Issues for the Assured Operation of On-line Infrastructure: Vulnerabilities, Threats, Security, and Safety in Cyberspace

William Johnston
Imaging and Distributed Computing Group,
Information and Computing Sciences Division
Lawrence Berkeley National Laboratory[1], Berkeley CA 94720

Abstract

As developers and maintainers of information infrastructure components in an open network environment -- large-scale Web servers, digital libraries, on-line instrumentation systems, etc. -- we are continually exposed to the malicious elements of cyberspace. We also believe that there is a great deal of emerging technology that can be used to protect on-line systems: public-key certificate-based authentication and authorization systems, public-key infrastructure to validate both human and system identities, various system-level techniques that will provide much more fine-grained control over what we expose to cyberspace, etc.

This document provide an overview of some of the current thinking about the vulnerabilities and threats in cyberspace, and some of the directions for addressing those issues. We also consider the potential contributions of the Lawrence Berkeley National Laboratory, and the DOE Labs, in general, to the problem of protecting on-line infrastructure and environments.

Contents

1.0 Preface

1. The work described in this paper is supported by the U. S. Dept. of Energy, Office of Energy Research, Office of Computational and Technology Research, Mathematical, Information, and Computational Sciences Division, under contract DE-AC03-76SF00098 with the University of California. Contact: wejohnston@lbl.gov, Lawrence Berkeley National Laboratory, mail stop: B50B-2239, Berkeley, CA, 94720, ph: 510-486-5014, fax: 510-486-6363, http://www-itg.lbl.gov/~johnston). This is report no. LBNL-39613.

The United States relies for its very existence--economically, socially, and politically--on an extraordinary sophisticated and intricate set of long-distance networks for energy distribution, communication, and transportation. Because these networks also rely upon each other, a truly serious disruption in any one will cascade quickly through the others, rending the vital fabric of our nation at its most crucial points. Under these circumstances, the ability to respond to national security crises will at least be severely constrained and may be completely interrupted for some crucial interval. Thus, in addition to their serious vulnerabilities to accidents and nature, these networks present a tempting target to terrorists and to any antagonist contemplating an international move contrary to U.S. interests.

"America's Hidden Vulnerabilities: Crisis Management in a Society of Networks", A Report of the Panel on Crisis Management of the CSIS, CSIS Science and Technology Committee, Center for Strategic and International Studies, Georgetown University, Washington, D.C., 1984 (cited in [Kluepfel]).

The dependence of the United States on computers and communications systems to run its critical power, finance and transportation systems places the country at risk in the event of an information warfare (IW) attack, according to a report prepared by a top-level Defense Department advisory panel. This reliance, it said, has "created a tunnel of vulnerability previously unrealized in the history of conflict" and could have a "catastrophic effect on the ability of [DOD] to fulfill its mission." [Brewin]

The report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D), obtained by Federal Computer Week, called the threat of an IW attack "significant," adding that the nation's "vulnerabilities are numerous, [and] the countermeasures are extremely limited...." [Brewin]

Information war has no front line. Potential battlefields are anywhere networked systems allow access--oil and gas pipelines, for example, electric power grids, telephone switching networks. In sum, the U.S. homeland may no longer provide a sanctuary from outside attack. [RAND]

We call protecting targets in cyberspace, such as government, business, individuals, and society as a whole, against [deliberately malicious] actions ... cyberspace security. In addition to deliberate threats, information systems operating in cyberspace can also cause unforeseen actions or events -- without the intervention of any bad actors -- that create unintended (potentially or actually) dangerous situations. ... Such safety hazards can result from both software errors and hardware failures.... In the new cyberspace world government, business, individuals, and society as a whole require a comprehensive program of cyberspace security and safety. [Hundley]

Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.

These critical infrastructures include:

- *telecommunications,*
- *electrical power systems,*
- *gas and oil storage and transportation,*
- *banking and finance,*
- *transportation,*
- *water supply systems,*
- *emergency services (including medical, police, fire, and rescue), and*
- *continuity of government.*

Threats to these critical infrastructures fall into two categories:

1. physical threats to tangible property ("physical threats"),

2. and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats").

Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation.

From: Executive Order, July 15, 1996 Establishment of President's Commission on Critical Infrastructure Protection. [Clinton]

The terms and concepts of "cyberwar" or "information warfare" are current "hot buttons" (and buzz words) in the military arena. The strictly military definition of information warfare (see below) encompasses a broader range of concepts than we are interested in here, but much of the discussion about information warfare defence is directly related to infrastructure protection, and addresses the same issues as for cyberterrorism.

Another issue that becomes clear in reading the available literature is that there is a wide range of opinion on exactly how vulnerable we (and other high-technology societies) are to cyberterrorism, and how likely it is that such activities will on a significant scale. Thoughtful and apparently knowledgeable people ascribe very different scales and likelihoods to the large-scale threats. (See for example, [Libicki1] for a "relaxed" point of view, [Wilson] for an "excited" point of view, and [Collins] for an extreme point of view.)

However, regardless of the level and type of malicious activity in cyberspace, most of it must be addressed by all on-line information systems in order to maintain a useful presence in the global information infrastructure. Cyberspace is, but its nature, very diffuse, and centralized security is no more a possibility than centralized control.

2.0 Background

In broad-brush, the threats to networked computing systems arise from several (non-wartime) motivations[2]:

2. Some of this classification is from [AndersonK94]. However I have separated his classification into motivation and organization, and have added terrorism as a distinct category.

- **Cyberterrorism and Information Warfare** - Attacks on networked system for the purpose of disrupting public infrastructure or committing other acts of sabotage or large-scale disruption. "Terrorism" is probably the term more appropriately applied to action by non-affiliated groups. "Information Warfare" is a military term that is somewhat broader, but also involves the actions of nation-states. ("Class-III Infowar"[3])
  Whether cyberterrorism has actually occurred, and on what scale, is a point of debate and definition.
- **Espionage** - Unauthorized access to networked systems or information for national or commercial economic or strategic objectives ("Class-II Infowar")
  Happens all the time.
- **Extortion and Crime** - Attacks on networked system for profit or unfair market share.
  Happens frequently, and in the case of the banking industry, on a large scale. (See [Schwartau3].)
- **Vandalism** - Access to a system for intellectual satisfaction or vandalism, "hacking". (Privacy = "Class-I Infowar)
  This is, of course, by far the more common form of cyber-crime. Annual loss estimates run to a $1,000M US.
- **System failure** - system failure due to software or hardware problems, or physical disruption due to any reason (e.g. natural disaster) have widespread deleterious effects that are indistinguishable from deliberate, malicious acts.
  At this point in time, by far the most widespread and dramatic cyberspace failures fall into this category. See [Hundley], [Neumann1], and [Neumann2].

The malicious acts are carried out by individuals or groups with certain characteristics:

- Organized groups - seeking access to computer and network systems for specific information or resources
  - define common goals (strategy)
  - select and research targets and develop intrusion methodologies (tactics)
  - use specialization of skills to support the common goals (division of labor)
- Individual intruders - seeking the challenge or thrill of gaining access to a computer system, or just the mean-spiritedness of vandalism

Anderson points out that in threatening computing systems there are significant differences in the motivation and approach of international groups that are based on cultural, regional, and economic factors. Aspects of countering the threats involves understanding both the motivation (e.g., see [Wilkinson]) and the international differences.

