military superiority by giving them the potential to degrade or circumvent its advantage in conventional military power. Attacks on the military, economic or telecommunications infrastructure can be launched from anywhere in the world, and they can transport the problems of a distant conflict directly to America's heartland.

Our cyber systems are at risk of intrusion by terrorists and this threat, although realized, is not given the attention it deserves. The response to date is lackluster in its scope and does not match the possible devastating effects of a systematically and intricately planned cyber attack.

This paper will provide the reader with an understanding of the problem, show the possible effects on the nation's security and look at a workable solution to the problem. This paper will take the reader on a journey into cyber terrorism starting with a look into the threats encountered day to day; the targets of cyber attacks; and who are the perpetrators. This paper will explain the response by the US government and look at a possible solution.

THE CYBER THREAT

While leading the world into the Information Age, at the same time the United States has become uniquely dependent on information technology -- computers and the global network that connect them together. This dependency has become a clear and compelling threat to the United State's economic well-being, public safety, and national security.

The world's networks, referred to by many as "cyberspace," know no physical boundaries. Our increasing connectivity to and through cyberspace increases our exposure to traditional adversaries and a growing body of new ones. Terrorists, radical groups, narcotics traffickers, and organized crime will join adversarial nation-states in making use of a burgeoning array of sophisticated information attack tools. Information attacks can supplement or replace traditional

military attacks, greatly complicating and expanding the vulnerabilities we must anticipate and counter. The resources at risk include not only information stored on or traversing cyberspace, but all of the components of our national infrastructure that depend upon information technology and the timely availability of accurate data. These include the telecommunications infrastructure itself; our banking and financial systems; the electrical power system; other energy systems, such as oil and gas pipelines; our transportation networks; water distribution systems; medical and health care systems; emergency services, such as police, fire, and rescue; and government operations at all levels. All are necessary for economic success and national security.

The Center for International Security and Cooperation defines Cyber-Terrorism as

Cyber Terrorism means intentional use or threat of us, without legally recognized authority, or violence, disruption, or interference against cyber systems, when it is likely that such use would result in death or injury of a person or persons, substantial damage to physical property, civil disorder, or significant economic harm.¹

The Federal Bureau of Investigation defines Cyber Terrorism as "Premeditated, politically motivated attacks against information, computer systems, computer programs and data which result in violence against noncombatant targets by sub-national groups or clandestine agents."² Independent audits continue to identify persistent, significant information-security weaknesses at virtually all-major federal agencies that place their operations at high risk of tampering and disruption.³

Tools of warfare in the Information Age may not be the same as in the past. Offensive information operations are attractive to many nations because they are cheap relative to the cost of developing, maintaining, and using advanced military systems. In fact, information operation tools are readily accessible to third world nations or non-state actors. "Globally, as a result of more open borders, rapid change in technology and greater information flow, we find ourselves confronting new threats that pose challenges to our interests and values; included is the use of information security and cyber terrorism."⁴

A National Intelligence Officer for Science and Technology told the Joint Economic committee recently:

IT will be the major building block for international commerce and for empowering nonstate actors. Most experts agree that the IT revolution represents the most significant global transformation since the Industrial Revolution. The integration, or fusion, of continuing revolutions in information technology, biotechnology, materials science and Nano technology will generate dramatic increases in technology investments, which will further stimulate innovation in the more advanced countries. The networked global economy will be driven by rapid largely

unrestricted flows of information, ideas, cultural values, capital, goods and services, and people: that is, globalization. This globalized economy will be a net contributor to increased political stability in the world in 2015, although its reach and benefits will not be universal.

Information attacks can consist of creating false information, manipulating information, and inserting malicious, logic based weapons in the space based, globally shared infrastructures for telecommunications and computing. Much of the information on how to exploit design attributes and security flaws of commercial computers is freely available on the Internet. George Will wrote:

Consider cyber terrorism assaults that can be undertaken from anywhere on the planet against anything dependent on or directed by flows of information. Call this soft terrorism. Although it can put lives in jeopardy, it can do its silent stealthy work without tearing flesh or pulverizing structures. It can be a weapon of mass disruption rather than mass destruction, as was explained by the President's Commission on Critical Infrastructure Protection in its 1997 report on potential cyber attacks against the "system of systems" that is modern America.⁵

The number of attacks on DoD computer networks and systems has been rising steadily. In 1990, 252 attacks were reported. Over 21,000 were reported in 2000. In the first six months of 2001, 34,754 incursions were reported. Many are not reported.⁶

The Federal Computer Incident Response Center counted 376 incidents affecting 2,732 federal systems and 86 military systems. Last year, the number of incidents reported was 586, involving 575,568 federal systems and 148 military systems. In the year 2000, an attack program called "ILOVEYOU" penetrated systems at the Defense Department, the CIA and at least a dozen other agencies, as well as an array of private companies such as AT&T and Ford.⁷

In the summer of 1997, the Joint Chiefs of Staff conducted the exercise called Eligible Receiver to find out how easy it would be for an enemy to attack US critical infrastructures and military computers. A small team of two dozen people using readily available computer hacking tools attacked the military's critical infrastructures, and within four days, crippled its ability to respond to a simulated crisis in the Pacific Theater.⁸

The National Security Agency has warned that foreign governments have already developed ways to attack US computer systems. Unfortunately, many infrastructure vulnerabilities are now routinely sought out, collated and described in great detail on the Internet by individuals apparently attracted by the ease of wide communication with like-minded persons and the virtual "lawlessness" of the forum itself. What may appear to be an instance of a hacker

breaking into a national security system may be indistinguishable from the precursors to a planned information attack. In the area of information and infrastructure security, there have been a soaring number of penetrations into commercial military and infrastructure-related computer systems. Former FBI Director Louis Freeh told Congress that FBI cases have been doubling every year⁹.

It is very difficult to assess whether an information attack is a crime or an act of war. It is clear that the lack of understanding and critical thinking about infrastructure vulnerabilities at the highest level of government has meant that the US has failed to develop effective strategy or policies for protecting critical infrastructures. There is a need for effective national policy and strategy to meet these pressing concerns.

THE TERRORIST THREAT

A well-planned and well-executed cyber attack on the United States won't just be a temporary loss of email and web sites. Terrorists could gain access to the digital controls of the nation's utilities, power grids, nuclear power plants and air traffic control systems and thousands of aircraft in mid flight. Control of these systems in the wrong hands would cause absolute havoc. A cyber attack followed by a physical attack on a nuclear power plant would be unthinkable. The terrorists are sufficiently advanced. They know the vulnerabilities of the systems and they know where to find the information they need to do the most harm.

