The following paper is an edited version of Chapter 12 from
The NCSA Guide to Enterprise Security
Published in 1996 by McGraw-Hill
By M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems, Norwich University
mkabay@compuserve.com

Objectives:
After studying this chapter, readers should be able to
1. Define the three levels of information warfare.
2. Give examples of each type of infowar.
3. Discuss actions for defending organizations and society against infowar attacks.

1 Introduction

This chapter looks at information security from a different perspective. It was originally written for the Canadian Security Intelligence Service and provides an overview of how deliberate attack on information technology can affect individuals, organizations and entire societies.

1.1 Historical Perspective

Throughout the history of conflict, technology has provided both weapon and target. When warriors mounted horses, their steeds provided both threat and vulnerability to opponents. To harm a single mounted man, one could attack his horse. To imperil a nation of horsemen, one could poison the herds. Armoured knights fell to crossbows, but a more subtle attack was to destroy the foundries.

The defining technology of civilization as we enter the twenty-first century is the computer. Computers are pervasive, necessary and vulnerable to attack. Computers are linked to each other through networks; one cannot pick up a daily newspaper without reading about the data superhighway that will supposedly bring cyberspace into our living rooms and allegedly bring anything from good grades to the end of civilization.

Cultures that depend on information systems are vulnerable to information warfare. Information warfare consists of deliberate attacks on data confidentiality and possession, integrity and authenticity, and availability and utility. Information warfare can harm individuals, corporations and other private organizations, government departments and agencies, nation-states and supranational bodies. Information warfare is the extension of war into and through cyberspace.

Military planners have recognized their dependence on information technology; some forces now speak of C4I: Command, Control, Communications, Computers and Intelligence. Protecting the technology of war against attack is an obvious extension of the military mind set; smart bombs require smart defences. However, there is still no general agreement within the military establishments of the planet on the importance of protecting civilian as well as military

information infrastructure. As for civil defence, there is a long way to go in including the information infrastructure as a necessary component of protection and recovery operations. Federal government departments are at least required to pay attention to the Government Security Policy, which mandates attention to security and business resumption planning (BRP); however, the task has barely begun in most departments. Provincial and municipal governments are at different stages of awareness and implementation of security and BRP. Finally, in the civilian arena, there are still many organizations which assume that disasters--let alone deliberate attack--will never strike.

Given the degree of dependence on information systems, it is essential to erect legal, organizational, and cultural defences against information warfare.

1.2 Conceptual Framework

Information technology has so permeated the popular culture that many people now recognize the term cyberspace. Cyberspace is the realm of communications and computation. A telephone call, for example, is said to exist in cyberspace; so does a MUD (multi-user domain, where people play games with each other and with computers) or an online database of bibliographic references. When fighter pilots use computer-generated displays to locate and destroy targets, they are working simultaneously in cyberspace and in the physical world.

Alvin and Heidi Toffler have recently published a cautionary text looking at the transformation of warfare. They explore many aspects of warfare in the age of cyberspace and have several sections dealing with information warfare proper. They provide a good introduction to the changes that must occur in military thinking as cyberspace expands.

Winn Schwartau has defined three levels of information warfare:

- Level one: interpersonal damage. Damage to individuals in recent cases includes impersonation in cyberspace (e.g., false attribution of damaging communications), appropriation of credit records (for fraud and theft), harassment (e.g., interruption of phone services) and loss of privacy (e.g., theft of medical records).

- Level two: intercorporate damage. Attacks on the financial and operational interests of corporations, government departments, universities and so on. Such attacks include industrial espionage, theft of services or money, and sabotage.

- Level three: international and inter-trading block damage. Destabilization of entire economies and societies. The techniques of information warfare levels one and two could be applied in a systematic way by terrorists, extortionists, or foreign governments.

2 Tools of Infowar

For those unfamiliar with the security of information technology (I.T.), the following sections will provide an introduction to the ways criminals, spies and saboteurs can attack such systems. This review will serve primarily to alert readers to vulnerabilities; this is not a primer on countermeasures.

Techniques of attacks on I.T. fall into four basic categories: penetration, disruption, programmatic attacks and physical interference.

2.1 Penetration Techniques

Breaching security perimeters is the first step in many, but not all, attacks on I.T. Attackers, especially criminal hackers, have developed a range of techniques generally called "social engineering." Many techniques involve eavesdropping, or unauthorized listening to communications. Weak access controls give many intruders a nearly open door into data processing and communications systems; brute-force attacks target harder perimeters. Traffic analysis, a component of SIGINT, or signals intelligence, allows an observer to deduce important information by monitoring communications flows. Finally, data leakage is the practically undetectable loss of control over or possession of information.

2.1.1 Social Engineering

Social engineering often begins with scavenging, the search through discarded materials for nuggets of valuable information. Scavengers (also known as Dumpster divers when they root through real garbage) are especially interested in security information that can help them penetrate the perimeter using identification and authentication data. Logon IDs (identification) and their passwords (authentication, or proof of legitimate use of the ID) are prizes in this search. Jerry Neal Schneider, for example, was a teenager with a peculiar propensity for rummaging through the discarded papers from his local Pacific Bell Telephone Company (PacBell) offices. Over several years, he amassed an impressive collection of only slightly out-of-date materials on PacBell policies and procedures. He infiltrated PacBell offices by pretending to be a reporter (no one checked his credentials) and obtained additional information on PacBell management of their inventory. Finally he struck: he ordered a drop off of several thousand dollars worth of PacBell equipment at an authorized spot and collected it using a repainted PacBell van he had purchase for a small sum. This stolen equipment was the start of a thriving, multimillion dollar business in used electronic gear; at one point he even sold some of the stolen materials back to PacBell for what the victims thought a good price.

In addition to physical garbage such as discarded paper and magnetic media, scavengers can search through data remnants such as erased files on disk. It's a pity the DOS "ERASE/DELETE" command was not called the "DESTROY-FIRST-BYTE-AND-LOSE-THE-POINTER" command; such a name might have taught more people that files "erased" by DOS

and WINDOWS are actually still on disk until their sectors (addressable areas on disk) are overwritten by later disk writes. Utility programs can easily recover some "erased" files because of this implementation. Even some ways of formatting a disk may not destroy pre-existing information; a “low-level format,” on the other hand, does obliterate all user data on the disk. Some file manager programs provide a “wipe” option for deletes which overwrites file sectors with random data before erasing a file, and this technique should be more widely used for sensitive data. In general, no one should exchange diskettes without wiping existing files.