2.1 Cyberwarfare / Information Warfare

It is necessary to consider Information Warfare in the context of infrastructure protection because much of the study and motivation is originating in the DoD. From DoD's point of view, the cyberterrorism scenario presents the DoD with a dilemma something like the Vietnam and Afghanistan situations of traditional military forces facing guerilla fighters, but now transplanted to our home soil:

3. These terms -- "Class I, II, and III Infowar" -- are used by Winn Schwartau, a well-known author and consultant in the field of information systems security. See [Schwartau1] and [Schwartau2].

> *Tactical maneuvering in this 'information realm' does not require the extraordinary equipment associated with physical military campaigns (e.g., fighters, tanks). Moreover, it requires no equipment of extraordinary cost. This opens up the means for 'warfare' to non-national players such as shadow groups and individuals anytime and anywhere. [Whitaker]*

The military definition of Information Warfare typically is some variation of:

> *Actions taken to achieve information superiority by affecting adversary information, information based processes, and information systems, while defending ones own information, information based processes and information systems.*

As the military uses the term, then, it is quite broad, encompassing all uses of information in military strategy. This includes not only manipulation of a nation's information infrastructure, attacks on command and control, but the very structure of the military itself.

Possible Information Warfare weapons are used (or at least could be used) by modern armies as well as by terrorists. They are for example (see [Devost2] and [Schwartau2]),

- Computer Viruses
- Worms
- Trojan Horses
- Logic Bombs
- Trap Doors
- Chipping
- Nano Machines and Microbes
- Electronic Jamming
- HERF Guns - EMP Bombs

Although the involvement of the military adds some new factors, the resources to be protected are so diffused throughout society that it seems that the threats to be defended against, and the methods of that defence, are probably similar to those for cyberterrorism. Therefore, much of the actual work of protecting the on-line infrastructure will also be diffused. The DoD information warfare discussions over the next several years will determine the extent and nature of the government's involvement in this task, and how it might influence the civilian sector.

2.2 Types of threats

> *In a Third-Wave[7] society, there are two general methods in which a terrorist might employ an information terrorist attack: (1) when information technology is a target, and/or (2) when IT is the tool of a larger operation. The first method implies a terrorist would target an information system for sabotage, either electronic or physical, thus destroying or disrupting the information system itself and any information infrastructure (e.g., power, communications, etc.) dependent upon the targeted technology. The second method implies a terrorist would manipulate and exploit an information system, altering or stealing data, or forcing the system to perform a function for which it was not meant (such as spoofing air traffic control).*
>
> *[Using] digital tools against digital targets, exploits vulnerabilities in military, commercial and civilian/utility systems that rely on information technology. The authors believe [this] to be "pure" information terrorism and likely the most difficult to detect and counter. The authors also believe that the equivalent of an "electronic*

Pearl Harbor" certainly is possible and would have devastating results. However, there are more subtle forms of information terrorism (e.g. electronic fund theft to support terrorist operations, rerouting of arms shipments, etc.) which would still be political crimes, but perhaps more dangerous because they are less dramatic than a "cyber-Chernobyl," and thus more difficult to detect, and can even appear as "common" crimes. [Devost1]

2.3 Reality of the Threats

If there's been a convincing demonstration of the existence of the capacity AND the motivation to accomplish an "electronic Pearl Harbor," I haven't seen it yet. Which leads me to believe there's still time to better understand the problem and the consequences of the various solutions. But all the trends suggest hat the potential for very disruptive and perhaps even devastating electronic attacks is growing, so now is the time to have these discussions and build awareness and consensus.

Brad Bigelow, National Communications System (OMNCS/N5), bigelowb@ncr.disa.mil . From http://www.stl.nps.navy.mil/lists/c4i-pro/4625.html .

Does the fact that government and DOD computer systems are broken into on almost a daily basis demonstrate anything? How 'bout Kevin Mitnick's adventures? Or does Robert T. Morris' ability to bring down a significant part of the internet scare anyone? Perhaps the demonstrated threat is there but we just haven't been sufficiently awake enough to know it.

Steven J. Schuster, AT&T Bell Labs, Guilford Ctr, W3-K46, P.O.Box 20046, Greensboro, NC 27420, S.Schuster@att.com / Voice (910)279-4555. From http://www.stl.nps.navy.mil/lists/c4i-pro/4630.html .

Winn Schwartau, in his breakthrough book on the subject, identified three levels of information warfare: Class I, Class II, and Class III.(114) These three classes are similar to the three levels of information I developed in 1993(115), as described in Chapter Two. In order to develop a threat assessment portfolio for information warfare, one must focus on the levels of information warfare that are currently being waged today.

As exemplified in Chapter Two, both Class I and Class II information warfare are being waged actively today against individuals and corporations. Perhaps the best example of Class I information warfare in recent months was the attack on Michelle Slatalla and Joshua Quittner after they released their book describing the "hacker wars" of 1990. A group of technically adept individuals calling themselves the Internet Liberation Front jammed Quittner and Slatalla's Internet e-mail accounts rendering them useless, and forwarded incoming phone calls to an out-of-state number "where friends and relatives heard a recorded greeting laced with obscenities."(116) This is just one isolated incident of what has been a recurring problem on the Internet recently.

Class II information warfare is also currently being waged at the corporate level. Intellectual property has been stolen and shipped to foreign nations.(117) Arguably,

even the collapse of one of Britain's oldest financial institutions, the Barings Bank was the result of Class II information warfare.(118) Without the reliance on information technology, the financial damage inflicted on Barrings by risky investments would never have been possible to achieve by one man.

On the Class III level, we have seen where military systems are targeted up to 300,000 times per year and how those targeted systems are penetrated 88 percent of the time. Only one infiltration of military and government systems was traced back to indicate sponsorship by another nation state. This does not mean, however, that such infiltration's are not taking place with state backing now. It only shows that we have not caught them. We know that nations like France, Germany and Israel have information warfare operations in place, but they have not used them to wage Class III information warfare, yet. We have also seen where nations have used offensive information warfare as a supplement to conventional military tactics, and how most advanced weapons systems are heavily reliant on information technology.

Excerpts from Matthew G. Devost's thesis "National Security in the Information Age" [Devost2].

2.4 Vulnerabilities

The problem is everywhere at once:

Information war has no front line. Potential battlefields are anywhere networked systems allow access. Current trends suggest that the U.S. economy will increasingly rely on complex, interconnected network control systems for such necessities as oil and gas pipelines, electric grids, etc. The vulnerability of these systems is currently poorly understood. [RAND]

New technologies run ahead of security:

Moreover, today's security solutions may not scale to emerging high- performance computing technologies, such as multimedia, ultra-high data rates, mobile computing, and very large-scale distributed information storage and retrieval. [DARPA]

Standardization also helps the cybercriminal:

The advancing policies of both industry and government are actually increasing the risk the West is in; for example: The creation of various standards (whether de facto through market clout or through imposition) does incredible damage; the major limiting factor to disease in humans, crops, and livestock has been the heterogeneous nature of the population; reduction of the technology arena to a homogeneous environment (for instance, with a major dominant hardware platform and operating system such as is occurring) only paves the way for the wreckers. [Wilson]

The potential for collateral damage is high:

Disabling the telephone system also, as collateral damage, disables all ancillary services which depend on communications via the system: police, fire, emergency medical care, alarms of all kind but primarily of security systems, power control, water, sewage regulation, etc. [Wilson]

The financial is (at this point) especially at risk:

It may be possible, with a little help from the systems already in place, to destroy the world's currency, capital, and equity markets in a matter of minutes. As the speed of technology came into play in the financial world, the brokerages and financial organizations quickly took advantage of it; it is now a competitive requirement for massive computing power to be constantly watching all the markets of the world, performing analyses, making decisions, and executing orders entirely without the approval or intervention of a human being. Such systems, called 'program trading,' have trillions of dollars at work directly, not counting the leverage gained from their positions; insertion of the right type of orders into the right machines could be devastating and trigger worldwide panic and financial collapse (for instance, the Japanese brokerages selling all their U.S. dollar positions, bonds, and stocks, coupled with reactionary orders in the American trading systems). It is odd that with all the speculation of disaster regarding the removal of humans from the decision loop for military technology, no one recognized the worse impending danger on the economic side.

