STRATEGY RESEARCH PROJECT

DEFENSIVE INFORMATION OPERATIONS - AN INTERAGENCY PROCESS

BY

MR. JAMES T. SCHUTZE
Department of the Army

USAWC CLASS OF 2001

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

USAWC STRATEGY RESEARCH PROJECT

DEFENSIVE INFORMATION OPERATIONS – AN INTERAGENCY PROCESS

by

MR. JAMES T. SCHUTZE
Department of the Army
HQ, U.S. Army Signal Command

Colonel Thomas McShane, U.S. Army
Project Advisor

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

ABSTRACT

AUTHOR: James T. Schutze

TITLE: Defensive Information Operations – An Interagency Process

FORMAT: Strategy Research Project

DATE: 2 March 2001 PAGES: 32 CLASSIFICATION: Unclassified

The United States military has long held the mission of protecting this country against foreign attack. One of the biggest threats facing the United States in the 21st century, however, is of a far different nature than that of a conventional armed attack. A cyber attack zeroing in on critical information or on the information systems which support critical national infrastructures could be launched from any corner of the globe, by a variety of potential state and non-state actors, and could be directed against military or civilian targets. Due to the quantity, complexity, and diverse ownership of this country's information systems and critical infrastructures, no single governmental or private agency can single-handedly provide an adequate defense. As a result, the nation's information and infrastructure protection effort requires governmental interagency and private sector cooperation. The Department of Defense, as a key player in the interagency effort, must rapidly respond to information attacks in coordination with a host of government departments and agencies, including the Departments of Commerce, Justice and State. It must be prepared to defend its own information and infrastructure; to support other government agencies in their defense, enforcement, and consequence management functions; and to counterattack with information operations weapons.

This paper discusses the nature and level of the cyber threat and DoD's roles in countering it in an interagency environment. The paper also looks at the legal issues DoD must consider in planning and executing its information defense mission. It examines the current arrangement for protection of the nation's infrastructure and suggests there are organizational issues impeding the speed and effectiveness of the country's defense that must be addressed.

TABLE OF CONTENTS

DEFENSIVE INFORMATION OPERATIONS — AN INTERAGENCY PROCESS

One of the biggest threats facing the United States in the 21st century is that of a cyber attack. The attack could be launched against military or civilian targets, and could zero in on critical information or the information systems which support critical infrastructures. Due to the quantity, complexity, and the diverse ownership of the information systems and critical infrastructures in this country, no single governmental or private agency can single-handedly provide an adequate defense. As a result, the nation's information assurance (IA) effort requires interagency and private sector cooperation.

The United States has begun to take this threat seriously and to organize for the protection of its national information and infrastructure. However, the organizations set up to perform the mission, including the military, are numerous; leadership and direction is fragmented; and the structure is too cumbersome to respond quickly to an attack.

A streamlined interagency protection organization, coupled with a national awareness and education program, is required to deal with the information threat facing the nation.

WHAT IS THE INFORMATION THREAT AND WHY SHOULD WE CARE ABOUT IT?

The nation's military and civilian information and information systems are at risk of being corrupted, disrupted, compromised, or destroyed. National security secrets and corporation proprietary information could be stolen, command and control of the nation's military could be disrupted, and the nation's critical infrastructure could be disabled by a successful cyber attack.

The consequences of such attacks would be catastrophic. Swiss research has determined that a complete computer breakdown would kill a nation's banking activities after two days, its commerce in two and a half days, and its factories in five days.[1] And attacks are currently occurring at some level every day. The U.S. Computer Emergency Response Team (CERT), only one of over 20 incident reporting centers, states that it receives 45-60 incident reports each day from the private sector. In 1999 the annual number of incidents exceeded 9,000.[2] Those numbers are likely just the tip of the iceberg. The Defense Information Systems Agency (DISA) found that when it evaluated, i.e., attacked, unclassified defense systems, only one in twenty victims knew they were attacked, and of those, only one in twenty reported it, meaning that only somewhere around one in 400 attacks were actually reported.[3]

A large number of attacks are directed at the Department of Defense (DoD). DISA estimated that as many as 250,000 attacks may have occurred in 1995.[4] In 1998, three teenagers were able to break into DoD systems carrying information on cargo shipments, payroll accounts,

health records and a host of other administrative, logistics, and personnel matters. Pentagon officials were worried that the hackers could disrupt military operations at a time when the U.S. was building up its force for operations in the Persian Gulf.[5]

Adding to the concern, at least ten foreign countries are developing information warfare and electronic intrusion techniques.[6]

NATURE OF INFORMATION OPERATIONS

The definition of information operations (IO) used by the American military is found in the Chairman of the Joint Chiefs of Staff's Joint Publication 3-13, *Joint Doctrine for Information Operations*. This publication states that "information operations involve actions taken to affect adversary information and information systems while defending one's own information and information systems." A subset of information operations, *defensive* information operations "integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and information systems." [7]

Offensive information operations can be a lucrative weapon. It has several advantages: it can minimize collateral physical damage; it can minimize friendly losses of personnel and equipment; it can help avoid escalation; and it's relatively cheap.[8]

Yet the focus of information operations for the United States is likely to be on defensive operations. That's because the U.S., with its growing dependence on information systems and its dominance in the world's technology market, is more vulnerable to an IO attack than are other nations. North America has 44 percent of the world's technology market;[9] while on the other hand, only 20 percent of the world may be significantly influenced by the information revolution.[10] In fact, one of the reasons the U.S. didn't use much of its offensive information operations capabilities in Serbia in the spring of 1999, according to the Washington Post, was due to the "rudimentary or decentralized nature of some Yugoslav systems, which officials said did not lend themselves to computer assault." [11]

Defensive information operations are fought on several fronts, reflecting the wide range of operations included in the information domain. Joint Pub 3-13 highlights the elements of defensive information operations as being information assurance, operations security (OPSEC), physical security, counterdeception, counterpropaganda, counterintelligence, electronic warfare (EW), and special information operations (SIO).[12] This paper will focus on the cyber aspects of information operations, with the primary attention on information assurance. Information assurance is defined as operations "that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and

nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." [13]

WHAT'S AT RISK?

The impact of cyber operations goes beyond the information systems attacked. Cyber operations also reach the infrastructure dependent on information systems, such as military weapon systems and commercial power and water systems.