In military or other high-security applications, a particular problem is magnetic remanence on defective hard disks. If a hard disk fails so that it is impossible to write data to it, there is no way to overwrite those data. There have been many cases of used disk drives being sent to a new customer by service companies as part of an exchange service; these disks may contain proprietary software and data of great value. One of the Sysops (system operator) of the NCSA Forum on CompuServe actually received such a used disk in exchange for her broken unit; it contained client lists from a competitor. If the data on the damaged disk are not encrypted, the disk drive can be subjected to degaussing (exposure to high magnetic fields). In military or government applications where highly confidential data are on the magnetic surface, even degaussing is not considered adequate. In these cases, physical destruction (oxy-acetylene torches are apparently favoured) does the job effectively.

Another magnetic remnant usable by the scavenger is leftover RAM: areas of temporary memory that have been released by programs but not cleared by the operating system. Examples include terminal memory after a session has completed, file buffers, and print buffers. When terminal emulation programs are used for communications, they sometimes reserve large areas of memory for display; one can scroll through an entire session from start to finish. Logging off without clearing this memory can allow someone else to read through the previous session, print it, or save it to disk for later analysis.

Social engineering's most powerful and commonly-used technique is impersonation. Impersonation can occur on the human level or electronically. For example, “piggybacking” consists of entering a secure area at the same time as an authorized user. When an employee slips an ID card through the reader and politely ushers a colleague through the door first, the pair have fooled the security system into allowing two people into the area on one ID. Similarly, when users leave work stations logged into a network without putting up a security screen, they have encouraged logical piggybacking into the network. Both forms of piggybacking are made easier by psychosocial factors which impede the implementation of security policies. Most people are socialized into holding doors open for others, so letting one's colleague (or a visitor) in through a security screen may not even register in the perpetrator’s mind as a violation of security: it’s just normal politeness. Blanking one’s screen and locking it before getting up for a coffee may make a naive user uncomfortable: it implies lack of trust of colleagues, and society teaches people to value trust. Appropriate awareness training and practice can overcome these inappropriate scruples.

On a technical level, it is possible for a computer system to impersonate another computer. In January 1995, an Advisory from the Computer Emergency Response Team Coordination Center (CERT-CC) at Carnegie Mellon University (Pittsburgh, PA) described a “spoofing” attack on

Internet computers. The attack, aimed at SUN workstations, depended on returning false addresses to obtain unwarranted authorization for network access. In electronic mail systems, it is often easy to alter the routing information to give the illusion that a message has originated at another or even at a mythical computer. It is also possible to use so-called anonymizing servers to remail messages stripped of all original identifying information. According to a report in February 1995 from a Swedish investigation, such a system in Finland has been used by paedophiles around the world to exchange pornographic computer files and to entice children into illicit meetings.

Other social-engineering methods of obtaining information include seduction, bribery, extortion and blackmail. Susan Thunder, a notorious prostitute-turned-hacker, habitually seduced nerdish computer systems operators and then rifled through their belongings during their post-coital stupor to find personal information of use in cracking their systems. As for bribery, one of the little-recognized risks of underpaying and generally abusing employees is that it is easier to suborn a disgruntled employee than a happy one. The full backups of a corporate system may cost $100 in physical media and may required the attention of an operator paid $25,000 a year; however, the value of such backups to a competitor may be in the $millions. Payment of a few months of salary to an unhappy and dishonest operator may bring a return on investment of several orders of magnitude.

Extortion consists of threatening damage unless the victim obeys instructions. There have been cases in which criminals steal the only backups to a system after destroying the original disk copies; such attacks are much rarer now that most people make frequent backups and keep them securely off site. Another form of extortion consists of threatening to sell proprietary and highly valuable information to a competitor.

Organizations which tolerate criminal violations such as software theft are vulnerable to blackmail. Any employee can call a toll-free number to report the use of unlicensed software. Whistle-blowers can report improprieties in government using toll-free numbers and have their anonymity protected; the Securities and Exchange Commission of the U.S. also provides such 800-numbers. Obey the law to avoid any vulnerability to this kind of information warfare.

2.1.2 Eavesdropping

Surveillance equipment has become widely available through catalogs and even store-front operations. Equipment used as props in James Bond movies is now inexpensive and easy to obtain. Wiretaps can be placed on phone lines without even having to connect wires directly to the metal; tiny microphones with radio emitters can broadcast a phone conversation to a listener outside the building. But since millions of people hook modems to their phones for communications between computers, eavesdropping now provides a means for monitoring data transmission. Unencrypted data sent over phone lines can be monitored at the origin, the destination, or anywhere in between. A $600 hand-held wide-band scanner can be used to detect transmissions passing through microwave relays at distances of 50 m and more from the towers. Satellite downlinks have “footprints” of up to 100 km in diameter where signals can easily be picked up and used. Cellular phone calls are trivially easy to monitor, as are any calls made over

domestic wireless phones. Anyone concerned with security should also disable baby monitors while making confidential phone calls; the monitors broadcast everything within earshot and have no security provisions for preventing eavesdropping. Finally, van Eck freaking is the practice of detecting signals at a distance, usually from video display terminals, and reconstituting them to usable form. Demonstrations of van Eck freaking have involved equipment costing less than $100 and have succeeded at distances of hundreds of meters. It would be possible to put appropriate electronic gear in an unobtrusive van for a few $thousand and then park the vehicle in the middle of an industrial park for a windfall of information, some of it useful at face value and some of it useful for criminal hacking.

Similarly, now that local area networks (LANs) have become the basic architecture for new information systems in the client/server model, eavesdropping on LANs is a powerful method for extracting valuable information. For example, it is easy to run LAN sniffers--programs which capture all transmissions on the network instead of only the ones destined for a specific, authorized work station. By putting a work station into “promiscuous” mode, anyone can monitor traffic and solve network problems; unfortunately, they can also decode the contents of packets being sent to other workstations on the LAN. Thus a dishonest employee could buy a LAN sniffer or download it from the Internet at no cost and then monitor the system manager's workstation until that person logged on. The system manager's ID and password might be visible and usable unless the network operating system encrypted such information (i.e., made the ID and password unreadable without the proper key).