Hackers can break into network systems. They use viruses to shut down commerce with devastating impact. They can break into power companies and shut them down. They can turn off phone systems and make it impossible to communicate. If 17-year-old Californian hackers can invade military computers then it is no stretch of the imagination to think terrorists can do the same thing.

Hostile foreign governments are sending people to American universities to study computer science and then take back the knowledge to their countries and use it against the United States. North Korea, Iran, Iraq and China are training people in Internet warfare. Non-state terrorist groups are using the Internet to learn about our digital control systems and our major infrastructures. Captured Al-Qaida computers show they were using the Internet to gain sensitive information about where America is the most vulnerable; physically and in cyber space. The terrorists using cyber space are not just the usual foreign enemies. A "next generation" Timothy McVeigh could be developing a virus that could undermine the American economy.

International terrorist networks have used the explosion in information technology to advance their capabilities. The same technologies that allow individual consumers in the United States to search out and buy books in Australia or India also enable terrorists to raise money, spread their dogma, find recruits, and plan operations far a field. Some groups are acquiring rudimentary cyber attack tools. Terrorists groups are actively searching the Internet to acquire information and capabilities for chemical, biological, radiological and even nuclear attacks. Many of the 29 officially designated terrorist organizations have an interest in unconventional weapons, and Usama bin Laden in 1998 even declared their acquisition a "religious duty".¹⁰

The Canadian Office of Infrastructure Protection and Emergency Preparedness Study lists Al-Qaida's Cyber Capability.

- Al-Qaida has not engaged in Cyber attacks in the past, however, bin Laden has suggested that Al-Qaida has the expertise to use the computer as a weapon.
- Al-Qaida studied US Security Briefs
- Al-Qaida actively researched publicly available information concerning critical infrastructures posted on web sites
- Hijackers utilized cyber cafes to communicate via Internet and order airline tickets
- Terrorists utilize web sites to actively recruit members and publicize propaganda as well as to raise funds.
- Web sites also contain information necessary to construct weapons, obtain false identification

Use internet as a communications tool via Instant Messenger, chat rooms, BBS, and email¹¹ The General Accounting Office said, "a clear risk exists that terrorists or hostile foreign states could launch computer based attacks on systems supporting critical infrastructures to severely damage or disrupt national defense or vital public operations or steal sensitive data".¹² Terrorists most likely would deface web sites in the US and Allied countries to spread disinformation and propaganda; execute denial of service attacks to prevent access to legitimate users and commit intrusions into systems of US and Allied countries potentially resulting in critical infrastructure outages and corruption of vital data.¹³ Marianne Sonnenberg from the Commission on Terrorism said, "The computer is the communications choice among terrorists."¹⁴

The Department of State reports:

Terrorists have seized on the worldwide practice of using Information Technology in daily life. They embrace IT for several reasons. It improves communication and aids organization. It allows members to coordinate quickly with large

numbers of followers and provides a platform for propaganda. The Internet also allows terrorists to reach a wide audience of potential donors and recruits who may be located over a large geographical area. In addition terrorists are taking note of the proliferation of hacking and the use of the computer as a weapon. Extremists routinely post messages to widely accessible web sites that call for defacing western Internet sites and disrupting online service for example. The widespread availability of hacking software and its anonymous and increasingly automated design make it likely that terrorist's will more frequently incorporate these tools into their on line activity. The appeal of such tools may increase as news media continues to sensationalize hacking.¹⁵

International media sources cite many instances of Al-Qaida using computers and the Internet to communicate internally. Bin Laden used technologies to aid in secure communication and information dissemination such as steganography (hiding information in a web site), encryption and chat rooms, message boards and news groups. It is very common for foreign terrorist organizations to use the Internet to raise funds and recruit, as well as communicate. Terrorists use encryption to hide data and communications and protect operational plans, Ramzi Yousef, an Al-Qaida member used encryption to conceal his plan to blow up eleven US airliners.¹⁶ The Scotland Yard arrested an Al-Qaida Cell in England. One of the suspects was a computer expert and was believed to have assisted bin Laden operatives with computer and web site activities.¹⁷ A lucky journalist in Afghanistan bought a computer from a fleeing Al-Qaida member. The information found on that computer included tactics for biological and chemical warfare and plans to make a video of people fleeing the World Trade Center disaster.¹⁸

The "shoe-bomb" suspect Richard Reid sent emails before he boarded a Paris-Miami flight. In those emails he indicated he would destroy an airplane and after being thwarted from boarding an earlier flight, he asked one recipient in Pakistan if he should go again. The mail was found on the hard drives of computers Reid used while in Paris.¹⁹

Lesser-known terrorists such as the Japanese cult, Aum Shinri Kyo, which attacked the Tokyo subway with sarin nerve gas, use the Internet. Fringe militia and grievance groups use the cyber world to promote their causes such as abortion protests and the message of hate groups.²⁰ Because of the rise of the Internet and low cost of IT structures, these suspects can operate and threaten US Security.

A networked organization such as Al-Qaida is harder to target than a hierarchical organization. It is flexible, responsive and difficult to target. Using the Internet makes them even harder to find. When an enemy is building a weapon of mass destruction, they leave clues that are detectable. A satellite photo might reveal a peculiar structure or intercepted

communications will reveal a location of a weapons building facility. One cannot see the trail left by cyber terrorists and a virus is much easier and cheaper to develop than a biological weapon.

The computers found in the caves of Afghanistan revealed the terrorist's reconnaissance on the Nation's infrastructure. The terrorists learned a great deal about our large facilities extracted from amply supplied web pages. Al-Qaida also had some computer experts in their cells. To date, published information has not shown that Al-Qaida used cyber attacks, but if a 15-year-old computer hacker can do substantial damage, then it is only a matter of time before the terrorists use this tool. It is also conceivable that the terrorist groups could enlist the help of the sophisticated hackers. If young educated people are brought into the folds of terrorist groups, this new generation will have the education and talent to execute acts of cyber terrorism. Attorney General John Ashcroft warned that potential terrorist invasions of computer networks could be just as dangerous as attacks on physical places, saying that more needs to be done to protect the nation's so called critical infrastructure.²¹

THE HACKER TOOLS

An unnamed US intelligence official boasted that with \$1 billion and 20 capable hackers, he could shut down America. A terrorist could also achieve this. In 2001, the Code Red Virus came within four hours of bringing down the Internet.²² Hackers can break into systems and do great harm. Hackers invade networks for reasons of prowess or financial gain. Cyber terrorists carry out politically motivated attacks. An organized crime group broke into a European banking system and diverted over a hundred million dollars into private accounts before they were caught. If terrorist groups like Al-Qaida can do extreme damage with a few hundred thousand dollars, imagine how many horrific acts a few hundred million dollars would finance for years to come. To qualify as a cyber terrorist, an attack should result in violence against persons or property or generate fear. To date most terrorists do not have the knowledge to carry out effective attacks, while a number of hackers who do have the knowledge do not have the motivation to cause damage. There are about a thousand professional hackers in the world; people with hard-core skills, perhaps one of them will develop a passion for a terrorist's dogma. The tools, training and education are available. It's only a matter of time.