Attacking the business community of the West is trivial compared with other targets. A simple tactic of hitting with maximum stealth and aiming for maximum damage with 'military grade' worm, virus, and penetration attacks will overwhelm any resistance they can offer. Some small protection against electronic attack has been implemented in the business community, yet it has a set of fatal flaws; such protection systems look for 'known' signatures of attack mechanisms, but the new and novel pass right through. Primary targets will be the mainframes, microcomputers, and networks that businesses in the West rely upon for everything from simple word processing, to decision support or factory automation. [Wilson]

Cyberspace is currently a somewhat fragile infrastructure that works because most want it to work: Like the highway system, there are both written and un-written rules of the road that people follow, even thought it is trivial to break these rules, because most people want and need the automotive transportation systems to work. The same is true for most people in cyberspace. The hacker community, however, is devoted to finding the many weak spots that most people who know about them would not only not attack, but be careful to avoid. (Phrack is one of the most "mainline" of the hacker publications.)

Phrack Magazine is one of the longest running electronic magazines in existence. Since 1985, Phrack has been providing the hacker community with information on operating systems, networking technologies, and telephony, as well as relaying other topics of interest to the international computer underground."
(http://www.fc.net:80/phrack).

The Table of Contents from the most recent issue of Phrack gives the flavor of their interest in the Internet, which is oriented toward exposing the weaknesses, and frequently providing instruction on how to exploit them:

```
1. Introduction
2. Phrack loopback
3. Line Noise
4. Phrack Prophile on Mudge                      by Phrack Staff
5. Introduction to Telephony and PBX systems     by Cavalier
6. Project Loki: ICMP Tunneling                  by daemon9/alhambra
7. Project Hades: TCP weaknesses                 by daemon9
8. Introduction to CGI and CGI vulnerabilities   by G. Gilliss
9. Content-Blind Cancelbot                       by Dr. Dimitri Vulis
```

```
   10. A Steganography Improvement Proposal          by cjm1
   11. South Western Bell Lineman Work Codes         by Icon
12. Introduction to the FedLine software system      by Parmaster
13. Telephone Company Customer Applications          by Voyager
14. Smashing The Stack For Fun And Profit            by Aleph1
15. TCP port Stealth Scanning                        by Uriel
16. Phrack World News                                by Disorder
```

2.5 Societal Issues

Societal issues play a large role in the hacker community. While the acts of individual hackers are usually at the "nuisance" level, several people have pointed out that some hackers grow up to a life of crime already equipped with the skills for cybercrime, as well as the fact that the same societal disaffection that seems prevalent in hackers may make them easy recruits for "serious" criminals and terrorists, etc.

The following quote is from a long article in Phrack (a hacker's magazine) that describes the circumstances that lead up to the theft of the entire British Telecom customer connection data base, that is now being made available to the hacker community. This database contains the technical details of every civilian phone connection in Great Britain, including the types of connections and the connected equipment of every law enforcement agency and police station.

> *These people [the "temps" that BT hires] are often unemployed graduates. Clever, but very, very bored. They don't get paid much, £4.00 an hour. That's what I was paid to write a nationwide database suite for BT but there I have to stop, the gag is cutting into me. They just want a decent job, and try to impress in case they get offered one, and the companies play on this and exploit without mercy. £4.00 an hour and they want unbridled enthusiasm, ideas, loyalty, commitment - who are they trying to kid!*
>
> *The governments of these lands talk big about how the information superhighway will change all our lives, and how committed they are to servicing this new form of infrastructure leading to a new, fresh and exciting dimension - but they also punish, abuse, prosecute, imprison and destroy the lives of the people who may be far better able to exploit their ignorance and expose the sensitive underbelly of their power - their information. If you ask me, the old guys will make CyberSpace just as ugly and corrupt as the society they have already spawned, nurtured and set on a path of destruction out here. I for one don't want or need their advice, support or money - let them lay in the bed they have made, I'll stay in CyberSpace. [Fleming]*

2.6 Approaches to Protecting the Infrastructure

There are a range of opinions on who should be doing what to protect the on-line infrastructure. The sections below sample some of these views. This review is useful because there is a bit of agreement on what should be done even by people who evaluate the vulnerabilities, risks, and threats, fairly differently.

2.6.1 Devost

"Matthew G. Devost has been conducting research on information warfare for three years. He has a masters degree in Political Science from the University of Vermont, where he served as a graduate Fellow authoring papers on the national security, legal and political implications of information

technology. Mr. Devost has also worked in law enforcement, education, and computer programming. Mr. Devost currently works as a Systems Analyst/Engineer for the Information Systems and Technology Group at SAIC, McLean, Virginia. Matthew_Devost@cpqm.saic.com".

Devost is "middle-of-the-road". From Devost's thesis, "National Security in the Information Age" [Devost2]:

> ***National Security Solutions for the Information Age***
>
> *Several steps must be taken to put the United States' digital house in order, and begin dealing with the threat to national security posed by information warfare. Though the following list is not completely inclusive, it should serve as a useful framework for dealing with the problem.*
>
> ***Step One: Declassify the Threat***
>
> ....
>
> *The existence of offensive information warfare capabilities coupled with the United States' heavy reliance on information technologies, has introduced a new threat to our national security. It has been shown that information warfare, most likely in the form of terrorism, is probable because the costs, both politically and economically, are lower than the benefits derived. If an autonomous nation or political group wishes to inflict damage, chaos and fear on American society with minimal costs, then its most rational option is to use offensive information warfare capabilities.*
>
> *If this threat is acknowledged, the response options available to the United States increase. Actions to decrease the impact of an information warfare attack can be undertaken in advance to minimize the damage incurred. Political scientist James Wyllie argues that "Deterrence demands that an adversary be made completely aware of the value of the issue in dispute to the deterrer, and the willingness to collect a price should the rival not be dissuaded from its unwelcome course of action."(122)*
>
> *Acknowledging the threat acts as a deterrent for several reasons.*
>
> *First, it increases the number of responses available to the United States because the issue has been addressed at a political level, and it demonstrates to the international community that this is an important issue. Our capabilities to deal with such an attack are increased because we are prepared for it.*
>
> *Second, it motivates the military and private industry to deal with this problem and create viable security solutions that minimize the vulnerability of the United States' information infrastructure.*
>
> *Third, it gives the United States a political catalyst to deal with this issue on a global level and to enter into treaties and agreements to protect the global information infrastructure and to avert common worst case scenarios. Let us examine each of these in greater detail.*
>
> ***Step Two: Increase Security***
>
> ....

As technological advancements in information technology continue, security must be a vital component. Perhaps, easier said than done. The security of our information systems must be continually increased. Security experts and hackers agree that encryption will be the critical component used to secure computer systems and information transfers of the future.

.... In order for this to occur, the United States government will have to release its stranglehold on encryption technology and allow U.S. companies to export this technology without restriction. Not only does this increase security and stability, but it will also generate growth in the software industry and allow U.S. companies to maintain a comparative advantage in this area.

....

Step Three: Increase Vendor Accountability

Step three is closely linked with step two. In order to increase security and not just manifest an illusion of having done so, vendors must be held accountable for the "secure" products they distribute. Though it is impossible to eliminate all security holes and to find every bug, more must be done to ensure the reliability of systems and software before they are shipped. Also, vendors should be required to create patches and fixes for security holes as they are found and distribute them to all customers.