Similarly, Internet sniffers permit unscrupulous people to monitor unencrypted transmissions through the network of networks that links tens of millions of users and millions of computers. In 1993 and 1994, there have been cases of special modified programs for establishing an interaction with computer systems; these Trojan login programs captured the first 128 characters of each session--plenty to determine a user's ID and password if sent unencrypted. Over ten thousand IDs were said to have been compromised by these Trojan login programs.

2.1.3 Intrusion

Classic failures in security that are exploited by criminal hackers, spies and saboteurs include wide-open old modems, canonical passwords, Joe accounts and generally bad password policies. Any system with a modem kept powered on and appropriate communications software running is at risk of attack and penetration. Factory pre-set passwords in computer systems, telephone switches, and voice-mail systems are a major entry point for intruders. So-called “Joe” accounts, where the password is the same as the ID (e.g., account MGR.FINANCE, password FINANCE) are far too obvious to allow on a system.

Brute-force attack involves trying all likely or possible authentication codes for a given ID. Such attacks often begin with dictionary files to deal with all the easily-guessed passwords and then moving on to random patterns of letters and numbers. The main vulnerability making such attacks possible is that system administrators place inadequate limitations on login speed; it's possible on some systems to try as many passwords as the communications speed allows. Another fundamental problem is that many systems and administrators permit a highly restricted

key space; i.e., there are too few possibilities for the authorization codes. As a trivial example, readers will note that on a five-position keypad such as is commonly used to keep doors locked, there are only 120 unique sequences of five digits. Even with only a few minutes per attempt, it does not take long to try all possible sequences.

2.2 More Subtle Attacks

Once intruders or dishonest authorized users have gained entry to a restricted system or a restricted area, they can extract information in various ways. For example, even if data are encrypted, traffic analysis (noting the volume of transactions flowing between nodes in a network or data sets in a database) can reveal information that should be restricted. Even the communications bandwidth alone can tell a spy something of value; e.g., if a manufacturing firm is planning to triple the channel capacity for its Brampton plant, a dishonest competitor will know that it may be worth infiltrating that plant because there is something new happening there. Homely details such as filenames can inadvertently reveal information or indicate importance; e.g., a file named URGENT.FAX is more likely to be of interest than F782H3B.TXT. Similarly, suggestive directory or folder names can attract the attention of spies or saboteurs; e.g, files in C:\R&D\NEW_PROD might be very interesting to an industrial spy. Finally, security restrictions themselves should be considered of extremely high sensitivity; the access control lists for a file might show unauthorized users which user ID could legitimately access it and thus provide a valuable new target.

Perhaps the most pervasive and subtle attack of all is data leakage--the insensible copying of restricted information. The main reason information can be stolen so easily is poor data security among users and administrators of work stations (the term personal computer should have been banned from office environments because of the false impression it creates). Such systems have standardized data formats (e.g., spreadsheet, database and word-processing files) that can easily be read on millions of systems around the world. In contrast, mainframe files tend to be in proprietary or site-specific formats which are considerably more expensive to convert and use. In addition, work stations often have high-capacity miniature media such as 1.44 Mb (megabyte, or millions of characters) diskettes a few cm in diameter (recent products can put 10 Mb on a diskette) or removable disk drives holding up to a Gb (gigabyte, or approximately 10^9 characters) on units that can be concealed in a pocket. Typically, work stations have limited or no physical controls against data theft; they rarely have access-control software installed.

Some simple precautions can make data theft less likely. Clearly labelling all removable media with tags that indicate their level of sensitivity and their ownership would make “accidental” removal of such media less excusable. Security programs on each workstation can prevent unauthorized access to the computer and control use of the diskette drives; the auditing features of such programs can provide a record of all activity by each user ID and by so doing further discourage casual data theft

2.3 Disruption

If people want to disrupt the work of an organization in the computer-driven world of today, they have many techniques available. Programmatic attacks and sabotage are easy to implement in most computerized environments. Denial of service attacks by saturation of capacity are also very easy and harmful.

2.3.1 Programmatic Attacks

Programmatic attacks use executable code to interfere with normal processing. Executable instructions determine everything that general-purpose computers can do. Programs are sets of instructions for specific purposes. There are programs in the equipment (hardware) itself--these are the "hard-wired" functions of the arithmetic logic units and other processors. Then there are programs which are put into read-only memory (ROM) units; these are called "firmware" by analogy to hardware and software. Software generally refers to program files (on DOS based computers, these have file extensions such as .COM, .EXE, .DLL and so on), but actually there can be executable instructions in the first sector of every disk as well.

Programmatic attacks include, among others, Trojan Horse programs, logic bombs, worms, viruses, knowbots and cancelbots.

A Trojan Horse program looks like a useful tool but actually has unauthorized and possibly dangerous functions. Trojan login programs, mentioned above, silently capture passwords for later inspection while authorizing sessions. Trojan compilers convert ordinary source code into executables that can include unauthorized back doors to subvert security. Logic bombs are any unauthorized sequence of instructions with a trigger (e.g., a date) and a payload (e.g., wiping out records in a database). Without the appropriate inactivation code, the logic bomb damages data according to the programmer's instructions. The disgruntled programmer shown in the movie Jurassic Park left a logic bomb in the system after he left; so did the mistreated programmer in the movie Single White Female.

In real life, some consultants in the CONSULT Forum of CompuServe have admitted publicly that they generally leave logic bombs in their custom-written computer programs for clients and remove the bomb only once the client has paid them in full for their work.

Worms are programs or other executables that spread through a network. Some worms send a copy of themselves into a neighbouring system and then "die." Robert T. Morris sent a worm into the Internet on November 2, 1988; unfortunately, due to programming errors, the worm reproduced madly in thousands of systems, causing havoc that consumed days of time for thousands of system administrators and users. Estimates of the damage caused run to the tens of millions of dollars in lost data and wasted time. Perhaps the only good thing coming out of the Morris Worm incident is that it (and another worm attack in late November 1988) led to meetings of Internet experts who then helped found the

Viruses are programs which insert themselves into other executables. The most widespread viruses "live" in disk boot sectors, from which they enter RAM on DOS and Macintosh workstations during system initiation. This "boot" process always looks at the boot sectors of diskettes and disks that are accessible; thus if an infected diskette is still in the boot drive (usually A: on a DOS machine), the virus is loaded and executed before the rest of the operating system is loaded--and thus before any normal security mechanisms are engaged. Once in memory, the viral code can do anything the operating system can do. For example, some of the five thousand known virus varieties can garble printer output, make all periods disappear from DOS commands, scramble file names, erase portions of disks, and make green caterpillars crawl around computer screens. Worse still, some viruses, such as those concocted by the Bulgarian "cyberpath" who calls himself Dark Avenger, cause subtle data damage that may not be noticed for months yet can falsify results with potentially fatal effects.