Specifically, military targets of cyber operations may include DoD sensitive, classified, or administrative **information** for purposes of stealing technology, of learning strategic, operational, or tactical plans, or of influencing perception and will; **computers** in order to disrupt operations or corrupt information important to operations; **weapons systems** to disorient or disable those with embedded information systems or dependent on information for correct operations (e.g., targeting systems or precision guided munitions); and **communications networks** in order to deny or disrupt command and control of government and military forces, or to deny or disrupt administrative and logistical support to the military. In short, a military as highly dependent on information as is this country's is extremely vulnerable to attacks on that information or on its processing and delivery.

Just as vulnerable is the nation's commercial and governmental infrastructure. Disruptions in our telecommunications networks, energy and water infrastructures, transportation systems, banking and financial computers and networks, emergency services and public media would be crippling. Business transactions would halt, people and goods could not be transported, the economy would stumble, and the media could lose credibility or the ability to get its message across. The effects on the public would be devastating. Essential and emergency services would be at risk, and the confidence and will of the American public could be quickly damaged if but one of the above information-dependent segments was successfully attacked.

WHY WE'RE AT RISK

We have become a nation dependent on information and information systems across the range of civilian and military processes. Our formerly disparate infrastructures have not only become increasingly automated, but increasingly interlinked as well.[14] A flare in one part of the nerve system can cause muscle movements throughout the body.

And we're not just marginally interconnected. The U.S. is the world's most advanced and most dependent user of information technology. We have one-half of the world's computer

capacity and more than 60% of the world's Internet assets.[15] That makes us economically powerful, but it also makes us the largest and most vulnerable target around.

One of the partners in this U.S. interconnectivity is the Department of Defense. DoD is vastly dependent on the U.S. civilian communications infrastructure. According to Dr. Arquilla of the Naval Postgraduate School and David Ronfeldt of RAND Corporation, over one-half of DoD's communications traffic runs over civilian communications systems.[16] Douglas Dearth and Charles Williamson claim that more than 90 percent of the Defense Information Infrastructure (telephone, Internet, video teleconference, etc.) rides on the U.S. National Information Infrastructure.[17] It should become obvious by considering this interconnectivity that one agency, neither defense nor non-defense, can adequately protect this tightly raveled network.

WHO PUTS US AT RISK?

Computer network attacks are cheaper and easier to mount than traditional military attacks. Thomas Friedman argues in his book *The Lexus and the Olive Tree,* that the Information Revolution "lowered the barriers to entry into almost any business" because of the low cost of sitting in your basement with "a single personal computer, credit card, phone line, modem, color printer, Internet link, and Web site" and becoming a global competitor.[18] The same is true for becoming a cyber attacker. Expressed in more military terms, cyber attacks are "relatively cheap and require much less in the way of forward basing, deployment, and logistical support than do traditional weapons and their delivery platforms."[19]

With all this cheap power at their disposal, potential cyber attackers are now a large and varied group. The question of who puts us at risk may more easily be restated as "who doesn't?" A partial list of potential threats includes such actors as other nation's militaries and foreign intelligence organizations, terrorists groups, ethnic and religious sects, criminals and their cartels, corporations intent on stealing secrets, disgruntled employees, and recreational hackers. Not to be forgotten are other threats, such as accidents and natural disasters. Again, the playbill of actors is so large, it is inconceivable that information operations defense is anything but a governmental interagency and private partnership effort.

TYPES OF INFORMATION THREATS

The kinds of threats that defensive information operations must protect against include:

- Destruction of information — for example, the erasure of a database important to decision making or operations. This could include a company's database of customers or the plans of a military operation.

- Corruption of information — for example, information that has been altered to implant false data that results in bad decisions or prevents smooth operations.
- Unauthorized information — this could include release of sensitive economic or political information, or could be false information misattributed to an authorized person.
- Misinformation or propaganda — release of false information, primarily to the public media, with the intent of influencing national opinion or will.
- Lack of communication or denial of service — disrupting or destroying the communications system itself to prevent information flow.
- Espionage — collecting unauthorized information.
- Web page misinformation or defacement — similar to misinformation or propaganda, but using the Internet as the media to destroy credibility, to discredit, or to change the message intended by the owner of the Web page.
- Auto-mechanical failure — using cyber attacks to cripple the operation of machinery or networks critical to operations. This could include shutting down a power grid or disabling warfare equipment that is dependent on automation or telecommunications systems to operate properly.

HOW WE CAN PROTECT AGAINST INFORMATION ATTACKS

According to the Joint Chiefs of Staff, there are four interrelated processes that support defensive information operations: information environment protection, attack detection, capability restoration, and attack response.[20] All four are important in both the public and private sectors. Interagency responsibilities vary across the four processes. For the moment, let's concentrate on what the Department of Defense can do to protect itself against information operations attack.

Information assurance begins with the information users, folks who can limit unauthorized access to DoD information by understanding system vulnerability, i.e., becoming educated, and by practicing information security through password controls and physical protection of DoD information assets. The second line of defense is the system administrators who manage an organization's overall information operations on a day-to-day basis. Additional defenders include information system providers who provide the automation and communication assets and services, and information systems developers who design and program the systems and applications. At higher levels, key organizations include the military services' information warfare centers that monitor information assurance, the law enforcement community (both

military and civil) who respond to information attacks, and the intelligence shops that provide warning and advice.[21]

Other considerations for the military in protecting its information and systems are to rapidly isolate DoD systems during attacks to prevent viruses or other agents from infecting DoD computer and communication systems; increase network diversity to provide robustness and expand the center of gravity; and share information with the private sector to better spot patterns of attack and to assist the NII in protecting itself.[22]

WHAT THE NATION IS DOING TO COMBAT THE RISK

The nation's overall response is currently centered around Presidential Decision Directive (PDD) 63: *Policy on Critical Infrastructure Protection.* This PDD, issued in May 1998, raised the country's awareness of the gravity of the information operations threat and focused the country's efforts on countering the peril. It created a host of government and private organizations to develop a body of policy and to manage and operate key information assurance centers. This PDD set the tone for interagency cooperation in defensive information operations.

The PDD sought to increase public consciousness by pointing out the increasing reliance upon critical infrastructures and cyber-based information systems, identifying what the nation considers to be its critical infrastructure,[23] indicating how infrastructures have become increasingly automated and interlinked, clarifying the mutual dependence between a strong military and a strong economy, and concluding that the "U.S. must take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, especially our cyber-based systems."[24] PDD 63 established a host of government and private organizations to manage the infrastructure protection mission, key among these being:

- Lead Agencies for Sector Liaison. Individual U.S. government departments or agencies that serve as the Lead Agencies for liaison with each infrastructure sector that could be a target for significant cyber or physical attacks. A representative at the rank of Assistant Secretary or higher serves as the Sector Liaison Official responsible for cooperating with private sector representatives (Sector Coordinators) in addressing problems related to critical infrastructure protection, and in recommending components of the National Infrastructure Assurance Plan. Lead agencies and sector coordinators also develop and implement a vulnerability awareness and education program for their sectors. The lead agencies are

Department of Commerce, Department of Treasury, Environmental Protection Agency, Department of Transportation, Department of Justice, the Federal Emergency Management Agency, Department of Health and Human Services, and the Department of Energy.