....

Step Four: Facilitate Private/Public Sector Cooperation

Both the public and private sectors of the United States have a vested interest in the creation of a secure information infrastructure. The military is incredibly reliant on private sector communications lines and does not have the resources to create new secure information technologies on its own. Robert Steele argues that the relationship between the private and public sector with regards to new technology has reversed. Where technology used to migrate from the military into the private sector, it now migrates in the opposite direction. Steele argues that the military and civil sector must now cooperate and that "the military must acknowledge that it cannot dominate information warfare and that it must completely recast its understanding of information warfare to enable joint operations with civil sector organizations including law enforcement, businesses with needed skills, and universities."(125)

....

Step Five: Conceptualize Our Information Sphere

Using a term borrowed from Air Force information warfare doctrine, an information sphere is an assessment of those information technologies that are vital to national security. At the core of the sphere are those technologies that are of greatest value: classified military networks and vital financial networks like the Federal Reserve. As you move away from the core, importance decreases to include non-classified military sites, communications networks and intelligence systems, other financial networks and transaction centers, other communication networks, power grids, private sector information systems and non-operational military information. The outer edge of the

sphere contains the least important information such as personal information and communications.

In order to formulate an integrated approach to addressing the threat of information warfare, the United States must define its information sphere.

....

Once we have conceptualized our information sphere, we must develop methods to asses damage incurred within it. Upon suffering an information warfare attack, the United States must be able to evaluate and assess the damage that its information sphere has sustained. Not only is this essential for repair, but it also allows us to gauge our possible responses based on the extent of the damage we have suffered.

....

Step Six: Multi-Level Education

Education can take place at several levels. First, policy makers can be made aware of the threat and what they can do about it. It is their public obligation to do so. It was suggested in a Congressional hearing that Members of Congress rent and watch the movie War Games in order to understand the threat and techniques used by hackers.(128) Granted, War Games was a revealing movie, but policy makers must have a better understanding of the threat to American national security than this movie provides. ....

The policy makers must also be made aware of what they can do to solve the problem. When discussing HERF Guns at the above mentioned hearing, one Member of Congress asked if such weapons might fall under the auspices of the Brady Bill and if they should be outlawed. Luckily, Mr. Schwartau was able to convince them that to do so "would be banning the microwave and communications industry from existence."(129) Though the threat of information warfare is very real, we should not react with ill-conceived responses, especially if it means sacrificing individual liberties.

At another level, those who run the systems or are in charge of security must be educated to understand and deal with the threats. The largest security hole in computer systems is the human factor. A whole book has been written devoted to this aspect of computer intrusion.(130) ....

Consider the following true anecdote where a hacker named Susan demonstrates her social engineering skills:

As Susan later told the story, a team of military brass...from three services sat at a long conference table with a computer terminal, a modem, and a telephone. When Susan entered the room, they handed her a sealed envelope containing the name of computer system and told her to use any abilities or resources that she had to get into that system. Without missing a beat, she logged on to an easily accessible military computer directory to find out where the system was. Once she found the system in the directory, she could see what operating system it ran and the name of the officer in charge of that machine. Next, she called the base and put her knowledge of military terminology to work to find out who the commanding officer was at the SCIF, a secret

compartmentalized information facility. Oh yes, Major Hastings. She was chatty, even kittenish. Casually, she told the person she was talking to that she couldn't think of Major Hasting's secretary's name. "Oh" came the reply. "You mean Specialist Buchanan." With that, she called the data center and switching from nonchalant to authoritative, said, "This is Specialist Buchanan calling on behalf of Major Hastings. He's been trying to access his account on the system and hasn't been able to get through and he'd like to know why" ...Within twenty minutes she had what she later claimed was classified information up on the screen. Susan argued "I don't care how many millions of dollars you spend on hardware, if you don't have people trained properly I'm going to get in if I want to get in."(131)

....

Finally, the public must be educated to understand the threat of information warfare so that it can endorse the actions taken by the government to deal with this problem. Mr. Schwartau's book does a great service in this area, but more effort is needed to bring information warfare into the public discourse. Citizens have to understand the reliance they have on information technology and the purpose it serves within society before we can justify protecting it.

Step Seven: Use Hackers as a National Resource

....

Some hackers are loyal to the ideals of their nation. For example, when news of Stoll's German hacker selling U.S. secrets to the KGB hit the underground many hackers responded with hatred towards the guy who had associated their movement with national espionage and threats to national security. They were willing to use their abilities to combat this problem, and were even willing to target Soviet computers for the Central Intelligence Agency. One case of a hacker making a contribution to society is the story of Michael Synergy and his quest for presidential credit information. Synergy decided one day that it would be interesting to look at the credit history of then President Ronald Reagan. He easily found the information he was looking for and noticed that 63 other people had requested the same information that day. In his explorations he also noticed that a group of about 700 Americans all appeared to hold one credit card, even though they had no personal credit history. Synergy soon realized that he had stumbled upon the names and addresses of people in the U.S. government's Witness Protection Program. A good citizen, he informed the FBI of his discoveries and the breach of security in the Witness Protection Program.(134)

....

Why should the United States government trust hackers? No trust is necessary. The United States is not offering the hackers anything that they don't already have, except recognition for their ability to discover security flaws. The hackers will remain on the networks regardless of what policy the United States follows concerning their activity. It is simply giving them the forum they need to meet people with similar interests on a legitimate basis, rather than a secret one. Robert Steele argues, "If someone gets into a system, that is not a violation of law, it is poor engineering. When we catch a hacker, rather than learn from him, we kick him in the teeth. When the Israelis catch a hacker, they give him a job working for the Mossad."(135)

Many U.S. corporations already allow the hackers to identify security weaknesses in their computer systems. The Legion of Doom, the most notorious group of hackers in the U.S., briefly entered the computer security business with the formation of their company called Comsec Security. Bruce Sterling reports, "The Legion boys are now digital guns for hire. If you're a well-heeled company, and you can cough up enough per diem and air-fare, the most notorious computer hackers in America will show up right on your doorstep and put your digital house in order - guaranteed."(136) Some argue that this is simply extortion, but individuals are not saying "pay up or else we will enter your system." They are offering their skills to secure vulnerable computer systems from possible electronic intrusion.

....

It is ridiculous to assume that the entire hacker subculture is motivated by criminal intentions. Hackers, like all other groups or subcultures, contain a diverse array of individuals. Every group has a criminal element and the hackers' criminal element is no different than the criminal element that exists within the law enforcement community. A General Accounting Office report on threats to the nations National Crime Information Center, found that the greatest threat to this centralized criminal database was not from outside hackers but from corrupt insiders.(138)

Most hackers are still young and have not formulated complete ideologies regarding right and wrong behavior. Bob Stratton, a former hacker who now works as a highly trusted security expert, argues that "These people (hackers) haven't decided in some cases, to be good or evil yet and it is up to us to decide which way we want to point them."(139) Mr. Stratton argues that we can mentor these individuals and thereby utilize their technological skills.

....

There does seem to be a trend in the past year to utilize hacker capabilities, both in the public and private sectors. This needs to increase, and perhaps some evaluation of our own laws might be necessary if we wish to continue knowing where the holes in the United States' information infrastructure are.

Step Eight: Global Institutions and International Agreements

Just as this issue has domestic political implications, it also has international political implications that need to be addressed. Once the United States acknowledges the potential threat of information warfare it must be prepared to deal with nations expressing similar concerns. Political deterrents like economic interdependence and fear of escalation must be backed by global institutions and international agreements that set standards and pacts for varying levels of information warfare.