Knowbots are programs which, like worms, move from system to system; they are designed to seek out specific information and report back to their originators. Cancelbots are knowbots which seek out electronic mail or postings to news groups (a kind of automated mailing list) on the Internet; when they find a specified target, they destroy the message. Cancelbots have been unleashed by cyberspace vigilantes who object to "spamming" of the Internet (the despicable practice of sending thousands of identical messages which end up inconveniencing millions of readers) with commercial or religious messages posted in unrelated forums. Unfortunately, cancelbots can equally well be instructed to destroy any other message, thus interfering with freedom of speech.

2.3.2 Denial of Service

Capacity saturation began in the early 1990s in connection with commercial spamming of the Internet. When Canter and Siegel, attorneys from Arizona, sent thousands of messages about the U.S. Dept of Immigration's Green Card Lottery into Usenet groups completely unrelated to such a topic, they angered many thousands of Internet users, many of which have to pay fees as a function of volume and most of which dislike irrelevant materials in their focussed newsgroups. One person from Australia "mail-bombed" Canter and Siegel's Internet address, sending them thousands of large e-mail messages full of abuse. The guilty pair's Internet provider crashed because it couldn't handle the volume.

A similar attack has been perpetrated on bulletin board systems (BBSs) when there are no limits to how many messages can be posted by a single user in a defined period; by automatically uploading hundreds or thousands of messages, a single individual can fill all available message slots or hard disks and prevent other people from uploading their own messages. The volume of useless messages also dilutes the value of the existing message base and drives away legitimate users. If the number of messages is fixed, the new messages can completely replace the old ones, entirely destroying the message base.

Another nasty denial of service attack is possible when repeated logon errors cause an ID to be locked out of a system or network but there are no delays imposed before trying another logon. By logging on to every ID in turn and deliberately entering invalid passwords, a single criminal

hacker equipped with a programmable communications package can shut down access to all but the supervisory IDs on a system.

I mention these simple-minded attacks because they illustrate that people of bad will can far too easily disrupt the work of well-meaning but naive system administrators and users. Although we have been thinking about examples involving Internet groups and BBSs, I invite readers to contemplate the likely effects if the same techniques were to be applied to corporate inventory systems, stock exchange accounts, banking systems, the emergency 911 telephone system, or the systems which generate their own pay cheques.

By the year 2000, distributed denial-of-service (DDoS) attacks were common; they use covertly-installed programs (*zombies* or *slaves*) that listen for coded instructions from a *master* program. Massive DDoS attacks on well-known Web sites such as Amazon.com and eBay.com resulted in so much interference with legitimate traffic that the victims lost millions of dollars in sales and services. Their stocks declined significantly immediately after the attacks.

2.3.3 Physical Disruption

Finally, one can apply physical interference to I.T. Sabotage has been a constant problem for anyone depending on expensive equipment; computers have been struck with axes, bombed, burned, drowned, shot and starved of electricity. These are the kinds of attacks that have concerned military thinkers involved in electronic warfare and countermeasures for years. However, new methods involving electromagnetic interference are causing concern in infowar circles. HERF (high-energy radio-frequency) guns can stop a computer dead at 100 m--or worse, cause mysterious malfunctions or data errors. In terms of productivity, having half a dozen people wasting three hours trying to analyze the peculiar behaviour of a computer is more expensive than simply having the computer stop working.

An extension of the HERF attack is the EMP/T (ElectroMagnetic Pulse Transformer) bomb. This is a device designed to emit high-intensity radiation sufficient to damage modern I.T. equipment. An small, easily concealed EMP/T bomb detonated in a van on a downtown Toronto or Manhattan street could wipe out the stock exchanges, major telephone switches, and countless businesses (the ones without disaster prevention, mitigation and recovery plans). The total damage to the north American economy could greatly exceed the consequences of a physical explosion from a physically-comparable device.

On a more personal level, most airplanes flying today have fly-by-wire systems in which control surfaces are controlled by servo-motors. Instructions to the servo-motors are generated using electronic equipment of great sophistication. Ordinary cellular phones, portable computers, and even hand-held children's video games have been shown to affect some planes' stability, especially during takeoff and landing. Given the ease with which one can manufacture a powerful HERF gun using off-the-shelf electronic equipment (a domestic microwave oven is a start), there is reason to worry that criminals or terrorists stationed outside the security fences will eventually aim one of these devices at a plane landing at an airport.

3 Case Studies of Infowar Techniques (as of 1995)

The following sections will provide readers with some examples of the application of the information warfare techniques to Schwartau's three levels (interpersonal, intercorporate, international) of conflict. Many examples of such attacks are documented in the RISKS Forum Digest, moderated by Dr Peter Neumann of SRI. Readers can subscribe by sending e-mail to

risks-request@csl.sri.com

with the message "SUBSCRIBE."

Another source of up-to-date information is the NCSA FORUM on CompuServe. Use "GO NCSA" for information on this service. Section 2 is dedicated to news and case studies; section 6 deals with disaster recovery; and section 16 deals with operations security (OPSEC) and information warfare. At time of writing (July 1995), participation had reached 35,000 and was climbing by 500 new participants every week.

3.1 Level One: Interpersonal Attacks

Schwartau has spoken and written extensively about the cyberspace shadow and its vulnerabilities. The cyberspace shadow is the model in cyberspace of a person or of an organization; e.g., a person's credit records, medical files in a hospital database, driving records and criminal records--all are aspects of the cyberspace shadow. Harm to the cyberspace shadow falls into three main categories: invasion of privacy, impersonation and character assassination, and harassment.

3.1.1 Invasions of Privacy

Concerns over the invasion of privacy via the cyberspace shadow are many. The Internet's Computer Privacy Digest is a useful source of information about such issues; it is available by electronic mail (e-mail) by sending the e-mail message "subscribe" to its moderator at its comp-privacy-request@uwm.edu address. Government and commercial intrusions into the privacy of individuals is of great interest, but there are also cases of harm from individuals.