In the spring of 1998, Department of Defense networks experienced a widespread and systematic attack. Over 20 major installations' networks were compromised. The attacks called "Solar Sunrise" occurred while the military was deploying forces to the Persian Gulf in response to Iraqi provocations. The defense community and law enforcement struggled for four days to understand the nature of the attacks and identify the threat. The attacks were launched from

computers in the United States and overseas. Two California teenaged hackers demonstrated an enormous vulnerability in the DoD's unclassified computer systems that play a critical role in managing and moving US armed forces all over the globe.²³

A 17-year-old New Hampshire hacker named Dennis Moran, using the alias "Coolio", invaded military computers in Feb of 2000. Luckily, in the case of Moran, the DOD Computer Emergency Response Team (CERT) and a regional CERT quickly notified the Army's Computer Crime Investigative Unit that an intrusion had occurred and had come from the same Internet address. The Army then worked with the FBI, and Air Force's Office of Special Investigation, and the State of New Hampshire to break the case. Moran admitted he vandalized two private sector firms, and broke into one Air Force and three Army servers. The military sites were able to block him. Moran was sentenced to 9 months in prison and ordered to pay \$15,000 in restitution.²⁴

Chinese hackers, angered by the death of a Chinese pilot in a collision with an American surveillance plane, defaced several government web sites in April 2001. They invaded government and business web sites including those run by the Navy and the departments of Labor and Health and Human Services.²⁵

An US-based international hacker ring recently penetrated several telecommunications firms. Former Attorney General Reno testified that this penetration "suggests the perpetrators could have disrupted telecommunications on a national basis had they so desired."²⁶ In October of 1997, a former Pacific Gas and Electric Company worker caused a widespread outage in the San Francisco region.

Hackers use several tactics to cause damage: viruses, worms, Trojans, logic bombs, trapdoors, distributed denial of service attacks and computer intrusion tactics.²⁷ Distributed denial of service attacks happen when the hacker sends massive packets into a system. The system is overwhelmed and shuts down. A worm is a self-replicating virus that does not alter files, but resides in active memory, duplicates itself and then attaches copies to other programs.²⁸ A hacker will leave a "Trapdoor" by hacking into a network and creating a way to get back in when they want and undetected. Logic bombs are programs that reside behind the firewalls. Hackers can set them off with a remote command and then do destruction to the network.

The "I Love You Virus" was initiated by a Philippine hacker and did millions of dollars in estimated damages worldwide. Other viruses cause network degradation. Other attacks involve all levels of sophistication and take all levels of intruder technical knowledge. Low

sophistication attacks might include guessing a password, and high sophisticated attacks would include disruption of service attacks, packet spoofing and sweepers.

The simplest intrusion method for hackers and terrorists alike is the vulnerabilities in software. A software company will publish a "patch" to fix a vulnerability in their software. Companies may take up to a month or more before they use the patch. During that time the hacker or terrorist has exact instructions on the vulnerability and time to use it against the company or organization.

All of these tactics listed above represent the most serious security breaches in the history of the Internet. After hackers brought down some of the most prominent, well secured, and sophisticated Web sites to a halt in February of 2000, Chris Rouland the director of a security research laboratory at Internet Security Systems said: "If hackers can shut down Yahoo, they can shut down anything they want tomorrow."²⁹ The computer hacking tools and virus creation kits are all available on the Internet, over 30,000 web sites in all.

THREATS TO AMERICA'S CRITICAL INFRASTRUCTURE

Presidential Decision Directive 63 states: "The US will take the necessary measures to swiftly eliminate significant vulnerability to both physical and cyber attacks on our critical infrastructures, including our cyber systems."³⁰

The United States is the most computerized and interconnected society in the world. The US has enormous military clout and can project national power anywhere in the world—within hours. We have a national intelligence system that will seek out indications and provide warnings of threats and surprise attacks. We have a high tech global economy capable of providing the comforts and convenience of daily life and power our military and intelligence might.

Our very existence is supported by a set of interdependent critical infrastructures. Information systems control the infrastructures that America's way of life and survival depends. These services are so vital that their incapacity or destruction would have a debilitating impact on the defense of economic security of the United States. Our critical infrastructure includes:

- Telecommunications
- Banking and Finance
- Water Supply Systems
- Transportation
- Emergency Services
- Government Operations

- Electrical Power
- Gas and Oil Storage and Delivery

With the benefits of technology comes a new set of vulnerabilities that can be exploited by individuals and terrorist groups as well as foreign nations. An enemy does not need to travel thousands of miles and confront superior forces in an attempt to attack the US. The enemies need not risk attacking our military or even take over an airliner. They can much more easily attack our digital underbelly. Serious threats to critical infrastructure are warfare at the strategic level—a long sought goal of some terrorist organizations. IT potentially alters the time line for strategic warfare.

Winn Schwartau, the man who coined the phrase “electronic pearl harbor” in 1991 and “Electronic Warfare”, wrote a novel called Pearl Harbor dot com. The plot involves a disgruntled mathematician who is a National Security Agency computer expert. He teams up with a moneyman and a few terrorists. He uses well-coordinated precision attacks on the infrastructure such as changing all the traffic lights in New York City to begin with. The chaos brings about more chaos. He exploits privacy, networks and security seams and his goal is to bring down the US government. In the novel, he creates panic, havoc, destroys information (think bank records) and his non-kinetic action causes kinetic effects. It is a novel but a recipe book for hackers and a work order for network security practitioners. It is also a vision of why the government needs cyber warriors.³¹

The merge of computers with telecommunications has created a huge area for possible exploitation of networked information systems. Damage could be done to any information system that is a part of it or assessable through it. Since information systems must have imbedded controls and operating systems, the possibilities for manipulation of a system once penetrated would be virtually limitless.