- Lead agencies for Special Functions. U.S. government agencies that have been assigned leads for functions reserved for the federal government, namely national defense, intelligence, foreign affairs, and federal law enforcement. Lead agencies are DoD, the CIA, and the Departments of State and Justice. The lead agency coordinates all the activities of the U.S. government in their area. An individual at the rank of Assistant Secretary or higher serves as the Functional Coordinator.
- Critical Infrastructure Coordination Group. Sector Liaison Officials and Functional Coordinators, as well as senior representatives from other concerned departments and agencies, including the National Economic Council, who meet to coordinate the implementation of PDD 63. The group is chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, who reports to the President through the two Assistants to the President for National Security Affairs and for Economic Affairs.
- National Infrastructure Assurance Council. This council is comprised of officials from major infrastructure providers and state and local governments. It meets periodically to strengthen the partnership of the public and private sectors in protecting critical infrastructures. Senior federal government officials participate in the meetings as appropriate.
- Chief Infrastructure Assurance Officer. Appointed by each federal department and agency, the CIAO is responsible for the protection off all aspects of the department's critical infrastructure, less that of information assurance. They perform vulnerability assessments on their departments' computer and physical systems. The information assurance function is assigned to the Chief Information Officer (CIO) of the department or agency. The CIO may be dual hatted as the CIAO if the department deems it appropriate.
- Information Sharing and Analysis Center. A private sector organization to serve as the mechanism for gathering, analyzing, sanitizing and disseminating private sector information to both industry and the NIPC (see paragraph below).
- National Infrastructure Protection Center (NIPC). Located at the Federal Bureau of Investigation, this center serves as the national critical infrastructure threat

assessment, warning, vulnerability, and law enforcement investigation and response entity. It fuses representatives from the FBI, DoD, U.S. Secret Service, the Intelligence community, the departments of Energy and Transportation, and the private sector in a mission to foster information sharing among agencies and the private sector. It also provides the principal means of facilitating and coordinating the federal government's response to an incident, of mitigating attacks, of investigating threats and of monitoring reconstitution efforts.[25]

The Department of Defense figures prominently in PDD 63, being both part of the interagency team formed for information defense, and having specifically assigned roles. As any other federal department or agency, DoD is responsible for protecting its own critical infrastructure, especially its cyber-based systems. Furthermore, it retains its role as the Executive Agent for the National Communications System and supports the President's National Security Telecommunications Advisory Committee. It functions, logically, as the Lead Agency for national defense. At the President's decision, depending on the nature and level of a foreign threat or attack, the National Infrastructure Protection Center may be placed in a direct support role to DoD or the national intelligence community. And finally, DoD and the Department of Commerce work together, in coordination with the private sector, to offer their expertise to private owners and operators of critical infrastructure to develop security-related best practice standards. DoD, then, is very much a team player in the nation's approach to protection of its critical infrastructure.

ANALYSIS OF CURRENT SYSTEM

Now that a structure is emerging to handle the defense against information attacks, we may believe we have reached the end state, or at least can see it over the horizon. Unfortunately, we are not quite that far along. There are a number of problems which critics have surfaced and which need to be addressed to provide a better level of protection than we've seen to date. One expert has summed up the problems succinctly by declaring that "the challenge in the years ahead of us is organizational, not technological."[26]

That's understandable when we consider the number of agencies and agents involved in the federal government's information protection effort. A *Washington Post* article on counterterrorism reveals there are 40 departments and agencies responsible for responding to terrorist attacks, and quotes the General Accounting Office as believing that counterterrorist programs "remain fragmented because key interagency management functions are conducted by different departments and agencies."[27] The same is true for the overall infrastructure

protection program. The GAO concludes in a report on critical infrastructure protection that "trust needs to be established among a broad range of stakeholders, questions on the mechanics of information sharing and coordination need to be resolved, roles and responsibilities need to be clarified, and technical expertise needs to be developed."[28]

No one disputes that a networked approach is required. GAO wisely points out that "it is not possible to build an overall, comprehensive picture of activity on the global information infrastructure. Networks themselves are too big, they are growing too quickly, and they are continually being reconfigured and reengineered. As a result, it is essential that strong partnerships be developed between a wide range of stakeholders in order to ensure that the right data are at the right place at the right time."[29]

The challenge, however, is to attain "unity of command," if we may borrow the expression from the principles of war, among this army of governmental and private agencies. The slow and ineffective response to the ILOVEYOU virus in May of 2000—which affected governments, corporations, media outlets, and other institutions, forcing many of them to take their networks off-line for several hours—"highlighted the need for greater information sharing and coordination."[30]

A second impediment to rapid response to information threats is the compartmentalization of authority among several government agencies. There is nothing wrong in the division of authority, as it limits federal power in terms of privacy issues and in the use of national intelligence assets or the military against American citizens and companies. It also increases efficiency by allowing individual agencies to concentrate on specific areas within the overall information protection battle. However, the compartmentalized approach also leads to lost efficiency as players try to determine who does what in the general scheme of things, and only constant exercise of the system through mock attack responses can make the cumbersome system work well.

WHO IS RESPONSIBLE FOR THE NATION'S OVERALL INFORMATION DEFENSE?

Since the federal government has no ownership of the private infrastructure, limited jurisdiction, and fiscally constrained intelligence capabilities, private organizations are largely responsible for their own defense.[31] The organizations established by PDD 63 enumerated above are responsible for assisting and coordinating their efforts.

Individual federal government departments and agencies, through their CIO and Chief Infrastructure Assurance Officer, are responsible for the protection of their department's information and critical infrastructure. The Office of Management and Budget is responsible for

overseeing and coordinating federal agency security. The National Institute of Standards and Technology (NIST), with assistance from the National Security Agency (NSA), is responsible for establishing related standards. And the Critical Infrastructure Coordination Group coordinates the government's and private sector's information protection efforts.