Privacy can be invaded in several ways. For example, managers or intruders can snoop through files and e-mail without explicit permission. On government and commercial systems, such snooping may explicitly be sanctioned by employment contracts and procedures manuals, but it nonetheless poses the risk of harming employee relations. Most employees assume that e-mail is as secure (or no more insecure) than postal mail (insultingly called snail mail by the electronic cognoscenti) and are deeply offended when their manager questions their 10 Gb databases of electronic pornography.

On a more prosaic level, market research firms are rabidly pursuing detailed information about individual's patterns of consumption. When one shops at a grocery store that supplies annotated receipts, it is highly unlikely that the data will be discarded; any purchase using a debit card or a

credit card makes it almost certain that the information will be stored and possibly released to market research organizations for analysis. Eventually, it is likely that individuals will received carefully-tailored, computer-generated junk mail configured to precisely their buying habits.

If video stores and book stores store and sell such data--or even allow these data to be stolen--there is a risk of harassment from extreme political and religious fringe groups. How would consumers like to be picketed, bombed or shot for having bought a book or video entitled Especially Offensive Uses of Common Vegetables? Or for that matter, Modern Birth Control or Lyndon Larouche and the Rise of the New American Fascism?

The potential for misuse of medical information is enormous, but in many clinics in Canada and around the world, older sensitive medical information is kept on charts and newer sensitive records are on work stations. The charts are carefully kept in locked filing cabinets, often with stout security bars of stainless steel and one-pound padlocks; in shocking contrast, the computers are completely unprotected by either physical anti-theft devices or by logical access control or encryption software. This situation results from the general level of unawareness of the vulnerability of computer systems to misuse. In one recent case, a male nurse's aide called a patient at home after her hospital stay to invite her on a date; when she demanded to know how he knew her name and phone number, he admitted that he had simply tapped a few keys on the computer at the nearest nursing station on her floor after seeing her in hospital. In Florida in December 1993, two security guards stole computers containing the medical records of 8,000 carriers of HIV, the cause of AIDS. Luckily, the thieves did not try to extort money from these people--no thanks to the inadequate security at their clinic.

3.1.2 Impersonation and Character Assassination

Another key issue in Level One infowar is identity and anonymity in cyberspace. In a previous paragraph, we saw that breaches of privacy can occur when identity is too easily obtained (e.g., personalized records of purchases). However, anonymity and pseudonymity (the use of a false identity or of someone else s identity) are serious questions. In a recent case reported in the NCSA Forum on the 2.5-million user CompuServe network (GO NCSA), a university student waited four months to open the envelope from his university computer centre containing his new Internet account and password. Unfortunately someone else deduced his password (first initial, middle initial, and start of his last name!) before he opened the envelope and sent hundreds of obscene and racist messages to faculty, students and strangers with predictable results to the naive user's reputation.

Internet e-mail includes its routing information (sender, date/time stamps, systems through which the message is forwarded) as ASCII headers placed at the start of the message, anyone with access to the e-mail messages can alter those headers. A foolish university student sent a death threat via e-mail to President Clinton; despite his attempts to disguise the origins of his message, he was arrested a few days later after some fairly easy detective work by the FBI and the Secret Service. Nonetheless, without using digital signatures and message digests (techniques for creating unique sequences that unarguably prove the identity of the sender and the integrity of

the message received) as a normal component of electronic communications, these cases of fraudulent identity will continue.

Winn Schwartau himself nearly had his reputation ruined a few months ago when someone used his logon on The Well, a popular network based in San Francisco, and sent out nasty and vulgar attacks on a criminal hacker. Grady Blount, a professor at Texas A&M University required police protection and had to move his classes to different locations after a criminal hacker stole his electronic identity and sent out thousands of hateful messages under the professor's name attacking various ethnic groups. In the real world, individuals have suffered for years after thieves obtained their social insurance numbers and credit records to order credit cards in the victim's name; the thieves rack up hundreds of thousands of dollars of purchase and then default on their payments, leaving the original owner of the electronic identity to pick up the bill--and the court cases, ruined reputations and even family breakup.

Some politicians have suggested that they'd like to receive e-mail as a method of gauging public support for or opposition to various political initiatives. The obvious question is whether political judgements should be based on opinions sent by a currently tiny minority of the population--those with access to e-mail. But even apart from this problem of bias, without reliable identification and authentication, individuals and hostile agents could easily sway gullible politicians into perceiving a warped vision of reality simply by using computers to generate tides of fraudulent but realistic opinions. Science fiction author Orson Scott Card imagined just this mechanism for distorting the political process in his novel, *Xenocide.*

3.1.3 Harassment

Other ways of causing problems for individuals have been documented and qualify as Level One infowar:

- For example, Kevin Mitnick is accused of having caused someone he disliked to be invoiced for an entire hospital's phone bill.

- A church's phone was reputedly call-forwarded to a 900 sex line.

- A person accused of spamming the Internet found his company's 800 number listed as a phone-sex line in various alt.sex groups on the Internet, resulting not only in thousands of dollars of charges to his company but personal humiliation when the receptionists refused to put up with any more of the heavy-breathing callers and sent them all to his own phone extension.

- In another case of Level One harassment discussed at a criminal hacker convention in December 1993, a poor soul found that a criminal hacker had used a war dialer (a program for automatically dialling phone numbers in sequence) and had left the victim's phone number on thousands of pager accounts. The innocent pager users were irritated at having made a call for nothing, but the victim's life was made untenable for a day.

- Finally, in a recent case in Toronto, a night auditor in a commercial centre obtained computer records for 28,000 credit-card transactions from January 1989 to May 1994. Using these data, the criminal, working with dishonest business confederates, generated phony transactions and shared the proceeds, amounting to C$1.5 million.

3.2 Level Two InfoWar

At the intercorporate level, infowar consists of industrial espionage, theft, and sabotage.

3.2.1 Espionage

Espionage is not new, but electronic systems make it much easier than in the days of breaking-and-entry and tiny cameras. American Airlines, for example, is reported to have been upset when valuable tables showing the expected rate of no-shows for each of its flights in North America were allegedly stolen on diskettes and given to Northwest Airlines. Such data leakage will become more common unless organizations implement effective policies for improving security awareness and monitoring compliance with written security policies.