....

2.6.2 Libicki

"Martin Libicki is a Senior Fellow at the Institute for National Strategic Studies at the National Defense University, where he specializes in the application of information technology to national security and other worldscale applications."

In “Defending the National Information Infrastructure” ([Libicki1]) Libicki sort of says -- relax, its a problem, but people are blowing it out of proportion.

He points out that, in principle, on-line systems can be better than traditional systems:

> *Nevertheless, against the terrorist, the virtual NASDAQ market can be secured with higher confidence than can the real NYSE stock floor -- if for no other reason than technology permits a system’s owners to control all of its access points and examine everything that comes through in minute detail. In the physical world, public streets cannot be so easily controlled, moving items cannot be so confidently checked, and proximity and force matters.*

Some of his proposals include:

> ***Some Things are Worth Doing***
>
> *Because even the privately owned NII is, in some sense, a public resource, a role for the Government is not entirely unwarranted. But this role must be carefully circumscribed and focussed. This section makes ten suggestions.*
>
> *1. Figure out how vulnerable the NII really is 18. What can be damaged and how easily? What can be damaged through outside attack; what is vulnerable to suborned or even malevolent insiders? For what systems can attacks be detected as they occur and by what means? What kind of recovery mechanisms are in place to return operations after a disruption; after an act of corruption? How quickly can systems be patched to make them less vulnerable? A similar set of questions can be asked about the military’s dependence on commercial systems. How thorough would outages of the phone-cum- internet have to be to system cripple military operations and in what way: operations, cognitive support to operations, logistics (and if so, internal to the DOD or external as well), mobilization? What alternative avenues exist for military communications to go through? What suffers when the 95% of military communications that go through public networks has travel on the DOD-owned grid? A third set of questions relates to the existing software suites on which the NII runs: does, for instance, today’s Unix need replacement or are known fixes sufficient? How useful are test-and- patch kits for existing systems?*
>
> *2. Fund research and development on enhanced security practices and tools and promote their dissemination through the economy. The United States spends a hundred million dollars a year in this area (split among DARPA, NSA, and others). Areas of research include more robust operating systems, cryptographic tools, assurance methodologies, tests and, last, but by no means least, standards. We know how to secure systems; what we do not know is how to make such knowledge automatic, interoperable, and easy to use. Cyberspace may need an information security equivalent of the Underwriters’ Laboratory capable of developing standard tests for systems security.*
>
> *3. Take the protection of military systems seriously. It should be assumed that any nation at war with the United States will attack military systems (especially unclassified logistics and mobilization systems) any way it can -- and hacker attacks are among the least risky ways of doing so. Assume that foreign intelligence operatives are, or soon will, be probing U.S. systems for vulnerabilities. DOD may also have*

legitimate concerns over classified systems in contractors hands and defense manufacturing facilities. It may be useful to stipulate that contractors with the U.S. military (even phone companies) have a reasonable basis for believing their systems are secure. Perhaps DOD needs some method of validating a vendor's source code while providing reasonable assurances that it will not be commercially compromised.

4. Concentrate on key sectors -- or more precisely, the key functions of key sectors. Since, the government cannot protect these systems, it may have to persuade (through its various devices such as contracts, regulation, technology assistance, the bully pulpit) their owners to take security and backup seriously. Several organizations are useful fora for discussing the threat (e.g., Bellcore or the National Security Telecommunications Advisory Council for phones; the National Electric Reliability Council or the Electric Power Research Institute for power plants), non-attribution incident recounting may be especially helpful. Odd as it may sound, critical systems should have some ways of reverting to manual or at least on-site control in emergencies.

5. Encourage the dissemination of threats data and the compilation of incidents data (and not just on the Internet where CERT does a good job). Raw data may have to be sanitized lest investigations be compromised or innocent systems maligned. Nevertheless, effective protection of the public information infrastructure must inevitably involve public policy, and no public policy that relies on "if you knew what I knew" can be viable for very long

6. Seek ways of legimitizing the "red-teaming" of critical systems, in part by removing certain liabilities from unintended consequences of authorized testing. Non-destructive testing of security systems may be insufficient until the state of the art improves; that is, only hackers can ensure that a system is hacker- proof. Unfortunately, hackers are not necessarily the most trustworthy examiners, and, tests do go wrong (the Morris worm propagated faster than intended because somewhere in its program "N" and "1-N" got confused with each other). Incidentally, such systems should be tested both with on-site access permitted, and without it (to better simulate national security threats).

7. Bolster the protection of the Internet's routing infrastructure -- not because the Internet is so important, but because protecting it is relatively cheap. Critical national and international routers should be made secure and the Domain Name Service should be spoof-proof. Note this is not the same as protecting every system on the Internet -- which is expensive and unnecessary.

8. Encourage the technology and use of digital signatures, in part by applying it to security systems and not just electronic commerce. Supporting policies may include research on private key infrastructures, enabling algorithms, and purchases that create a market for them.

9. Work toward an international consensus on what constitutes bad behavior on the part of a state -- and what a set of appropriate responses may be. A consensus permits the rest of the world to handle states that propagate, abet, or hide information attacks by limiting their access to the international phone and internet system -- in much the same way that a similar consensus permits similar trade restraints. That said, proof

that a state has sponsored information attacks will be difficult to establish, and states embargoed on suspicion may often be able to convince themselves and others they have been singled out for other reasons.

10. Strengthen legal regimes that assign liability for the consequences of hacker attacks so that the primary onus rests with the system being attacked (subject, of course, to whatever can be recovered from the actual perpetrator).

Other Things Should be Avoided

This section details what is more important: seven things to avoid.

1. Avoid harping on information warfare to the extent that warfare becomes the dominant metaphor used to characterize systems attacks (much less all systems failures). Porting the precepts of inter-state conflict to computer security tends to remove responsibility for self-defense from those whose systems have been attacked. It is not at all obvious that protection from attacks in cyberspace should be yet one more entitlement.

Why? Promoting paranoia is poor policy -- especially when systems still crash often enough on their own. Once something is called war, a victim's responsibility for the consequences of its acts dissipates. A phone company that may have to recompense customers for permitting hackers to harm service should not be able to claim force majeure because it can argue that it was a war victim. Characterizing hacker attacks as acts of war also creates pressure to retaliate against hackers real or imagined. Reasonable computer security is not so expensive that the United States should be forced to go to war to protect its information systems. If, though, the United States needs an excuse to strike back (say, to forestall nuclear proliferation), the supposition that the target has sponsored information terrorism can be summoned as needed.

2. Don't waste much more effort on traditional intelligence collection for hacker warfare. Crime requires means, motives, and opportunity. Means -- cadres of hackers with some access to connectivity (e.g., not sitting in Pyongyang) -- may be easily assumed. Sixty percent of all Ph.Ds awarded in computer security by U.S. universities went to citizens of Islamic or Hindu countries. Put some effort into motive, to understand plausible patterns of attack by other nations (so as to know what needs security work most urgently). Spend the rest of the time on opportunity, which is to say, finding vulnerabilities so that they can be fixed.

3. Don't waste time looking for a Minimum Essential Information Infrastructure for the NII as a whole 19. Such as list will be undefinable (minimum to do what -- conduct a nuclear war, protect a two MRC mobilization, staunch panic?), unknowable (how can outsiders determine the key processes in a system and ensure that they stay the same from one year to the next?), and obsolescent well into its bureaucratic approval cycle (the NII is changing rapidly and has a long way to go before it gels). More to the point, the government has no tools to protect only the key nodes; what it might have are policies that encourage system owners to protect themselves (and they in turn will determine what needs to be protected first).