The Federal Bureau of Investigation, which also houses the NIPC, is responsible for law enforcement. Through their primary role in the NIPC they are the nation's first real line of defense. To assist in their criminal investigation efforts they recently set up the first regional forensics laboratory in San Diego, capable of finding evidence seized on computers. The laboratory will be an interagency effort, drawing expertise from the University of California San Diego and the U.S. Navy's Space and Naval Warfare Systems Command.

The role of law enforcement looms large in combating information attacks. According to an article in the Washington Post, "Instead of turning cyber assaults into another arms control issue, the administration prefers to treat them internationally as essentially a law enforcement concern. U.S. officials have supported several efforts through the United Nations and other groups to facilitate international cooperation in tracking computer criminals and terrorists."[32] This emphasis on treating international attacks initially and primarily as criminal matters also involves the Department of State as the agent to work with foreign governments to obtain their support in criminal prosecutions.

The Federal Emergency Management Agency is responsible for consequence management after an attack. If the attack affected an area's energy supply, for example, FEMA would be responsible for coordinating the national efforts to ensure emergency medical support and feeding and housing those affected by the loss of power.

The intelligence community is responsible for supporting the nation's information defense through intelligence collection. As they have also generally conducted covert operations in peacetime that do not consist of traditional military activities, it remains to be seen what their exact role will be in the division of labor in both defensive and offensive information operations.[33]

THE DEPARTMENT OF DEFENSE'S ROLE

The Department of Defense's responsibility is varied. Probably its most significant role would come in spearheading a retaliation if the nation were assaulted with a computer attack by a foreign government or a major terrorist organization supported by one. The military response could use conventional weapons or could use computer network attack. The Department of Defense, recognizing the importance of computer attacks in the Information Age, has assigned

the management of it to the US Space Command, a functional Commander in Chief (CINC) located in Colorado Springs, Colorado. In the context of information defense operations, then, the DoD's major roles would be deterrence, and failing that, retaliation on behalf of the nation.

The DoD can also provide support to FEMA in consequence management if requested. Its expertise in communications and computers can be enlisted by other federal agencies, as the FBI has done in setting up its computer forensics laboratory. However, the Posse Comitatus Act currently prevents the DoD from being the lead agent in domestic acts of computer attack which are perceived to be law enforcement issues.

HOW REAL IS THE THREAT?

The information warfare literature reveals there is a considerable range of opinion regarding the imminence and the severity of the information threat. Since our sense of urgency in improving the response to the information threat will undoubtedly be driven by the perceived level of danger, the reality of the threat is a major issue.

SOME ANALYSTS ARGUE THE THREAT IS OVER-STATED

Several analysts downplay our own vulnerability and the ability of potential hostile actors. One recurring theme is that if the threat is so real, how come we haven't yet seen a severe attack? Another argument is that, yes, there are threats out there, but they are more nuisance than substance, and that an electronic Pearl Harbor is not likely to happen any time soon. Sound bites from the naysayers at a December 1999 "Information Revolution and National Security" conference cosponsored by the U.S. Army War College Strategic Studies Institute and the University of Pittsburgh Center for International Security Studies include:

> "The technological threats...are not yet as significant as some of the dominant policy debates suggest. We have seen very little evidence of cyber-terror attacks...Most hackers are juveniles who thus far have done little damage against relatively unimportant targets."[34]
>
> "I wonder why, if asymmetries are such a threat, we have not seen more cyber-terrorism happening. We have not suffered much yet from digital disruption. We have been saying this is a problem, but nobody has used it to come after us."[35]
>
> "I would question the traditional wisdom on whether terrorists have the tools, expertise, and access needed to conduct these attacks. Web tools are like hand grenades rather than bullets—they cause problems in networks but cannot be

targeted that well. They are not atomic bombs, either—they are not that powerful."[36]

"Similar to the way the media has gone overboard the past couple of years regarding the prospect of an attack against the United States with biological weapons, the imminence of information warfare attacks has been, in the words of Mark Twain, greatly exaggerated."[37]

"The empirical evidence that exists shows only that computer viruses never constitute much more than 'annoyances' in networked computing."[38]

"Today the notion of using bits and bytes to bring whole systems down is very much exaggerated."[39]

MANY ANALYSTS BELIEVE THE RISK IS HIGH

Nevertheless, the preponderance of analysts believes we are in real danger. A spokesman for U.S. Space Command told a reporter that "we have evidence that a large number of countries around the world are developing the doctrine, strategies and tools to conduct information attacks on military-related computers."[40] One of our major potential adversaries, the Chinese People's Liberation Army, has established a university to train personnel in Information Warfare (IW) theory and technologies and is sharpening its focus on IW.[41]

The military relies on sophisticated computer-assisted weaponry and is increasingly orienting itself on a rapid global force-projection strategy. Therefore, the ability to provide timely and accurate information is vital to all aspects of combat operation.[42] That makes information a center of gravity, and the evidence shows that it is at risk. In a military exercise called Eligible Receiver in June of 1997, analysts from the National Security Agency used off-the-shelf computers and widely available hacker programs to demonstrate that they could disrupt computer operations at major military commands and interrupt electrical power and emergency phone service in several U.S. cities.[43] Eight months later three teenagers gained access to DoD computer files carrying sensitive information on cargo shipments, payroll accounts, health records and other administrative, logistical, and personnel material. It took DoD and law enforcement officials almost a month to track down the offenders in a search operation code named Solar Sunrise.[44]

Other evidence lends support to the belief that the nation is in danger. Computer virus attack damages in 1999 amounted to approximately $7.6 billion, according to Computer Economics, Inc.,[45] with much of the damage occurring in the private sector. Militarily, there was a sharp increase in attacks on DoD computer systems following the bombings of the Chinese Embassy

in Belgrade.[46] Internationally, China's cyber attacks against Taiwan in 1999 were probable causes of a nationwide blackout and the crash of many of the nation's banking teller machines.[47]

Compounding the threat, computer network attacks are relatively easy to launch, giving almost anyone with the desire the needed ability to execute. The equipment is relatively cheap commercial-off-the-shelf goods, doesn't require a logistics tail, is difficult to detect and locate, and is increasingly easy to use, i.e., the required skills level keeps dropping.[48]

Finally, one has to wonder, if the U.S. can mount computer attacks today, is there much hope that our adversaries cannot do the same thing to us tomorrow? Reportedly, AT&T was asked in the 1970s to include "bits and pieces" in the national telephone switch it sold to Poland that would allow it to remotely shut down that country's communications infrastructure. It's also been reported that we developed similar capabilities against North Korean 360/370 military computers.[49] If we were capable of creating those Trojan horses, what makes us think that high technology foreign exporters to us couldn't or wouldn't do the same thing? Since we get much of our commercial chips and software manufactured offshore, we, ourselves, are open to increased vulnerability.[50]

And just as the U.S. military boasts of its ability to crack into weapon computer systems, an adversary could do the same thing to us. According to an article in Federal Computer Week, an Air Force officer sitting in a hotel room in Boston used a laptop computer to hack into a Navy ship at sea and implant false navigation data into the ship's steering system. Gen. John Jumper, Air Combat Command's commander, said, "we should be talking about microchips that manipulate electrons and get into the heart and soul of the SA-10 and SA-12 and tell [the anti-aircraft missile system] it's a refrigerator and not a radar. Those things we are capable of doing today."[51] On the down side of this new found capability, a program manager responsible for the Army's Information Assurance Architecture for the Digitized Force said the potential exists for hackers to infiltrate the computer systems used in tanks and other armored vehicles.[52] Unfortunately for us, then, the technology cuts both ways.