Another interesting example of data leakage occurred in Australia, where dishonest employees sold information to unscrupulous accountants showing how the department of revenue chose its candidates for financial audits.

Encyclopedia Britannica lost control of 3,000,000 names of subscribers and prospects, conservatively evaluated at $1,000,000 in assets; the culprits were employees in the data processing department.

Companies have been caught hiring moles in rival organizations and sending out information via electronic mail; Symantec and Borland, two well-known software companies from the West Coast of the U.S., battled each other in court over one such case. In 1992, Eugene Wang, a VP at Borland International Inc., allegedly sent his future employer, Symantec Corp. CEO Gordon E. Eubanks e-mail containing confidential Borland data. The case was dismissed in August 1993 by the Superior Court in Santa Cruz county, California, when the judge discovered that Symantec had paid some U$13,000 in expenses incurred by the public prosecutor's office.

In this world of sharp competitive advantages, a single diskette holding a thousand pages of information can slip away in a vest pocket or a purse and be worth millions to a competitor. General Motors' Opel division is embroiled in a legal battle with Volkswagen over information allegedly spirited from Opel to VW by Jose Ignacio Lopez de Arriortua, a senior executive upon being hired away from Opel. Three crates of confidential VW information were allegedly discovered at his apartment by German police investigators. The accusations continue.

3.2.2 Theft

The theft of telephone services is estimated to be reaching $8 billion in North America alone. Young criminals have been found scanning for codes by using binoculars in airports and train stations; there are telephone boxes in some cities where people line up to pay $3 for 10 minutes of long-distance calls anywhere in the world--and individuals or companies pay the bill. Some criminal phone phreaks have invaded voice-mail systems, illegally setting up their own voice-mail boxes for personal use. Another kind of theft recently occurred in Germany, where two employees placed microcomputers in a switching centre and placed thousands of calls to 1-900-SEX lines in the Caribbean. Charges were randomly allocated to clients all over Germany, and the phone company had to pay tens of thousands of dollars to the overseas aural sex operations. The criminals in Germany then received part of the illegal profits from the sex-line operators in return for their nefarious deeds.

In case reported in October 1994, a ring of criminal hackers operating in the United States, England and Spain stole the telephone calling card numbers of 140,000 subscribers of AT&T Corp, GTE Corp, Bell Atlantic and MCI Communications Corp. These thefts are estimated to have resulted in U$140 million of fraudulent long distance calls. In a significant detail, Ivy James Lay, a switch engineer working for MCI, was known in criminal hacker circles as “Knight Shadow.” He is accused of having inserted Trojan horse software to record calling-card and ordinary credit-card numbers passing through MCI's telephone switching equipment. European confederates, led by 22-year old Max Louarn, of Majorca, Spain, paid him for the stolen data, then set up elaborate call centres through which users could make overseas calls. This is one of the most obvious cases where young but experienced criminal hackers appear to have planned a Level Two attack on major corporations.

Another example of Level Two theft occurred in Hartford, Connecticut in April 1993. A new automated teller machine (ATM) was installed in a suburban mall. It functioned acceptably at first, but soon began behaving peculiarly. It would accept a user’s card, ask for the personal identification number (PIN), and then announce that it was out of order, suggesting the user switch to a nearby ATM. This was an elaborate spoof, and the criminals who installed the ATM used the card numbers and PINs their machine had recorded to create bogus ATM cards. They stole over $100,000 in three weeks but were eventually caught because they didn’t realize that their picture was being recorded on video at the many ATMs where they used their fake cards. Diligent cross-matching by the police showed that all the fraudulent transactions were associated with withdrawals by the same people and so the criminals were defeated.

The latest spectacular ATM attack occurred between Friday the 18th and Monday the 21st of November 1994 in and around Portland, Oregon. Two thieves stole a bank card from a purse left in a locked van in a suburb; the owner had unfortunately written her PIN on her Social Security card. The thieves used the stolen card within minutes at an ATM a few blocks away and retrieved the daily maximum--U$200. By what may have been a stroke of luck, the daily limit did not apply that weekend, for the Oregon TelCo Credit Union was in the midst of upgrading its ATM software. The thieves were able to “jackpot” 48 bank machines in 724 withdrawals over the next 54 hours, stealing U$346,770 in all. They occasionally fed empty envelopes into the ATMs, claiming to have deposited a total of U$820,500 into the victim’s account--and again, the bank software failed to block the fraudulent deposits as it should have. Four suspects were

arrested within days of the spree, but why the bank software should have been so easy to dupe is still not explained.

3.2.3 Sabotage

In the late 1980s, a New Jersey magazine publisher began receiving complaints from its customers. Voice mail messages renewing valuable and important advertising had never been heeded. Employees claimed they never received the calls at all, and the voice-mail system supplier was called in for technical support. Investigation showed everything normal, suggesting the dreaded intermittent problem. However, customers began reporting a problem which could not be accounted for by defective software or hardware: outgoing messages had been altered to include rude and sometimes lewd language and suggestions. Attention shifted to inbound calls. In a short time, investigation showed that someone was interfering with the phone system, re-recording employees' welcome messages and deleting inbound messages from clients. The culprits proved to be a 14-year old and his 17-year old cousin, both residents of Staten Island.

Why did the youngsters attack the publisher's voice mail system? It seems that the younger had ordered a subscription to a magazine dedicated to Nintendo games (don't laugh, it's no weirder than magazines about home decoration). The magazine subscription offer included a colourful poster normally costing U$5. The magazine arrived; the poster didn't. The youngsters phoned the company, were assured they'd receive the poster, and waited. No poster. So they entered the company's voice mail, cracked the maintenance account codes and took over the system. Their shenanigans resulted in lost revenue, loss of good will, loss of customers, expenses for time and materials from the switch vendor, and wasted time and effort by the publisher's technical staff. Total cost (admittedly, estimated by the victim): U$2.1 million.

However, sabotage is by no means the purview of teenagers.

A plumber in Philadelphia was arrested in January 1995 and accused of having arranged for the local phone company to install call-forwarding on several phone lines. All the calls to these numbers were duly forwarded to the plumber's office. Unfortunately, the calls were intended for several of his competitors; he and his staff skimmed the profitable cases from the influx of calls from his competitors' clients and refused service or were rude to the rest, damaging his competitors' reputations. After a few weeks, a happy client called her plumber to thank him for having repaired a pipe over the Christmas holidays; he, of course, had no record of having worked over the holidays, and after a short investigation, the criminal scam was discovered and the perpetrators arrested.