THREATS TO GOVERNMENT AGENCIES AND THE DEPARTMENT OF DEFENSE

Congress’ investigative arm, the General Accounting Office (GAO), disclosed that in 1999 and 2000 there were more than 1,300 cyberattacks on Air Force, Army and Navy sites. In excess of 700 were deemed “serious” intrusions. Thirty-two federal agencies reported 155 computers were taken over temporarily by hackers last year. Three-quarters of the hacks involved foreign attackers. Sallie McDonald, a computer security official at the General Services Administration, testified before the House Committee on Energy and Commerce’s Subcommittee on Oversight and Investigations this April that 75 percent of the attempts by

hackers to break into government computers last year originated from abroad, up from 60 percent in 1999.

Cyber terrorism is in the realm of uncertainty and puts our security in question. In his classic book "On War", Carl von Clausewitz wrote: "War is the realm of uncertainty; three quarters of the factors on which action is based are wrapped in a fog of greater or lesser uncertainty."³² Former President Clinton said "Our security is challenged increasingly by nontraditional threats. Rather than invading our beaches or launching bombers, these adversaries may attempt cyber attacks against our critical military systems and our economic base."³³

The American military is the most information dependent force in the world. It uses its computers to help design weapons, guide missiles, pay soldiers, manage medical supplies, write memos, control radio networks, train tank crews, mobilize reservists, issue news releases, find spare parts and communicate tactics to combat commanders.³⁴ The Army is using computers in their first "digital division". This transformed unit has brought computers and networks to the battlefield. The Army plans to expand its digital effort through 2005.³⁵ The Marine Corps is joining the technological age with marines running around Camp Pendleton not only armed with rifles but with laptop and hand-held computers. They are exercising a capability to send and receive targeting information for manned and unmanned weapons. The 3rd Fleet is using new computer systems and software to connect generals and admirals with a digital picture of the battlefield.³⁶ There is not much in the Air Force that is not networked and controlled by computers.³⁷

Many military missions rest on a foundation of computer driven information networks. Almost 95 percent of military communications travel on civilian systems. The Internet was created for sharing, not security. Military computers are tied into the Internet commonly used by everyone else on the planet. Military bases are hooked into the electric power grid. The Army moves its tanks and vehicles by the rail systems and pentagon purchases are made through the federal banking system.³⁸ If the civilian computer systems stop working, America's armed forces will be immobilized.

General Ralph Eberhardt, commander of USSPACECOM, testified before the U.S. Senate Armed Service Committee Strategic Subcommittee on Computer Network Defense and Computer Network Attack. "There is a real and growing threat to Department of Defense unclassified computer systems and networks. It is no secret that the U.S. military's operational capability depends on information superiority ---our ability to make smarter, faster decisions. This is both a tremendous advantage and a potential vulnerability".³⁹

THE NATIONAL RESPONSE TO THE THREAT

The US government has become very concerned about protecting and safeguarding the nation's computer networks and information infrastructure. Secretary of Defense Rumsfeld said: "The nation is vulnerable to new forms of terrorism ranging from cyber attacks to attacks on military bases abroad to ballistic missile attacks on US cities."⁴⁰ To defend the nation, different federal agencies have been created to develop tools, strategies and policies to deal with intrusions that could damage vital national information. Information is oxygen to a democracy. The information can't flow if the national infrastructure is damaged. To combat this threat, President William Clinton signed Presidential Decision Directive 63, "Critical Infrastructure Protection" in 1998. President Clinton wrote: "I intend that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."⁴¹

In the FY 1997 Defense Authorization Act, Congress directed the President to develop and report on a strategy to protect the nation against information attack. At a minimum, an effective national strategy would assign responsibilities to departments and agencies, direct an architecture for indications and warning of possible attacks, and establish a decision making process integrating key government and industry players. It would coordinate existing activities (such as security disciplines, industrial base policy, disaster preparedness) to maximize their effectiveness, and to identify the key areas of additional work and investment that are needed for maximum payoff.

In May 1998, President Clinton signed a new Presidential Decision Directive—PDD63-- that lays a foundation for infrastructure policy development and appoints a National Coordinator for Security, Infrastructure Protection and Counter Terrorism to direct PDD-63 activities.⁴²

The PDD declares as a national goal the ability to protect infrastructures from intentional acts; emphasizes the importance of public and private partnership, and directs each sector to produce a plan; establishes a structure for coordination and directs the NSC principals to submit a schedule to implement a national plan integrating the sector plans.⁴³

DEPARTMENT OF DEFENSE RESPONSE

To combat computer network attacks within the Department of Defense, on 1 October 1999, the President assigned USCINCSpace the responsibility to lead the Computer Network Defense (CND) mission. USSPACECOM created the Joint Task Force for Computer Network Defense (JTF-CND) and the Joint Information Operations Center (JIOC) to protect and defend information vital to military forces and to bolster CND of all networks operated as part of the

Defense Information Infrastructure. The mission of the Joint Task Force-Computer Network Operations is subject to the authority and direction of USCINCSpace. The JTF-CNO, along with the unified commands, services and DOD agencies coordinate and direct the defense of DOD computer systems and networks; coordinate and, when directed, conduct computer network attack in support of CINCs and national objectives.⁴⁴

Computer Network Operations are comprised of two specific yet complementary mission areas: Computer Network Defense (CND) and Computer Network Attack (CNA). The CND mission is to defend DOD computer networks and systems from any unauthorized event whether it is a probe, scan, virus incident or intrusion. The CNA mission is to coordinate, support and conduct, at the direction of the National Command Authority (NCA), computer network attack operations in support of regional and national objectives.⁴⁵

In December 2000, USCINCSpace directed his staff to look at the feasibility of combining specific aspects of CND and CNA under a single operational commander. The intent behind the consolidation was to operationalize CND and CNA and fully integrate those capabilities with air, land, sea and space forces across the full spectrum of conflict. In April of 2001, the JTF-CND was redesignated Joint Task Force-computer Network Operations (JTF-CNO). The newly named organization is comprised of the Land Information Warfare Activity (LIWA), Marine Forces-Computer Network Defense (MARFOR-CND), Navy Component Task Force-Computer Network Defense (NCTF-CND), Air Force Information Warfare Center (AFIWC) and the Defense Information Systems Agency's (DISA) DOD Computer Emergency Response Team (DOD CERT).

The JTF-CNO is located in Arlington, VA and maintains a 24-hours per day, seven days per week watch. It is collocated with the Defense Information Systems Agency (DISA) Global Network Operations and Security Center (GNOSC). The JTF monitors the status of DOD information networks and conducts operations across the defense information infrastructure.