4. Don't sacrifice security to other equities. It is difficult, for instance, to see how the NII will be secure without the use of encryption; yet the Government is loathe to

encourage its proliferation (thus Clipper chip and export controls). The controversy seems to be complicating the credibility of Government attempts to secure the NII.

5. Don't put so much emphasis on getting commercial systems to adopt existing security practices that they are unable to take advantage of tomorrow's innovations -- particularly those that enable collaborative computing. Yes, some key systems (e.g., systems that control dangerous devices) must be secure regardless and, yes, many expected innovations have security problems that must be attended too. The entire systems field, though, is too dynamic for a straightjacket approach.

6. Don't eliminate heterogeneity unnecessarily; it makes coordinated disruption harder and preserves alternative paths. Common industry approaches to security matter less than standard protocols and application portability interfaces across industries.

7. Don't try to make policy without detailed understanding of how information systems are used. Strategic nuclear policy is where engineering details matter little (that they explode is far more important than how they explode). With systems security, it is the very details that are the portals to or barriers against attack.

2.6.3 DARPA

Research program:

This program aims to integrate scalable security capabilities into emerging critical technologies, increase the cost and difficulty of attack, and broaden the commercially available and affordable security options and alternatives. This program develops technologies to prevent unauthorized entrance to systems, protect the network infrastructure, and protect information in repositories and in transit. Security tools and services will be developed that can be used by commercial carriers, by third-party providers of security services to make available scalable value-added security support, or by end-system applications to embed security functions. Resultant security technologies can be flexibly combined to meet specific needs and to provide varying degrees of protection.

The program will provide affordable and measurable security solutions for the DoD, and meet the DoD needs for security policy enforcement and high assurance. Secure enclave technologies will allow a distributed set of users to interact as if they were behind a common security perimeter. Secure operating systems that can isolate suspect software and enforce locally- specified security policies are essential for distributed computing and cooperative problem solving across security boundaries. Technologies that allow the interoperation of basic security functions across different key management infrastructures are essential for decentralized security management across administrative domains. The program will foster industry-standard security service interfaces and toolkits so that security can be easily embedded into applications and products. The development of security metrics and evaluation tools will lead to measurable security. Assurance technologies will integrate trusted system development techniques into standard system development environments, and high-assurance components will be included in standard microkernels that will be reused in commercial products.

Tools for Network Security

This area develops the technologies to create a networking infrastructure resistant to external and internal attack, where the infrastructure is intended to support wireless, mobile, and fixed location hosts.

Secure Computing Systems

This area develops technologies to support dynamically instantiated secure enclaves by allowing specific computing resources within a computer system to be assigned to and confined to specific security domains, where these security domains may cross administrative boundaries.

Assurance and Integration

This area develops tools for the development of trusted systems as well as a set of common "middleware" services to help developers build secure distributed applications across heterogeneous platforms.

Survivability and Vulnerability

This area investigates issues regarding vulnerabilities in the nation's computing infrastructure and in emerging critical technologies that could be exploited by an information warfare enemy.

Excerpts from the DARPA information systems security program description. [DARPA]

3.0 The Role of LBNL and the Department of Energy Laboratories

As with the other parts of this paper, these comments and suggestions are mostly limited to issues associated directly with networked computing systems.

I believe that DOE generally, and Lawrence Berkeley National Laboratory specifically, have a contribution to make to the security of on-line infrastructure because of our work in widely distributed applications, on-line instruments, and network protocols.

3.1 Related LBNL Research, Development, and Operations Areas

3.1.1 ESNet

Apart from DoD, DOE's ESNet is one of the largest "single-enterprise" network providers, supplying both open and closed network services to over 30 scientific institutions in the US, and direct international communications links to Japan, Germany, Italy, and Brazil (mechanisms for direct connection to Russia are currently being formulated). ESNet -- centered at LBNL -- is part of the National network backbone, interconnecting with the other backbone components at several national network exchange points.

The ESNet program at LBNL includes the Network Operations Management Center, directory services supporting public-key based authenticating, support for IP multicast-based video and audio conferencing, widespread network access to scientific research facilities, state-of-the-art, high-performance communications for scientific collaborators, including access to National Energy Research Scientific Computing Center.

ESNet also support research and development activities in network protocols, distributed applications - including on-line access to remote instrumentation, and various new network services - including new variations of distributed collaboration tools,

3.1.2 Network R&D

Research projects include (http://ee.lbl.gov):

- CBQ - Class-Based Queueing (quality-of-service and link-sharing for IP networks);
- EPD - Early Packet Discard (an IP network optimization strategy for ATM switches);
- RED - Random Early Detection Gateways (IP-level congestion control);
- SACK TCP - Selective Acknowledgments (improved TCP performance in congested networks);
- SRM - Scalable Reliable Multicast (new protocols to support large-scale distributed collaboration); and the Virtual InterNetwork Testbed project.

Many of these projects are directly related to improved robustness of the Internet, and therefore the information infrastructure that depend on it.

3.1.3 Remote Collaboratories and on-line Instruments

Remote operation of laboratory systems, transparent sharing of scientific data and insights, and collaboration tools of all sorts, represent the scientific community's evolution into cyberspace. (See [Johnston95V] and http://www-itg.lbl.gov.) It is our goal that the mechanisms that underlay the remote collaboratory functionality be robust. Some of these mechanisms are intended to protect

against intrusion, control stream compromise, provide data integrity and confidentiality, etc. Work in remote collaboratories is addressing:

- Security
  The requirements of assured remote operation, as well as widely dispersed sharing of proprietary data make the remote collaboratory applications nearly idea testbeds for a variety of security approaches and functions (as described below).
- Data Dissemination
  Secure and reliable (multicast) transport protocols are required in order to share data among widely distributed collaborators.
- Safety
  Many of the devices that are being brought on-line have never been operated remotely. This leads to the need to address the general issue of principles of safe remote operation, including fail-safe and fail-soft guarantees in the face of infrastructure degradation, failure, or corruption.
- Resource Arbitration
- Video Conferencing
- Tele-Presence
- Network Support
- Electronic Notebooks

3.1.4 Security for Widely Distributed Systems

Security as a component of widely distributed systems supports aspects of assured operation and of dynamic reconfiguration. LBNL's work in this area addresses several (but, of course, not all) vulnerabilities of widely distributed infrastructure.

- Frontdoor vulnerabilities
  The "frontdoor" of systems and applications provide the legitimate means of access (login, remote execution, remote file access, application interfaces, etc.). Securing the frondoor involves "strong" (cryptographic) authentication of the users, definition of their access and action rights, preventing man-in-the-middle attacks through end-to-end data integrity and confidentiality. Further, the strong authentication must be transparent, easily administered, portable, and secure in open networks.

  Our work in this area is focused on architectures for open implementation of public-key cryptography infrastructure, and the application security architectures and components that provide secure and appropriately limited access to resources. (See [Johnston96S].)
- Backdoor vulnerabilities
  There are a wide variety of system weaknesses -- design flaws and design trade-offs, software bugs, etc. -- that can allow penetration and compromise of a system through unintended access mechanisms. Our primary work in this area is "TCP wrappers" in the kernel. This approach essentially allows each system to be configured as its own firewall by imposing configuration, use, and access restrictions on all of the external portals of the system. (In the case of the many on-line Unix systems in the scientific community, attacks through uncontrolled portals constitute a large part of the overall threat to open systems.) We are looking at coupling this approach into our public-key security architecture work for definition and administration of the access rights.