Despite the divergence of opinion on the severity of the information threat, one thing appears certain. The more determined and resourced the adversary is, the more our information and critical infrastructures are at risk. We would be highly vulnerable if opposed by a peer information operations competitor in war, or even by a determined and well-resourced terrorist organization.

LEGAL ISSUES OF INFORMATION WARFARE IMPACT A MILITARY RESPONSE

If, as postulated above, the military's role in the interagency process will primarily be that of deterrence and retaliation against attack, there are some major legal issues that must also be considered.

THE DOD GENERAL COUNSEL WEIGHS IN

The United States did not use most of its information warfare arsenal during the conflict in Yugoslavia in the 1990's for three reasons: the untested state of the U.S. cyber arsenal; Yugoslavia's information technology was not advanced enough to be an effective target; and important to this discussion, nettlesome legal issues.[53] According to the Washington Post, midway through the war with Yugoslavia, the Defense Department's top legal office issued guidelines warning that misuse of cyber attacks could subject U.S. authorities to war crimes charges. The guidelines, "An Assessment of International Legal Issues in Information Operations" issued by the DoD's Office of General Counsel, marked the U.S. government's first formal attempt to set legal boundaries for the military's involvement in computer attack operations, according to a Washington Post reporter.[54]

The guidelines reinforce the need for close interagency cooperation, because in many if not most cases, the U.S. response to international information attacks will likely be led by the Departments of Justice and State rather than the military. The reasons for this are pointed out in the DoD General Counsel's assessment:

- It's difficult to identify the originating attack computer due to such things as the anonymity afforded by traveling through a number of intermediate relay points, using an anonymous bulletin board service, or using a device that generates false origin information.
- It's difficult to identify whether the attacker is an authorized user or has an authorized purpose. That is, once the computer has been located, it is difficult to ascertain whether an authorized user initiated the attack, and if so, whether the attack itself was authorized by the organization employing the user.
- Even if an intrusion is verified as coming from a foreign country, it's difficult to determine whether the attack is state sponsored. And in a globally connected world, an attack can come from anywhere in the world, not just from a computer within the borders of the guilty nation.

- Since an international attack is initially difficult to attribute to a state, it is likely to be treated as an individual attack, and individual attacks are criminal, not military, matters, which should be pursued by the Departments of State and Justice.

The General Counsel's assessment also raises the issue that in times of peace, a computer network attack could be perceived by the UN Security Council as a "threat to peace," or act of war, similar to an armed attack. A U.S. military counterattack to a cyber intrusion, therefore, could be on the same footing as using conventional weapons—an assault on a nation's sovereignty. With possible war crime implications, such a counterattack would likely be used only as a last resort or in self-defense against a major computer attack by a foreign source.

Further tightening the handcuffs of a military response, because of privacy restrictions almost all cyber attacks are initially treated as law enforcement investigations, preventing national security agencies from gaining access to the data.[55] However, even the law enforcement community has encumbering legal restrictions that slow down a response to cyber attacks. Under current law, investigators need a court order to trace back beyond the most immediate Internet service provider. In the Solar Sunrise case mentioned earlier where three teenagers successfully hacked into DoD computer systems, U.S. investigators sought nine court orders to pursue the electronic trail of the teens as the attacks spread through multiple servers in the U.S., as well as sites in the United Arab Emirates, Germany, France, Israel, and Taiwan.[56]

APPLICABILITY OF THE LAWS OF WAR

Nevertheless, the military does have an important role in computer network defense, particularly if practiced during armed conflict. If the nation deems that a retaliatory attack is warranted, there are good reasons why the DoD would be the lead agent in the effort. Not only has DoD built considerable expertise in computer network attack, the DoD General Counsel raises the issue that under one of the principles of the laws of war, the *Distinction of Combatants from Noncombatants*, only members of the armed forces should conduct combatant information operations during international armed conflicts, since combatants must be trained in the law of war, serve under effective discipline, and be under the command of responsible officers.[57]

Other principles of the law of war, on the other hand, are good guidelines in either peace or armed conflict, and should inform military action pursued in the name of information defense:

– *Military Necessity*: Purely civilian infrastructures must not be attacked unless the attacking force can demonstrate that a definite military advantage is expected.

– *Proportionality*: Attacks may be carried out against lawful military targets even if some amount of collateral damage is foreseeable, unless the foreseeable collateral damage is disproportionate to the military advantage likely to be attained. Accordingly, commanders should make a reasonable effort to discover whether the targeted system is being used for civilian purposes that are essential to public health and safety.

– *Indiscriminate Weapons*: Related to the concept of minimizing collateral damage, commanders must ensure IO techniques (e.g., malicious logic) are not indiscriminate, i.e., they don't spread to other information systems providing essential services to noncombatants, don't spread to information systems belonging to neutral or friendly nations, and don't release dangerous forces, such as opening dam floodgates, causing oil refinery fires in populated areas, or releasing radioactivity.

CONCLUSION

Although the US military is assigned the mission of defending the nation from attack, when it comes to protecting the nation's critical infrastructure, the Department of Defense is but one of many players, necessitating a robust interagency process and public-private cooperation. The DoD has neither the ability nor the authority to monitor and protect the cyber networks that increasingly drive the nation's critical infrastructure. Therefore the Defense Department must accept and embrace a coordinated, multi-agency response to attacks on the nation's cyber domain.

However, there are glaring seams in coverage between agencies and the public-private sector that remain troubling. There appears to be a lack of unity of command and effort engendered by the nation's highly diversified approach to protection. A large bureaucracy has been established, but no one seems to have the overall picture and no one short of the President has command of the numerous department and agency responses.