The JTF-CNO leverages the existing intrusion detection capabilities of the unified commands, its components and DOD and non-DOD agencies to fulfill the Computer Network Defense mission. The JTF receives intrusion data from these sources and then fuses the information with intelligence and technical data into a big picture synopsis of the incident. After correlating the information, the JTF-CNO assesses the impact to the network operations and military operations, and then identifies a course of action that will restore the network, then coordinates the necessary actions with the appropriate DOD or non-DOD organizations. They then prepare a plan and with approval to execute that plan. The JTF directs actions through its four military service components and the DOD CERT.⁴⁶

The JTF-CNO deserves a permanent designation. Something named a Joint Task Force is temporary by nature. The JTF-CNO to date has proven itself to be a very capable organization and other government organizations with the same mission area should look to the JTF-CNO as a pathfinder organization.

The Department of Defense developed its Critical Infrastructure Protection Plan and the Joint Information Assurance Reserve Project (JIARP) and related Reserve component Information Operations (RC IO) initiatives to support this mission. Presidential Budget Directive 707 is one of two Presidential Budget Decision (PBD) supporting the October '00 DEPSECDEF-approved OSD (Reserve Affairs) sponsored Joint Reserve Component Virtual Operations Organization (JRVIO) initiative. The Joint Information Assurance Reserve Project (JIARP) is an important contribution to information operations. "My pet dream is to have a unit of Reserve hackers in Silicon Valley". A speaker at the US Army War College expressed in a nutshell the concept of Reserve participation in Information Operations.⁴⁷

Developing information-warfare capabilities in the reserve component offers a great way for the federal government to tap into civilian expertise in information warfare. Guardsmen and reservists have access to information technologies not found in most parts of the US government. The formation of reserve units specializing in information warfare would be cost effective, play to reservist's core competencies, and improve our defense against such attacks.

The related initiatives to leverage more effectively Reserve Component skills in the Information Operations/Information Assurance mission areas provide a sound DoD investment strategy, given the exodus from active duty of intelligence, IO, and information technology-skilled personnel. Many skills necessary for information operations are found in the civilian and reserve community and not on active duty.⁴⁸ The US government is hungry for IT professionals. They can not pay what the civilian sector can offer. They can offer scholarships for education in computer science in exchange for government service, but ultimately they lose the talent. The reserve involvement is an excellent way to keep that expertise at work for the nation.

FEDERAL AGENCIES RESPONSE

Congress mandated better security procedures, including a requirement that agencies give the Office of Management and Budget reports detailing assessments of computer security. The General Accounting Office and independent cyber security specialists assess the federal computer system is vulnerable to devastating attacks by terrorists, criminals and increasingly malicious hackers. The Administration created an Office of Cyberspace Security and announced in October 2001 it will spend \$10 million to counter cyber terrorism. The head of the

new office, Richard Clark, announced a plan to create a new secure Internet solely for government use.⁴⁹

In 2000, the CIA created the Information Operations Center and brought together their best and brightest to develop a strategy for dealing the cyber threat.⁵⁰

The FBI created the National Infrastructure Protection Center (NIPC) intended to direct efforts to protect both government and private sector computer networks from cyber attacks. PDD 63 required the FBI through the NIPC to serve as national infrastructure threat gathering, assessment, warning, vulnerability and law enforcement investigation and response entity. The NIPC is linked electronically as a national focal point. It has established its own relationships with the private sector and it is the principal means of coordinating US Government response, investigation of intrusions. It is located within the headquarters of the FBI in Washington DC.

The NIPC's mission is to detect, warn of, investigate and respond to cyber intrusions. It also coordinates the FBI's computer intrusion investigations. It shares, analyzes and disseminates information and provides training for cyber investigators. It has a 24 hour-7 day a week watch and warning capability. The NPIC gathers together experts from the FBI, other federal agencies, state and local government officials, and representatives from private industry to develop tools, techniques and strategies to respond to and investigative unlawful acts involving computer intrusions and unlawful acts that threaten or target the nation's critical infrastructure. The NIPC issues Cyber Notes, a biweekly newsletter that describes a summary of software vulnerabilities identified during the previous 2 weeks. They also provide alerts to viruses and intrusions.⁵¹

The NIPC is supposed to be a clearinghouse and share information. But there are problems with the organization. Their track record is not sterling. Cable News Network (CNN) broadcast a warning about the Love Bug virus before NIPC even had the information on their web site. NIPC changed their leadership and management team early in 2002. The change may help their responsiveness. But it will not overcome the private sector's reluctance to report their vulnerabilities. Their physical location is daunting to private business. Corporations are uncomfortable reporting their problems to an organization they think is associated with the FBI.

Corporations also are reluctant to report their intrusions to any government organization. The corporations fear the information will be available to the general public under the "Freedom of Information Act". Corporate council is afraid they might lose proprietary information if the public has access to their reports. Corporations might share their intrusions if they knew that information would not be available to the public. They would also share more if the center were relocated out of the Federal Bureau of Investigation.

THE CIVILIAN RESPONSE TO THE THREAT

The television advertisement by EDS picturing the little girl hacking in to an automobile factory and painting her name on the side of the car is very clever and speaks volumes about the security of civilian infrastructure. The Forrester Research Group in Cambridge MA published a study that said most businesses spend less on network security than they do on coffee.⁵² Security measures are time consuming and can slow down commerce. There is no way to go back to the old systems of 10 years ago. Basic infrastructures that make the economy work all depend on computer networking and are connected on the Internet. Computer controlled networks run all banking transactions, oil, gas and electric. Railroads are IT businesses. A railroad company knows where every one of their trains and boxcars are located, what they are loaded with and where they are going. If the IT systems went down, the trains would stop. Wal-Mart is what it is today because of networking their operations.

Power may be generated in one area but used in another. A hacker/terrorist could attack the grid and cause rolling black outs. If an electric grid goes down, it would take several days to bring back on-line.

The economy is built on information, technology information, and infrastructure. It has permeated into all aspects of the economy and the way business handles goods and services. Industry and the economy thrives on networking and because of it industry and the economy are at risk. Essential software and hardware were not designed with security in mind.

The Computer Crime Survey and the FBI performed a computer crime survey. They found in the year 2001:

- 85% of their respondents detected security breaches within past 12 months.
- 64% acknowledged financial losses due to computer breaches.
- 186 of 538 respondents revealed amount of losses amounting to \$377,828,700
- 2000 survey revealed \$265,589,940 in losses from 249 respondents

The types of losses reported were theft of proprietary information worth over one hundred and fifty million dollars. The businesses lost over ninety two million dollars in financial fraud. The Internet connection was cited by 70% of the respondents as the most frequent point of attack as opposed to 31% attacked through an internal system.⁵³

Forty percent of the attacks and abuses were from the outside. 38% of the company's detected denial of service attacks. Ninety four percent detected viruses and 91% detected employee abuse. Civilian companies are reluctant to report the intrusions to Law Enforcement. 36% of the survey respondents reported their intrusions. That is up from 25% reported in the 2000 survey.⁵⁴ The Civilian companies are unwilling to divulge their intrusions to the

government. The fact that NIPC resides in the FBI building makes this even worse. The NIPC should move to a neutral location if they want civilian industry participation.