- Denial-of-service vulnerabilities
  There are many aspects of denial attacks. However, at the IP network level, many of the vulnerabilities could be ameliorated through secure identification of the source of packets (this could thwart flooding attacks), secure updates of router information (to prevent deliberate mis-configuration of the network itself), and secure association of the system names and IP addresses (to thwart spoofing attacks). The currently emerging work on secure Domain Name Servers and the addition of public-key information to the DNS records potentially gives us some fairly powerful tools to address the points mentioned. We are working to integrate some of these secure DNS capabilities into our security architectures, as well as working toward deployment of the prototype secure DNS.
- Prototype secure, widely distributed applications
  Our work in very high-speed, high-capacity, widely distributed network storage systems (see [Johnston96A], [Johnston96N], and [Johnston95])is being integrated with our public-key based security architecture work in order to test the utility and effectiveness of this approach to protecting the "frontdoor" of applications and systems.
- Security testbeds for DOE applications
  LBNL was the primary organizer of the second "U. S. Department of Energy, Joint Energy Research / Defence Programs Computing-related Security Research Requirements". (December, 1996)

  The first objective of this workshop was to identify steps that can be taken toward building parts of security infrastructures that can then be used to support research on the identified problems in security testbed environments. One testbed goal is to get some complete security architectures operating in realistic environments so that we can reassess, more accurately evaluate, and make progress on the research issues.

  The second objective to the workshop was to identify outstanding issues for wide deployment and use of the public key cryptography infrastructure needed to provide security for a variety of DOE applications.

3.2 Areas Where LBNL might Contribute to the Security of the NII

Based on our background and involvement in distributed collaboratories, security for distributed systems, and our work with the electric power industry, LBNL might address, in addition to the R&D issues noted above, the following NII issues especially for the on-line scientific environment and various aspects of the electric power system:

- What aspects of what infrastructure are supported by what computing and communication technologies?

  For example, the power transmission industry will put its capacity brokering on-line using Web technology. The required information will be obtained from backend databases (e.g. those of the transmission capacity providers) and Web forms-based processing will submit bids for capacity.

  Computing technology: Web servers frontending company-specific databases, Web server-based processing of "bids" (and ultimately, closing the "loop" with automated power grid scheduling based on this brokering)

Communication technology: All Internet technology based, the major (information) users and producers might interconnect via a private Internet (“Intranet”), but some gateways to the global Internet are inevitable, and probably legitimate.)

- What networking and telecommunications technologies and infrastructure are being used?
- What are the threats to services that use these technologies, or combinations thereof?
- What sorts of security models and architectures could protect against these threats?
- Are different models, architectures, and security services needed for threats from hackers, cyberterrorists, and cyberwarfare?
- What are the common elements of defences against the three classes of perpetrators?
- Is there significant differences in the importance of protecting against disruptive vs. intrusive threats?

Specific projects that are underway include:

- Demonstration security architectures protecting real distributed applications / systems
  We are, or will be in the very near future:
  - working with ORNL to integrate our public-key security architecture into an IPv6 testbed
  - working with Ames Lab to support their digitally signed code project
  - integrating the security architecture with the Mbone video/audio conferencing tools
- Operational security testbeds - with the other DOE Labs, both open and closed testbeds can be developed

  The “testbeds” would be in the form of applications suites and security infrastructure -- not new network testbeds. The networks can be provided by ESNet.

4.0 Annotated Bibliography

“Emerging Challenge: Security and Safety in Cyberspace” [Hundley]

This is a good overview of the general aspects of cyberspace vulnerabilities and security. It is available as a reprint from RAND.

“The Precipice Problem: A Guide to the Destabilization of Western Civilization” [Wilson]

A good (and exciting and witty) overview of many of the potential threats in cyberspace.

“Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance” [DoD1]

This Joint Chiefs of Staff report offers a well-balanced analysis of the DoD’s concerns about information security and electronic national security. In terms of general cyberspace security issues, most interesting sections are:

SECTION 1 - INTRODUCTION
- 1.2 SCOPE
- 1.3 BACKGROUND
- 1.4 THE NATURE OF INFORMATION WARFARE

SECTION 2 ENVIRONMENTAL CONSIDERATIONS
- 2.1 INFRASTRUCTURES
  - 2.1.1 Introduction
  - 2.1.2 Functional Activities and Infrastructures
  - 2.1.3 Electric Power Generation and Distribution Infrastructure
  - 2.1.4 Infrastructure Protection
  - 2.1.5 Infrastructure Assurance
  - 2.1.6 Nature of the Information Infrastructure
  - 2.1.7 Information Infrastructure Vulnerabilities
  - 2.1.8 Information Infrastructure Assurance
- 2.5 TECHNOLOGY ENVIRONMENT
  - 2.5.1 Fundamental Information Security Requirements and Techniques
    - 2.5.1.1 Authentication
    - 2.5.1.2 Encryption
    - 2.5.1.3 Communications
    - 2.5.1.4 Firewalls, Guards, and Multilevel Devices
  - 2.6.3 Adversary Capabilities
  - 2.6.4 Threats to the Information Infrastructure
    - 2.6.4.1 Who is the Adversary?
    - 2.6.4.2 The Extent of the Threat

“Web site for Information Warfare and information Security” [Schwartau1]

This is a good starting point for Web information on cyberspace security issues. Schwartau is a well know consultant in the field.

"An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: "The Day After . . . in Cyberspace II" ([AndersonR96])

This paper is the report of what is essentially a structured brain-storming session by RAND and DARPA on cyberspace security. The following is the list of issues that they came up with:

- Critical Concepts
  + "Safe havens" should be developed as a fallback means for systems when under attack
  + Tactical warning/attack assessment (TW/AA) is an important concept for cyberspace security
- Operational Aspects
  + Operational aspects of security (dealing with people, procedures, regulations) are vitally important to any solution
  + The concept of "cyberspace hot pursuit" needs attention. We need software tools to aid in the backtracing of incidents, to discover the perpetrator.
  + We need procedures for the prepositioning of backup systems and software. The concept of "safe havens" in information systems was discussed, along with the related idea of prepositioning verifiably accurate software (and possibly hardware) for rebaselining corrupted systems.
  + "Red teams" are needed to test system defenses.
  + Map the networks. We need maps of the interconnections among the networks of cyberspace to resolve questions such as: How do energy grid control systems depend on the public switched telephone network (PSTN)? Some agency(ies) should be tasked with maintaining an updated map of the tens of thousands of links and interrelationships and interdependencies among key networks.
  + Personal ID verification systems should be employed.
  + The concept of "human firewalls" should be considered in an emergency.
  + A "two-person rule" might be used for critical decisions or system changes.
  + Consider better pay and status for critical system operators. Personnel might then be less vulnerable to bribes, and less likely to become disgruntled or disaffected. It is widely understood that the trusted insider poses the greatest threat to critical information systems.
- U.S. Government Roles
  + A cyberspace security analogue of government defined automobile safety regulations.
  + A cyberspace analogue of the U.S. Centers for Disease Control (a worldwide clearinghouse).
  + A cyberspace security analogue of Underwriters' Laboratory.
- Key R&D Suggestions
  + Study "distributable secure adaptable architectures"
  + Study "rapid recovery" strategies and systems
  + Study "understanding and managing complex systems"
  + Study the design of processes for developing secure software systems
  + Study the concept of a Minimal Essential Information Infrastructure (MEII)
  + Study the MEII functionality for various segments of our society
  + Study the analogy of "biological diversity" for complex information systems
  + Study the biological immune system metaphor for software
  + Study "dynamic diversity" in infrastructure information systems
  + Replace software with firmware?
  + Study the ability to "sterilize" data passing through our telecommunications systems

+ Study the ability to reengineer or retrofit legacy information systems to enhance their security
+ Sponsor development of an aircraft-like “black box” recording device
+ Sponsor development of software or hardware that would record tamper-proof audit trails for information systems
+ Develop software that can perform real-time pattern detection as an aid to attack assessment

“National Security in the Information Age” ([Devost2])

This thesis is a fairly readable overview.