In a Washington, D.C. area office of the Bureau of Mines of the U.S. Department of the Interior, someone destroyed the data on hard disk drives of 19 microcomputers and stole two more. The incident occurred on Friday, August 12, 1994 around 18:30. The saboteur set up the instructions for formatting all 19 systems, then walked through the installation pressing the ENTER key on all the machines. The damage was complete within 15 minutes. Ironically, it appears that the criminal may have performed a dry run a week before, when two systems were inexplicably found formatted. After this incident, a few workers heeded security specialists' warnings that

they should use access-control software with good passwords on their machines, but most did not. Those who passworded their computers were not hurt by the sabotage. Luckily for the Bureau, the culprit did not know enough about computers to overwrite the hard disks, and so technicians were able to salvage most of the data using disk utilities to undo the formatting.

In a recent application of HERF techniques for sabotage, a spectator was arrested for allegedly causing the crash of several large model airplanes at the Medeira races in Spain in the autumn of 1994. According to a report published in Schwartau's Security Insider Report, the accused "was using a frequency scanner to find what frequency the flier was using, then swapped the crystal of his own transmitter to match, thus causing the plane to lose control and in most cashes crash.... Just to add a bit of perspective, these planes cost upwards of $10,000 and travel at well over 100 mph. The impact energy is about three times that of a .45 bullet. I don't think there were any injuries, but there very easily could have been, to any of the thousands of spectators...."

4 Level III Infowar

Previous articles on "Economic Espionage" by Samuel Porteous in *Commentary* number 32 (May 1993) and number 46 (July 1994) discuss how governments all over the world have supported a wide range of open and clandestine espionage designed to confer benefits on national enterprises. Mr Porteous has also recently published a summary of this situation in *Intelligence and National Security* 9(4):735-752 (October 1994).

Government involvement need not be limited to espionage, however. In July 1985, two officers of the French intelligence service killed a photographer when they blew up and sank the Rainbow Warrior, a ship owned and operated by the environmental group Greenpeace, while it was in port in Auckland, New Zealand. If governments are willing to resort to this kind of action, what could possibly impede them from any other tactic, especially when it might be even harder to trace the originators? Level Three information warfare attacks could involve immediate attacks causing serious damage or insidious attacks with even more serious consequences.

4.1 Immediate Attacks

- Civil aviation: interference with control towers, radio communications, and even the avionics of commercial aircraft would paralyze huge sectors of an economy. In North America, even fog at O'Hare International Airport in Chicago or Pearson Airport in Toronto can cause repercussions to spread over the entire continent. Delays in air transport would not merely inconvenience holiday travellers or lead to cancellations at hotels and resorts; they could also interfere with business meetings, cause manufacturing slowdowns, increase congestion on land routes, and, as always, affect the stock market.

- The phone grid: when the 911 system goes down, there can be chaos. Emergency calls for medical help, fire services, or police action can go unanswered for long periods,

leading to danger or social disorder. When the regular phone system fails, even for an hour, the economic consequences merely from the impossibility of completing credit card transactions can range into the millions of dollars. If a single determined criminal hacker was able to infiltrate the MCI switch in Cary, North Carolina (see above) to steal telephone codes, there is nothing to stop a trained information warfare specialist to do the same for more insidious purposes.

- National and international banking systems and stock markets depend on the unimpeded and timely flow of accurate information. The slightest perturbation in such systems could have catastrophic consequences for the world monetary and financial systems. Mexico's currency devalued by about half over a few weeks simply because of uncertainty over the country's stability; Canada may experience the same phenomenon as the debate over the secession of Quebec continues. If a foreign nation were to want to destabilize a country, interfering with the monetary networks and stock markets would be an excellent way to do so. Feeding incorrect information into the networks, deleting transactions, even spreading rumours through the Internet could cause more damage--untraceably--than bombing a building.

4.2 Insidious Attacks

As Schwartau has frequently pointed out, destroying things in an obvious way has immediate effects; however, at least the victim recognizes the problem. Once the bomb goes off, we can start repairing the damage. The really nasty attacks are the ones we don't recognize.

In his novel, *Terminal Compromise,* Schwartau explores several techniques that would be useful in Level Three information warfare. For example, he envisages viruses with long latency; that is, self-reproducing programs which do no damage for quite a long time, allowing them to spread invisibly throughout a nation's computers. Information warfare viruses, being written by serious operatives instead of by neurotics, could have insidious payloads; for example, they could subtly alter data in spreadsheets, making changes of, say, a few percent in random cells. The confusion and disruption caused by such errors would be far worse than the outright crash of a program; people would spend countless hours trying to find the errors in their (usually undocumented) spreadsheets--or suffer the consequences of incorrect budget estimates, erroneous engineering calculations, and impossible predictions from numerical models.

It would be possible to introduce errors into much of the commercial software produced in a specific country; for the U.S., for example, just arrange to infiltrate agents into Microsoft and Computer Associates (firms which produce enormous amounts of software). Even with the best will in the world, no one can stop all accidental errors; how much more difficult, then, to catch errors deliberately concealed by malicious programmers.

Another approach to ruining a specific economy would be to distribute hardware deliberately engineered to cause problems--the Pentium chip on purpose. The Pentium chip debacle occurred when Intel, maker of the 80x86 series of microprocessors used in several generations of IBM-PC compatible microcomputers, failed to notice errors in the design of their newest chip. It made mistakes in certain floating-point divisions. Unfortunately for everyone, the maker failed to announce this error publicly, and there was a brouhaha when the bug was discovered. Now imagine a foreign government arranging to plant agents in the laboratories of major hardware and software manufacturers. After a few instances of catastrophically bungled programs or chips are discovered, the reputation of an entire industry can be damaged for a long time. Even the rumour of such problems could cause disruption, loss of productivity, and international trade imbalances.

5 Discussion: Civil Defence in Cyberspace

With every advance in technology comes new vulnerabilities to attack. Civil defence contingency planning currently pays attention to preventing and recovering from damage to the physical infrastructure of society. With the growing dependence upon information technology in our complex civilizations, we must hasten to include cyberspace in our concerns.