The Riptech Study of January 2002 reported that in over 100,000 attempted cyber attacks, most succeeded due to software not being updated with available fixes or patches.

The very nature of the computer systems that companies spend so much trying to protect creates another set of problems. Although it has become very popular of late to blame Microsoft, in this instance there is an element of justification. The dominance of their software and operating systems only adds to the ease with which these may be exploited. This has been borne out by the most successful viruses of recent years, which have invariably manipulated the widespread reliance on Microsoft products.⁵⁵

The private sector is averse to the bad publicity that can be generated by disclosure of a successful attack on an IT system or website. Anything that draws attention to the vulnerabilities of businesses can have serious financial consequences. Many corporations trust no one. The building of trust between companies and law enforcement agencies is essential to protect the infrastructure. The creation of "flexible, evolutionary approaches that span both the public and private sectors" was called for in the Presidential Decision Directive 63 (PDD-63).⁵⁶

The NIPC has created INFRAGARD: Partnership for Protection. Members benefit with a forum to communicate. Infragard disseminates threat warnings and provides education and training on infrastructure protection. The members, both civilian and government can share information in a trusted environment.⁵⁷ The NIPC should be removed from the law enforcement environment and placed in a neutral location. Civilian companies would be more willing to share information if the NIPC was not located in the headquarters of the FBI.

Government and industry must work together to protect our national infrastructure security. Industry should upgrade their cyber security measures to guard against cyber attacks.

- Maintain heightened level of alert and logging levels in times of crisis
- Report suspicious activity to law enforcement
- Apply and follow best practices from computer and physical security
- Secure critical information assets against known exploits and vulnerabilities and back up vital data
- Use ingress and egress filtering to protect against Denial of Service attacks

The software companies can help protect their products by literally "standing down" writing new products until they can retool and focus on IT security. Vulnerabilities are posted every day and every week, but from the time the software companies post the patches and the private companies use the patches, the hackers or terrorists can invade. Standing down would break

the cycle and vulnerabilities would be eliminated. Each new software product should be tested for security before it hits the market.

Our critical information infrastructures and the government and business operations that depend on them are at risk. The government and the civilian sector share the responsibility to improve Internet security and coordinate effective national response to computer incidents and events. To be successful, there must be participation and cooperation among government agencies, law enforcement, commercial organizations, the research community and practitioners who have experience in responding to computer security incidents.

SUMMARY, CONCLUSION AND RECOMMENDATION

The economic prosperity that our nation enjoys today is largely founded in the Information Age and in our global leadership in information technology. Our continued leadership and prosperity in the global economy may well hinge on our national commitment to act as leaders in bringing integrity and responsibility to the global information environment we have helped to create. Information superiority in the Information Age is a clear national imperative. "Wars in the 21st century will increasingly require all elements of national power—not just the military. They will require that economic, diplomatic, financial, law enforcement and intelligence capabilities work together."⁵⁸

As this country has grown and prospered, the nation's leadership has responded to new issues with new government cabinet level departments. When the nation began to grow beyond the original colonies, a Department of Interior was created to deal with the expansion issues. When the farmer's needed a voice in government, the Department of Agriculture was created. The Departments of Commerce, Labor, Transportation, Health and Human Services, Energy, Education and the Veteran's Administration all were set up when the nation felt there was a need for a new cabinet level department.

Now more than ever, a new cabinet level department is necessary for a unified effort to fight cyber terrorism. This is the time to start a Department of Cyber Security. This department would house the NIPC, the JTF-CNO (hopefully newly named) and a civilian cyber organization representative. Liaisons from DoD, the intelligence agencies, DIA, CIA and NSA would be included to keep the flow of information moving. Representatives from law enforcement would also work to protect the infrastructure. The department would develop a national strategy on cyber security written with the civilian sector, universities and businesses. Who better to tell how to protect an electric grid than an electric company? Each department would man a cell to keep sharing information and passing along critical information. This department would create

standardized methods to protect the nation's infrastructure. With all of these organizations working together, all can stay ahead of trends, and share their talent and resources. This department should promote and sponsor education programs and scholarships for young and talented cyber wizards and put their education to work. It should promote higher education in computer science and specifically in IT security and leverage the knowledge gained at research institutions and the teaching universities. Once this knowledge is pooled, the experts can figure out the best ways to secure the infrastructure.

Communication with the private sector is crucial. The department should work to enhance communication, coordination and cooperation between the government and private companies. It could provide inducements and mandates to the private sector, asking for the assistance of the companies with the expertise. Consumers say they can't find a secure product, yet vendors say companies won't pay the extra dollar for the secure product. This department would be the enabler. The government would put the correct groups together and be a convening power, not a heavy-handed government. With the NIPC out of the law enforcement location, civilian companies would be more willing to work with the government to protect their infrastructure.

This Department of Cyber Security would be on equal footing with the other Cabinet level departments and have the resources to get the job done effectively. Policy without resources is just rhetoric. The department would have to be funded amply to stay technically advanced and leaning forward. This department would be a starting point to think this problem through systematically. It would raise the bar and limit the perpetrator's options and their chances for success. It could be the model for others in the globe to follow.

The US Government must keep terrorists off-balance, forcing them to worry about their own security and degrading their ability to plan and conduct operations. The complexity, intricacy and confluence of cyber threats necessitate a fundamental change in the way the government and the civilian sector do business. To keep pace with the cyber threat challenges the US should aggressively challenge analytical assumptions, avoid old ways and embrace alternate analysis and viewpoints. The US should constantly push the envelope beyond the traditional and exploit new systems and operations opportunities to anticipate and counter cyber threats.

WORD COUNT =7932

ENDNOTES

¹ Article 1.2 of the "Proposal for an International Convention on Cyber Crime and Terrorism" by the Center for International Security and Cooperation.

² Scott R. Sutherland, "Cyberterrorism", Briefing slides, US Army War College, Carlisle Barracks, PA, 8 February 2002.