As a result, it appears that a number of changes are in order. First is a reorganization of the initial structure set up to provide federal-level protection and coordination. It may be propitious that a new administration is coming to power at the same time that holes in our information protection coverage come to light through recent denial of service attacks and rapidly spread viruses. I'd recommend that the new administration establish unity of effort through the creation of a National Information Protection Director (NIPD) reporting directly to the President to:

- Develop national policy for both peacetime and wartime
- Coordinate Interagency activities by providing distinct lane assignments
- Share threat information better between public and private organizations

- Consolidate the efforts of the intelligence and defense communities
- Oversee a national database of attack patterns and methodologies
- Increase federal support to research and technology
- Inform and educate private infrastructure companies
- Pre-determine military response triggers and responsibilities so that many of the current legal concerns are addressed in advance
- Continue the current initiatives to offer education and higher pay for information assurance specialists
- And perhaps most importantly, plan and exercise repeatedly for a cyber attack response.

PROPOSED STRUCTURE OF AN NIPD

The NIPD would be a federal civilian government agency, organized in two directorates: one for policy and planning and the other for operations. The NIPD director would report directly to the President and would be invited to attend National Security Council and National Economic Council deliberations as required by those two bodies. The NIPD would make extensive use of the interagency process.

The Policy and Planning Directorate of the NIPD would be responsible for developing the nation's policy and proposed legislation regarding information defense. It would have representation from all government departments and agencies and from the private sector in its effort to ensure that policy addresses technical, legal, and privacy concerns. It would assign clearly defined roles for each department and lay out the requirements for rapid communication of attack warning orders and advise. The planning function would include development of coordinated plans for responses to a number of contingency conditions. These plans would help clarify the roles of each department during an attack and would make clear to each party who they are responsible to communicate and coordinate with during an emergency response.

The Operations Directorate of the NIPD would be responsible for the day to day protection of the nation's information security. It would have divisions for warning, analysis, and enforcement. The Warning Division would operate an attack warning center dedicated to quickly notifying all government agencies and the private sector of imminent or occurring information attacks. The warning center would be co-located and closely aligned with the current NIPC. It would be the first place that departments and private organizations would report attacks to.

The Analysis Division would include the NIPC with its current functions, except for the warning mission. It would have more of a preventative perspective, offering advice to

government and private organizations on protection trends and techniques. It would maintain a database of attacks for future analysis and response. It would coordinate with the CERTs in the government and private sector in performing its duties. It would also be responsible for periodic exercise of the warning and response plan developed by the Policy and Planning Directorate.

The Enforcement Division would be responsible for all enforcement issues. This would include assigning action to the various federal departments and agencies in response to an information attack. Representation of the Justice, State, and Defense Departments would be required in this division. Proposed use of the military in response to information attacks would be rapidly surfaced to the NIPD Director for relay to the NSC and President. The operations of the FBI's forensic laboratory would also be included in this division.

The establishment of a new NIPD position wouldn't exclude a continuing call in some corners for the establishment of a national Information Technology "Czar,' similar to the Y2K Czar. In fact, the NIPD and IT Czar may be one and the same person. An NIPD would provide the needed public visibility for information protection. It would also offer a unified vision and direction for the nation; rally the public and private sector's information protection efforts and resourcing; educate the general populace and end-users on the threat; develop policy that liberates the national defense and law enforcement communities from unneeded restrictions; and organize, direct, and coordinate the efforts of the many agencies required to defend the nation against an information attack.

In summary, the nation's information protection mission is rightfully an interagency concern. The Department of Defense must work with several federal agencies to help organize the nation's defense, to participate in the nation's protection, and even to provide the offense, or retaliation, that may be required in the case of a severe attack. However, the nation's somewhat fragmented protection structure must be reorganized. DoD's role must be clearer, better planned, and continuously exercised to ensure a swift and sure response to attacks on the nation's information and critical infrastructure.

WORD COUNT: 6996

ENDNOTES

[1] J M J Bosch, "Information operations–challenge or frustration?" *Military Technology* 24 (May 2000): 86-89; available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 07223226.

[2] Thomas E Copeland, ed., *The Information Revolution and National Security.* (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, 2000), 108.

[3] Martin C. Libicki, "Protecting the United States in Cyberspace," in *Cyberwar: Security, Strategy, and Conflict in the Information Age,* ed. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden (Fairfax, VA: AFCEA International Press, 1996), 97.

[4] Jack L. Brock, Jr. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks–Statement of Jack L. Brock, Jr., Director, Defense Information and Financial Management Systems, Accounting and Information Management Division, in testimony before the Permanent Subcommittee on Investigations, Committee on Government Affairs, U.S. Senate* (Washington, D.C.: United States General Accounting Office, May 22,1996), 2.

[5] Bradley Graham, "U.S. Studies New Threat: Cyber Attack; Hackers, Simulation Expose Vulnerability." *The Washington Post* (24 May 1998): sec. A, p. 1; [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 01908286.

[6] Those countries include Russia, China, South Korea, Cuba, Japan, France, Germany, Iraq, Israel, and Bulgaria. See Steven M. Rinaldi, *Sharing the Knowledge: Government-Private Sector Partnerships to Enhance Information Security.* (USAF Academy, Colorado: USAF Institute for National Security Studies, 2000), 8.

[7] U.S. Department of Defense. *Joint Doctrine for Information Operations.* Joint Pub 3-13 (Washington, D.C.: Chairman of the Joint Chiefs of Staff, 9 October 1998), pp vii and viii.

[8] Office of General Counsel, U.S. Department of Defense. "An Assessment of International Legal Issues in Information Operations," Second edition, November, 1999, 45, available from <http://www.cs.georgetown.edu/~denning/infosec/DOD-IO-legal.doc>; Internet; accessed 14 December 2000.

[9] Copeland, 16.

[10] Ibid., 3.

[11] Bradley Graham, "Military Grappling With Guidelines For Cyber Warfare; Questions Prevented Use on Yugoslavia." *The Washington Post* (8 November 1999): sec. A, p. 1; [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 01908286.

[12] Joint Pub 3-13, viii.

[13] Ibid., GL-7.

[14] Bill Clinton, "White Paper–The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63." (Washington, D.C., 22 May 1998), 1.

[15] MacDonnell Ulsch and Scott Steinert-Evoy, "We're Not Ready for Cyber Attacks." *Boston Globe* (23 May 2000): sec. E, p. 4; [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 07431791.

[16] Thomas E .Copeland, ed, *The Information Revolution and National Security* (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, 2000), 121.