5.0 References

AndersonK94 Kent E. Anderson, “International Intrusions: Motives and Patterns”, Proceedings of the 1994 Bellcore/Bell South Security Symposium, May 1994.
http://www.aracnet.com/~kea/Papers/paper.shtml

AndersonR96 “An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: “The Day After . . . in Cyberspace II”. Robert H. Anderson and Anthony C. Hearn. RAND Report MR-797-DARPA.
http://www.rand.org/publications/MR/MR797

Brewin “Information Warfare: U.S. sitting duck, DOD panel predicts”. Bob Brewin and Heather Harreld, Federal Computer Week, November 11, 1996.
http://www.fcw.com/pubs/fcw/1111/duck.htm

Buchan “Information War and the Air Force: Wave of the Future? Current Fad?”. Glenn Buchan, RAND, IP-149.
http://www.rand.org/publications/IP/IP149/

Clinton Executive Order: July 15, 1996 “Establishment of President’s Commission on Critical Infrastructure Protection (“Commission”)”. William J. Clinton, The White House, July 15, 1996
Available at http://www.infowar.com/CIVIL_DE/Cyberwar.html-ssi

Collins “The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge”, Remarks by Barry C. Collin, Institute for Security and Intelligence
http://www.acsp.uic.edu/OICJ/CONFS/terror02.htm

DARPA “Defensive Information Warfare”.
http://www.csto.arpa.mil/ResearchAreas/Defensive_Information_Warfare.htm

DoD1 “Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance”. U. S. Dept. of Defense, Joint Chiefs of Staff
Available at http://www.infowar.com/mil_c4i/joint/joint.html-ssi

Devost1 “Information Terrorism: Can You Trust Your Toaster?”. Matthew G. Devost, Information Systems and Technology Group, Brian K. Houghton and Neal A. Pollard, The Strategic Assessment Center, Science Applications International Corporation.
http://www.infoterror.net/terrorism/itpaper.html

Devost2 “National Security in the Information Age”. A Thesis Presented by Matthew G. Devost to The Faculty of the Graduate College of The University of Vermont In Partial Fulfillment of the Requirements for the Degree of Master of Arts Specializing in Political Science May, 1995.
Available at http://www.terrorism.com/documents/devostthesis.html

Fleming “The Truth...and Nothing but the Truth”. Steve Fleming, Phrack Magazine, Volume Seven, Issue Forty-Eight, File 16.
http://www.fc.net/phrack/files/p48/p48-16.html

Hundley “Emerging Challenge: Security and Safety in Cyberspace”. Richard Hundley and Robert Anderson. IEEE Technology and Society Magazine, Winter 1995/1996. Available from
http://www.rand.org/cgi-bin/Abstracts/getab.pl?14103327-14103737

Johnston96A "Distributed Environments for Large Data-Objects: The Use of Public ATM Networks for Health Care Imaging Information Systems" W. Johnston, W., Jin Guojun, Gary Hoo, Case Larsen, Jason Lee, Brian Tierney, Mary Thompson. Asia-Pacific Information Infrastructure Testbed Forum, Seoul, Korea, June, 1996.
Available at http://www-itg.lbl.gov/~johnston/APII.1.1.fm.html

Johnston96N "Distributed Environments for Large Data-Objects1: Broadband Networks and a New View of High Performance, Large-Scale Storage-Based Applications". William Johnston, Jin Guojun, Gary Hoo, Case Larsen, Jason Lee, Brian Tierney, Mary Thompson. Interworking '96, Nara, Japan, October, 1996.
Available at http://www-itg.lbl.gov/~johnston/NARA/NARA.1.7.fm.html

Johnston96S "Security Architectures for Large-Scale Remote Collaboratory Environments: A Use-Condition Centered Approach to Authenticated Global Capabilities" W. Johnston and C. Larsen.
Available at http://www-itg.lbl.gov/~johnston/Security.Arch.Global.Cap.html

Johnston95V "The Virtual Laboratory: Using Networks to Enable Widely Distributed Collaboratory Science". W. Johnston, and D. Agarwal. A NSF Workshop Virtual Laboratory whitepaper.
Available at http://www-itg.lbl.gov/~johnston/Virtual.Labs.html)

Johnston95 "A Distributed Parallel Storage Architecture and its Potential Application Within EOSDIS" William E. Johnston and Brian Tierney, Lawrence Berkeley Laboratory; Jay Feuquay and Tony Butzer, EROS Data Center / Hughes STX. NASA Mass Storage Symposium, March 1995.
Available at http://www-itg.lbl.gov/DPSS/papers.html

Kluepfel "Countering Non-lethal Information Warfare: Lessons learned on foiling the Information Superhighwayman of the North American public switched telephone network". Hank Kluepfel. Originally in Proceedings of the IEEE 29th Annual 1995 International Carnahan Conference on Security Technology.
Available at http://www.infowar.com/CIVIL_DE/kluepfel.html-ssi.

Libicki1 "Defending the National Information Infrastructure". Martin C. Libicki, Advanced Concepts, Technologies, and Information Strategies, Institute for National Strategic Studies, National Defense University.
http://www.ndu.edu:80/ndu/inss/actpubs/niitemp.html

Neumann1 "Risks Forum" Peter G. Neumann moderates the ACM Forum on Risks to the Public in the Use of Computers and Related Systems. One manifestation of this is the widely-read on-line Risks Forum newsgroup news:comp.risks . Also see the archives at http://catless.ncl.ac.uk/Risks .

Neumann2 Computer-Related Risks, Peter G. Neumann. Published by ACM Press / Addison Wesley,1995, ISBN 0-201-55805-X, 384pp. paperback. (ACM Telephone orders 1-800-447-2226, ACM Order #704943.)

RAND "Information Warfare: A Two-Edged Sword". RAND Research Review, Fall 1995. Vol. XIX, No. 2
http://www.rand.org/publications/RRR/RRR.fall95.cyber/infor_war.html

Schwartau1 "Web site for Information Warfare and information Security". Winn Schwartau. http://www.infowar.com/

Schwartau2 Information Warfare - Cyberterrorism: Protecting Your Personal Security In the Electronic Age. Winn Schwartau. Thunder's Mouth Press, New York, 1996. Tel. 212.780.0380, ISBN: 1-56025-132-8
http://www.infowar.com/chezwinn/winnbook.html-ssi

Schwartau3 " ... four reports ... discuss the June 2 and June 9, 1996 London Time articles about alleged extortion on banks in England. Some surprising results. The story isn't over yet." Winn Schwartau.
http://www.infowar.com/class_3/class_3.html-ssi

Whitaker http://www.informatik.umu.se/~rwhit/IW.html. Randall Whitaker, Adjunct Researcher Institutionen for Informatik, Umea Universitet, Sweden.

Wilkinson "Terrorism: Motivations and Causes", Commentary No. 53 - a Canadian Security Intelligence Service publication.
http://www.csis-scrs.gc.ca/eng/comment/com53e.html

Wilson "The Precipice Problem: A Guide to the Destabilization of Western Civilization". Michael Wilson - The Nemesis Group
Available at http://www.infowar.com/class_3/class3_3.html-ssi