³ August Gribbon, Washington Times 26Oct01

⁴ A National Security Strategy for a Global Age, The White House, December 2000

⁵ George F. Will "Now, Weapons of Mass Disruption?" Newsweek October 29, 2001

⁶ Walter Pincus, "Hacker Hits On Pentagon Computers Up 10% This Year" Washington Post 9 Dec 2000

⁷ Leah James and Jestyn Cooper, "Organized exploitation of the information super-highway", Jane's Intelligence Review. 1 July 2000.

⁸ The President's commission on critical infrastructure protection, report on critical foundations, protecting America's infrastructure (Oct 1997)

⁹ Threats to US National Security Hearing Before Senate Select Committee on Intelligence, 105th Congress (Jan 28, 1998) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation)

¹⁰ Statement by Director of Central Intelligence George J. Tenet before the Senate Select Committee on Intelligence on the "Worldwide Threat 2001: National Security in a Changing World." 7 Feb 2001

¹¹ Scott R. Sutherland, "Cyberterrorism", Briefing slides, US Army War College, Carlisle Barracks, PA, 8 February 2002

¹² Critical Infrastructure Protection Significant challenges in Safeguarding Government and Privately controlled systems for computer-based attacks. GAO -01-1168T September 9, 2001.

¹³ Scott R. Sutherland, "Cyberterrorism", Briefing slides, US Army War College, Carlisle Barracks, PA, 8 February 2002

¹⁴ Marianne Sonnenberg, Fox television news interview 19 Jan 02

¹⁵ Patterns of Global Terrorism 2000 United States Department of State April 2001
Department of State Publication Wash DC.

¹⁶ Dorothy E. Denning and William E. Baugh Jr. "Encryption and evolving technologies Tools of organized Crime and Terrorism" WGOC Monograph Series (1997)

¹⁷ Chris Hastings, David Bamber "2 white Britons probed for aiding bin Laden". London Sunday Telegraph. 21 Oct 2001.

- ¹⁸ Alan Cullison and Andrew Higgins "Forgotten Computer Reveals Thinking Behind Four Years of Al Qaeda Doings" Wall Street Journal 31 December 2001
- ¹⁹ Nancy Ing, Pete Williams and Robert Windrem msnbc.com/newscast 21 Jan 2002
- ²⁰ Michael James "Hate Online" Baltimore Sun 26 October 1998
- ²¹ "Ashcroft Warns About Cyberattacks" Dallas Morning News 13 Feb 2002
- ²² "Cyber Terrorism" Senate Judiciary Subcommittee CSPAN Broadcast 13 Feb 2002
- ²³ USSPACECOM, "Joint Task Force Computer Network Operations" briefing slides with scripted commentary. JTF-CNO, Washington DC. October 2001.
- ²⁴ USSPACECOM, "Joint Task Force Computer Network Operations" briefing slides with scripted commentary. JTF-CNO, Washington D.C. October 2001.
- ²⁵ "China warns of coming hack attack" Agence France-Press Washington Times 22 Apr 01
- ²⁶ Oversight of the Department of Justice Hearing Before the Senate Judiciary Committee, 105th Congress (July 15, 1998)
- ²⁷ Bill Gertz, "Beijing's strategy targets Taiwan's Information networks", The Washington Times. 22 July 2001, A3.
- ²⁸ Dorothy E. Denning, "Web Hacks and Computer Break-Ins", OSAC Cyber Library. 18 January 2000
- ²⁹ "The Internet is Under Siege" The Record, Northern New Jersey 13 Feb 2000
- ³⁰ President William J. Clinton, Presidential Decision Directive (PDD-63) Washington D. C.: Government Printing Office, 1998
- ³¹ Winn Schwartau, Pearl Harbor Dot Com. Interpact Press, Inc. Seminole, FL, 2002
- ³² Carl von Clausewitz, On War New York, New York, Penguin, 1968
- ³³ Bob Deans Atlanta Journal Constitution August 2 1998
- ³⁴ Michael Bilbert, "Builders of the New Army" Tacoma News Tribune. 11 Jun 2001
- ³⁵ Ann Roosevelt, "Army Tests First Digital Brigades in Combat Exercise" Defense Week 9 April 2001, pg 1
- ³⁶ James W. Crawley, "Marine, Navy Units to Work out the bugs on High Tech Battlefield" San Diego Union-Tribune. 19 June 2001

³⁷ Greg Jaffe, "In the New Military, Technology May Alter Chain of Command" Wall Street Journal. 30 Mar 2001

³⁸ Neil Munro "The Pentagon's new Nightmare: an electronic pearl harbor. Washington Post 16 July 1995

³⁹ General Ralph E. Eberhart, commander in Chief, North American Aerospace Defense Command and US Space Command before the US Senate Armed Services Committee Strategic Subcommittee Wash DC 8 Mar 2000

⁴⁰ Secretary Rumsfeld address to the National Defense University, January 31, 2002.

⁴¹ President William J. Clinton, Presidential Decision Directive (PDD-63) Washington D. C.: Government Printing Office, 1998.

⁴² President William J. Clinton, Presidential Decision Directive (PDD-63) Washington D. C.: Government Printing Office, 1998

⁴³ President William J. Clinton, Presidential Decision Directive (PDD-63) Washington D. C.: Government Printing Office, 1998

⁴⁴ USSPACECOM, "Joint Task Force Computer Network Operations" briefing slides with scripted commentary. JTF-CNO, Washington D.C. October 2001.

⁴⁵ Frank Wolfe "DoD Could Prevent Most Intrusions of Unclassified Networks" Defense Daily 18 May 2001.

⁴⁶ "Many DoD Web Sites Remain blocked in Classified Cyber Security Case" Inside the Pentagon 23 Aug 2001

⁴⁷ The ideas in this paragraph are based on remarks made by a speaker participating in the Commandant's Lecture Series.

⁴⁸ Colonel Brian Williams, USAF. USAF/XOI-RE "PBD 707" Electronic mail message to MG Bruce Wright, USAF, AIA/CC, 23 Sep 01

⁴⁹ August Gribbin, "Secure new Web urged for Government only" Washington Times 26 October 2001, Pg A22

⁵⁰ Statement by Director of Central Intelligence George J. Tenet before the Senate Select Committee on Intelligence on the "Worldwide Threat 2001: National Security in a Changing World" 7 Feb 01.

⁵¹ David A. Vise, "FBI Takes Aim at Cyber Crime" Washington Post 6 Jan 2001

⁵² "Cyberterrorism", Judiciary Committee, CSPAN broadcast 13 Feb 2002

⁵³ Tim Rosenberg, "CyberTerrorim: Dangers and Possibilities" briefing slides, US Army War College, Carlisle Barracks, PA, 25 January 2002.