[17] Douglas H. Dearth and Charles A. Williamson, "Information Age/Information War," in *Cyberwar: Security, Strategy, and Conflict in the Information Age,* ed. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden (Fairfax, VA: AFCEA International Press, 1996), 20.

[18] Thomas L. Friedman, *The Lexus and the Olive Tree,* (New York: Farrar, Straus, and Giroux, 1999), 65.

[19] Office of General Counsel, 45.

[20] Joint Pub 3-13, III-1.

[21] Ibid., III-10.

[22] Steven M. Rinaldi, *Sharing the Knowledge: Government-Private Sector Partnerships to Enhance Information Security,* (USAF Academy, Colorado: USAF Institute for National Security Studies, 2000), 1-2.

[23] These being telecommunications, energy, banking and finance, transportation, water, and emergency services.

[24] Clinton, 1.

[25] Critical Infrastructure Assurance Office, "Protecting America's Critical Infrastructures." 22 May 1998; available from <http://www.info-sec.com/ciao/63factsheet.html>; Internet; accessed 2 December 2000.

[26] Copeland, 127. The comment was made by Dr. John Arquilla of the Naval Postgraduate School of Monterey. He summed up the bureaucratic challenge by stating that "We are beginning to get some interservice coordination, and a little bit of interdepartmental cooperation. The challenge in the years ahead of us is organizational, not technological. Unless we begin to develop some sense of loyalty to an entity greater than an individual service, or the State Department, or one of the other governmental actors involved, we are not going to move ahead."

[27] Vernon Loeb, "After Counterterrorism Bill Fails, Nation's Preparedness Is Debated." *The Washington Post* (9 October 2000): sec. A, p. 21; [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 01908286.

[28] Jack L. Brock, Jr., *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination–Statement of Jack L. Brock, Jr., Director, Governmentwide and Defense Information Systems, Accounting and Information Management*

Division, in testimony before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, U.S. House of Representatives (Washington, D.C.: United States General Accounting Office, 2000), 13. Emphasis (underlining) not in original text.

[29] Ibid., 5-6.

[30] Ibid., 2.

[31] Dan Verton, "Bush eyes overhaul of e-security," *Computerworld* (18 December 2000); available from <http://www.computerworld.com/cwi/story/0,1199,NAV47_STO-55335,00.html>; Internet; accessed 21 December 2000.

[32] Bradley Graham, "Military Grappling With Guidelines For Cyber Warfare; Questions Prevented Use on Yugoslavia." *The Washington Post* (8 November 1999): sec. A, p. 1; [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 01908286.

[33] Office of General Counsel, 44.

[34] Copeland, 4. From Thomas E. Copeland's introduction to the conference report.

[35] Ibid, 89. From presentation by Lieutenant Colonel (Select) Gregory J. Rattray, United States Air Force, on "The Cyberterrorist Threat."

[36] Ibid., 90.

[37] Ibid., 93. From presentation by David Isenberg, Arms Control Implementation Division, Dyn Meridian, on "An Electronic Pearl Harbor? Not Likely."

[38] Ibid., 96-97.

[39] Ibid., 125. From presentation by Dr. John Arquilla, Naval Postgraduate School, and David Ronfeldt, RAND Corporation, on "Towards a National Information Security Strategy."

[40] Brendan P. Rivers, "Information warfare: Where's the action?" *Journal of Electronic Defense* 23 (October 2000): 53-56; [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 0192429X.

[41] Brendan Rivers, "PRC sharpening IW focus," *Journal of Electronic Defense* 22 (August 2000): 20. [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 0192429X.

[42] Clarence A. Robinson, Jr., "Geeks in the wire." *Journal of Electronic Defense* 23 (October 2000): 47-51; [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 0192429X.

[43] Bradley Graham, "Military Grappling With Guidelines For Cyber Warfare; Questions Prevented Use on Yugoslavia." *The Washington Post* (8 November 1999): sec. A, p. 1; [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 01908286.

[44] Ibid.

[45] John J. Stanton, "Rules of cyber war baffle U.S. government agencies," *National Defense* 84 (February 2000): 29-30; [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 00921491.

[46] Robert Wall, "USAF Expands Infowar Arsenal." *Aviation Week & Space Technology* 151 (15 November 1999): 102-103; [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 00052175.

[47] Ibid.

[48] Brendan P. Rivers, "Information warfare: Where's the action?" *Journal of Electronic Defense* 23 (October 2000): 53-56; [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 0192429X.

[49] Winn Schwartau, "Ethical Conundra of Information Warfare," in *Cyberwar: Security, Strategy, and Conflict in the Information Age,* ed. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden (Fairfax, VA: AFCEA International Press, 1996), 246.

[50] Rinaldi, 7-8.

[51] Dan Verton, "Hacker-controlled tanks, planes and warships?" *Federal Computer Week*, March 21, 2000; available from <http://www.fcw.com/fcw/articles/2000/0320/web-hacker-03-21-00.asp>; Internet; accessed 21 March 2000.

[52] Ibid.

[53] Bradley Graham, "Military Grappling With Guidelines For Cyber Warfare; Questions Prevented Use on Yugoslavia." *The Washington Post* (8 November 1999): sec. A, p. 1; [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 01908286.

[54] Ibid.

[55] Verton.

[56] Bradley Graham, "U.S. Studies New Threat: Cyber Attack; Hackers, Simulation Expose Vulnerability." *The Washington Post* (24 May 1998): sec. A, p. 1; [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 01908286.

[57] Office of General Counsel, 7.

BIBLIOGRAPHY

Alberts, David S. *Defensive Information Warfare.* Washington, D.C.: National Defense University, 1996.

Barr, Steven. "Getting Serious About Competing for High-Tech Workers." *The Washington Post* (5 October 2000): sec. B, p. 2. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 01908286.

Bosch, J M J. "Information operations–challenge or frustration?" *Military Technology* 24 (May 2000): 86-89. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 07223226.

Brock, Jack L., Jr. *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination–Statement of Jack L. Brock, Jr., Director, Governmentwide and Defense Information Systems, Accounting and Information Management Division, in testimony before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, U.S. House of Representatives.* Washington, D.C.: United States General Accounting Office, 2000.

Brock, Jack L., Jr. *Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations–Statement of Jack L. Brock, Jr., Director, Governmentwide and Defense Information Systems, Accounting and Information Management Division, in testimony before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate.* Washington, D.C.: United States General Accounting Office, 1999.