⁵⁴ Tim Rosenberg, "CyberTerrorism: Dangers and Possibilities" briefing slides, US Army War College, Carlisle Barracks, PA 25 January 2002

⁵⁵ Leah James and Jestyn Cooper "Organized exploitation of the information super-highway" Jane's Intelligence Review 1 July 2000.

⁵⁶ President William J. Clinton, Presidential Decision Directive (PDD-63) Washington D. C.: Government Printing Office, 1998.

⁵⁷ David A. Vise "FBI Takes Aim at Cyber-Crime" Washington Post 6 Jan 2001.

⁵⁸ Secretary of Defense Rumsfeld address to the National Defense University, January 31, 2002.

BIBLIOGRAPHY

- Allman, William F., "Computer hacking goes on trial." US News & World Report, 22 Jan 1990, 25
- "Ashcroft Warns About Cyberattacks," Dallas Morning News. 13 February 2002.,
- Bamber, David and Chris Hastings, "2 White Britons probed for aiding bin Laden." London Sunday Telegraph. 21 Oct 2001
- "China warns of coming hack attacks," Washington Times. 22 Apr 2001 p A1.
- Clinton, William J., President. Presidential Decision Directive (PDD-63). Washington, D.C. GPO, 1998.
- Crime, Terror, & War: National Security & Public Safety in the Information Age , 105th Congress. United States Senate Committee on the Judiciary Subcommittee on Technology, Terrorism, and Government Information. November 1998.
- "Computer Virus Spawns 2nd Version" The Arizona Republic. 21 Jul 2001.
- Cooper, Jestyn and Leah James, "Organized exploitation of the information super-highway," Jane's Intelligence Review. 1 July 2000
- Cullison, Alan and Andrew Higgins, "Forgotten Computer Reveals Thinking Behind Four Years of Al Qaeda Doings", Wall Street Journal. 31 December 2001. pg 1.
- Danzig, Richard, "The Next Superweapon: Panic" The New York Times. 15 November 1998
- Denning, Dorothy, "Web Hacks and Computer Break-Ins", OSAC Cyber Library. 18 January 2000. Available from the Overseas Security Advisory Council, US State Department.
- Eberhart, Ralph E.General, Statement before the US Senate Armed Services Committee Strategic Subcommittee. Washington D.C., 8 Mar 2000.
- Garamone, Jim, "Protecting Critical Military Infrastructures", American Forces Press Service. 7 Dec 2001.
- Gertz, Bill, "Beijing's strategy targets Taiwan's information networks," The Washington Times. 22 July 2001, A3.
- Gilbert, Michael, "Builders of The New Army," Tacoma News Tribune. 11 June 2001.
- Guart, Al, "German Programmer Unleashed Cyberbug." New York Post, 13 Feb 2000, 4
- Gershwin, Lawrence K., "Cyber Threat Trends and US Network Security", Statement for the Record for the Joint Economic Committee., 21 June 2001.
- Grange, David L. "Asymmetric Warfare: Old Method, New Concern." National Strategy Forum Review 10, no. 2 (winter 2000) : 6-11.

- Gannon, John C., National Security in the Next Generation, Address at the Academy of Senior Professionals at Eckerd College, St. Petersburg, Florida. 27 Mar 2001.
- "Hackers enlisted soldiers attack programs were planted," The Cincinnati Post. 14 Feb 2000
19A
- Ing, Nancy, et al., "E-mail ties Richard Reid to Pakistan" MSNBC.COM. 19 January 2002.
Available at www.msnbc.com/news accessed 21 January 2002.
- Jaffe, Greg, "In the New Military, Technology May Alter Chain of Command," Wall Street Journal. 30 Mar 2001, A1.
- James, Michael. "Hate Online." Baltimore Sun, 26 Oct 1998
- Kelley, Jack, "Terror Groups Hide Behind Web Encryption", USA TODAY. 6 Feb 2001 1A
- Kitfield, James, "Anti-Terror Alliance," Government Executive, February 2001
- Lehman, John F. and Harvey Sicherman, AMERICA'S MILITARY PROBLEMS AND HOW TO FIX THEM. Foreign Policy Research Institute. Volume 9, Number 3 February 2001.
- Many DOD Web Site Remain Blocked In Classified Cyber-Security Case" Inside the Pentagon
23 Aug 2001, pg 1.
- McLaughlin, John E., "The Changing Nature of CIA Analysis in the Post-Soviet World". Remarks at the Conference on CIA's Analysis of the Soviet Union, 1947-1991, Princeton University, NJ, 9 Mar 2001.
- "Pakistani Charged in Hacking." Washington Post. 23 Oct 2001
- Pincus, Walter, "Hacker Hits On Pentagon Computers Up 10% This Year," Washington Post 9 Dec 2000, 8.
- Rosenberg, Tim, "CyberTerrorism: Dangers and Possibilities" briefing slides, US Army War College, Carlisle Barracks, PA, 25 January 2002.
- Sutherland, Scott R., "Cyberterrorism", Briefing slides, US Army War College, Carlisle Barracks, PA, 8 February 2002.
- "Schwartau, Winn, pearl harbor dot com Seminole, FL: Interpact Press, 2002
- Settle, Jim, "Terrorism on the Net," USA TODAY, 5 June 1996, 2A
- United States Department of State, Patterns of Global Terrorism. Department of State Publication, Washington D.C. April 2001.
- USSPACECOM, "Joint Task Force Computer Network Operations" briefing slides with scripted commentary. JTF-CNO, Washington D.C. October 2001.
- "US is vulnerable on Internet", New York Times. 21 Oct 1997.
- Vise, David A., "FBI Takes Aim at Cyber-Crime," Washington Post. 6 Jan 2001, A2

- Waller, J. Michael, "Asymmetrical Warfare". February 2002: available from.
<http://www.ranger.org/usara/s2/editorials/asymmetrical_warfare.htm> Accessed 16 Feb 2002.
- Will, George F., "Now, Weapons of Mass Disruption?", Newsweek. 29 Oct 2001 pg 76.
- Wilson, Fred, "Net faces questions of security on line" The Boston Globe. 24 February 1996.p1.
- Wren, Christopher, "Computer Expert Testifies in Terror-Plot Trial" New York Times. 24 July 1996.
- Wren, Christopher, "Terror Case Hinges on Laptop Computer" New York Times. 18 Jul 1996.
- Wolfe, Frank, "DoD Could Prevent Most Intrusions of Unclassified Networks", Defense Daily. 18 May 2001, pg 6.
- Zuckerman, M. J., "Feds ready anti-terror cyberteam," USA TODAY, 5 June 1996