Brock, Jack L., Jr. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks–Statement of Jack L. Brock, Jr., Director, Defense Information and Financial Management Systems, Accounting and Information Management Division, in testimony before the Permanent Subcommittee on Investigations, Committee on Government Affairs, U.S. Senate.* Washington, D.C.: United States General Accounting Office, 1996.

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

Chaisson, Kernan. "Cyber offensive mission to begin." *Journal of Electronic Defense* 23 (March 2000): 15. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 0192429X.

Chaisson, Kernan. "Cyber warfare rules 'bumfuzzle' DOD lawyers." *Journal of Electronic Defense* 23 (January 2000): 16-17. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 0192429X.

Chaisson, Kernan. "IW part of EW." *Journal of Electronic Defense* 23 (February 2000): 15. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 0192429X.

Clinton, Bill, President of the United States. "White Paper–The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63." Washington, D.C., 22 May 1998.

Copeland, Thomas E., ed. *The Information Revolution and National Security.* Carlisle, PA: U.S. Army War College, Strategic Studies Institute, 2000.

Cragin, Charles L. "A ready, capable total force." *National Guard* 53 (March 1999): 10-11. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 01633945.

Critical Infrastructure Assurance Office. "CICG Subgroup Roles and Work Plans." 22 March 2000. Available from http://www.ciao.gov/CICG/CICG_group_structure.htm>. Internet. Accessed 2 December 2000.

Critical Infrastructure Assurance Office. "Protecting America's Critical Infrastructures." 22 May 1998. Available from http://www.info-sec.com/ciao/63factsheet.html>. Internet. Accessed 2 December 2000.

Critical Infrastructure Assurance Office. "Summary of Presidential Decision Directives 62 and 63." 22 May 1998. Available from http://www.info-sec.com/ciao/6263summary.html>. Internet. Accessed 2 December 2000.

Frank, Diane. "Agencies pit education vs. cyberattack." *Federal Computer Week* (9 January 2000): Available from http://www.fcw.com/fcw/articles/2001/0108/web-trans-01-09-01.asp>. Internet. Accessed 11 January 2001.

Friedman, Thomas L. *The Lexus and the Olive Tree.* New York: Farrar, Straus, and Giroux, 1999.

Graham, Bradley. "Military Grappling With Guidelines For Cyber Warfare; Questions Prevented Use on Yugoslavia." *The Washington Post* (8 November 1999): sec. A, p. 1. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 01908286.

Graham, Bradley. "U.S. Studies New Threat: Cyber Attack; Hackers, Simulation Expose Vulnerability." *The Washington Post* (24 May 1998): sec. A, p. 1. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 01908286.

Hubbard, Zachary P. "Information warfare in Kosovo." *Journal of Electronic Defense* 22 (November 2000): 57-60. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 0192429X.

Koch, Andrew. "USA to form new warfare centre." *Jane's Defence Weekly* 032 (13 October 1999): 1. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 02653818.

Loeb, Vernon. "After Counterterrorism Bill Fails, Nation's Preparedness Is Debated." *The Washington Post* (9 October 2000): sec. A, p. 21. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 01908286.

National Infrastructure Protection Center. "Advisory 00-058: Cyber Attacks Against U.S. Web Sites in On-going Middle East Conflict." 3 November 2000. Available from http://www.nipc.gov/warnings/advisories/2000/00-058.htm>. Internet. Accessed 2 December 2000.

National Infrastructure Protection Center. "Advisory 00-060: E-Commerce Vulnerabilities." 1 December 2000. Available from http://www.nipc.gov/warnings/advisories/2000/00-060.htm>. Internet. Accessed 2 December 2000.

Navas, William A. Jr. "Posse comitatus, the Army of the 21st century and the law of unintended consequences." *National Guard* 53 (January 1999): 34. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 01633945.

Perry, Tony. "California and the West; Interagency Lab Targets Digital Evidence; Crime: FBI chief Freeh says nation's first regional computer forensics facility will serve as a prototype." *The Los Angeles Times* (15 November 2000): sec. A, p. 3. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 04583035.

Rinaldi, Steven M. *Sharing the Knowledge: Government-Private Sector Partnerships to Enhance Information Security.* USAF Academy, Colorado: USAF Institute for National Security Studies, 2000.

Rivers, Brendan P. "Information warfare: Where's the action?" *Journal of Electronic Defense* 23 (October 2000): 53-56. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 0192429X.

Rivers, Brendan. "PRC sharpening IW focus." *Journal of Electronic Defense* 22 (August 2000): 20. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 0192429X.

Robinson, Clarence A. Jr. "Geeks in the wire." *Journal of Electronic Defense* 23 (October 2000): 47-51. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 0192429X.

Sharp, Walter Gary, Sr. *CyberSpace and the Use of Force.* Falls Church, VA: Aegis Research Corporation, 1999.

Stanton, John J. "Rules of cyber war baffle U.S. government agencies." *National Defense* 84 (February 2000): 29-30. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 00921491.

Tritak, John S. "Defending America's cyberspace: New kinds of threats and responses." *Journal of Electronic Defense* 23 (August 2000): 53-54. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 0192429X.

U.S. Department of Defense Joint Staff. *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance.* Washington, D.C.: Information Warfare Division (J6K), Command, Control, Communications and Computer Systems Directorate, U.S. Department of Defense Joint Staff, 1995.

U.S. Department of Defense Office of General Counsel. "An Assessment of International Legal Issues in Information Operations." Second edition, November, 1999. Available from http://list site info. Internet. Accessed 14 December 2000.

U.S. Department of Defense. *Joint Doctrine for Information Operations.* Joint Pub 3-13. Washington, D.C.: Chairman of the Joint Chiefs of Staff, 9 October 1998.

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

U.S. Department of the Army. *Information Operations: Doctrine, Tactics, Techniques, and Procedures.* Field Manual 3-13. Washington, D.C.: U.S. Department of the Army, 30 September 2000 (final draft).

Ulsch, MacDonnell, and Steinert-Evoy, Scott. "We're Not Ready for Cyber Attacks." *Boston Globe* (23 May 2000): sec. E, p. 4. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 07431791.

Verton, Dan. "Bush eyes overhaul of e-security." *Computerworld* (18 December 2000): Available from <http://www.computerworld.com/cwi/story/0,1199,NAV47_STO-55335,00.html>. Internet. Accessed 21 December 2000.

Wall, Robert. "USAF Expands Infowar Arsenal." *Aviation Week & Space Technology* 151 (15 November 1999): 102-103. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 00052175.

Willingham, Stephen. "China plans to bolster information security efforts, Attaché says." *National Defense* 84 (February 2000): 16. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 00921491.