As this article has shown, there are many ways to harm the interests of individuals, organizationa and nations using the new weapons of information warfare. To strengthen our collective resistance to such threats, we should work at many levels to bring information technology and its protection into our personal, corporate and political discourse. The following suggestions will serve as a starting point and are discussed below:

- Raise individual awareness of privacy and security in cyberspace
- Raise corporate commitment to information security
- Expand fundamental orientation of risk management
- Increase military education and planning for information warfare
- Encourage cooperation between military and civil authorities
- Set national priorities to include information security
- Encourage mandatory reporting of information system attacks and failures
- Establish international agreements on jurisdiction over attacks in cyberspace

5.1 Raise Individual Awareness of Privacy and Security in Cyberspace

Some attacks in cyberspace come from relatively young people. Some children and especially teenagers find computer crime attractive because it expresses their natural tendency to rebel against adult norms, enhances their sense of affiliation with a group, emphasizes intelligence and technical skill, and can be lucrative. In addition, most parents know little about the activities of their children in cyberspace

Although there are already successful efforts in the K-12 school systems, we should collectively expand the availability of good-quality training and awareness materials for children in our educational system. For the youngest children, awareness of the social norms already evolving in cyberspace can be taught in entertaining and memorable wasys; for example, Gale Warshawsky of the Lawrence Livermore National Laboratory in the United States has created a group of charming puppet characters who introduce very young children to concepts of information privacy, data integrity and even viruses.

At the Reconstructionist Synagogue of Montreal, the congregation invited me to speak on Ethics in Cyberspace in May 1995. The program was directed to children and their parents and includes videos and discussion about the problems caused by breaches of security. Parents and children received a checklist of questions suitable for family discussion:

National Computer Security Association

Ten Questions Parents Should Ask Their Children

A. Respect for intellectual property rights

1. Do you legitimately own all of the software, games, and programs you have or use?

2. Where did the contents of your report / project / homework come from -- does any of it belong to someone else? Did you write/create/author what you're passing off as your own work? Where did you get the text and images you're using? If you copied text and images from another source, did you have permission? If you didn't need permission from the "owners" of the information you're using, did you credit them for the material?

B. Respect for other people's property rights

3. Do you ever use other people's computer, disk-space or processing capability, or look at or copy their files or information, without their knowledge or permission?

4. Do you have any prank programs, computer viruses, worms, trojan horse programs, bombs, or other malicious software?

C. Respect for social values

5. Do you have any computer graphics files, clips, movies, animations or drawings that you would be embarrassed about? Do you have them legitimately? Are they things you would be comfortable showing me? Showing your grandmother? Do you have any pictures, video clips, sound clips, articles, text, or other software or files which contain pornography, violence, dangerous instructions other distasteful material? Do you access or view any of these kinds of things when using the net?

6. Do you have any newsletters, plans, guidelines, or "how-to" documents or files that you would not be comfortable showing to your mother? For instance, making bombs, breaking into systems, stealing telephone access, stealing computer access, stealing passwords, pornographic or violent text, guides, descriptions? Do you create, contribute to or receive anything like this?

D. Questions related to network use

7. Do you ever connect your computer to a telephone, use a modem, or otherwise use a network?

   If so, consider the following questions:

8. With whom do you associate when you use the Net? Tell me about your contacts.

9. Do you ever use an assumed name, a handle, or an alias instead of your real name? Do you supply a false information about yourself when using a bulletin board, a news group, a message group, or forum, any part of the net, or when using e-mail or when otherwise communicating? Do you use your real age & sex when communicating with your computer? Do you use any false information such as a fake addresses or phone numbers or use someone else's credit card number when using your computer? Do you ever send messages or e-mail in such a way that the recipient cannot tell that you sent it? Have you ever modified data, text, messages, or other computer information so that it looks like someone other than you created it or made the changes? What are you trying to hide by not using your real name? Are you trying to pretend you are something or someone you are not?

10. Do you use telephone, video, cable-TV, computer network, bulletin board, or other network services without paying for them?

5.2 Raise Corporate Commitment to Information Security and Ethics

In a recent survey (Computerworld 95.03.20, p.16; reporting on Susan J. Harrington's article, “Computer Crime & Abuse by IS Employees” in the March/April 1995 issue of the Association for Systems Management's *Journal of Systems Management*) of more than 200 programmers and other information technology professionals at nine Ohio-based manufacturing and service

companies, 41% admitted that they would illegally copy software for themselves or a friend, 7% would adjust a bank account system to avoid incurring a service, and 10% saw nothing wrong with sending a virus program that would output the message, “Have a nice day.”

With this level of ethical commitment in the workplace, it is no wonder there are growing problems of industrial espionage and sabotage.

One solution is to apply the same methods used to change corporate culture in the TQM (Total Quality Management) movement. Clear mandates from upper management, backed by appropriate investment in awareness and training, are crucial elements in the defence against information warfare. Robert Hauptman of St.Cloud University in Minnesota is editor of the *Journal of Information Ethics;* in a recent article (“Doing Business Online: Add Ethics To The Agenda” in *InfoWeek* 95.02.06, p. 64), he argues, “It's time to stop accepting illegal activity as the normal price of doing business in Cyberspace.” Organizations must identify specific examples of illegal and unethical behaviour, define sanctions against perpetrators, monitor compliance, and apply appropriate punishment, including dismissal. Incidentally, it would be a good idea to establish sound security precautions *before* firing people for unethical behaviour....

5.3 Expand Fundamental Orientation of Risk Management

Threat and risk assessment has traditionally dealt with the probability of Acts of God. Fire, flood, earthquake, even burglary can be looked at as involving random events. However, in today’s competitive and unethical environment, the likelihood of being attacked is an unknown and unknowable function of an organization’s attractiveness and preparedness. The most successful and least secure organizations will be victim. Faced with a choice between an unkempt hovel and a palatial residence, a thief will try to rob the more lucrative target. But suppose a thief sees two palatial residences: one has Doberperson Pinchpersons (politically correct guard dogs) roaming the space inside a 3 meter fence, infrared motion detectors and a direct link to a security company; the other has locks on the doors. There’s not much doubt about the selected victim.

In my courses, I like to explain the principle of appropriate defence with a story. Two hikers are walking happily along a trail in Alberta when they come upon a huge grizzly bear. Turning tail, they being running down the trail. One huffs to the other, “This is (pant, gasp) crazy. We can’t outrun a grizzly bear! They can run 30 km an hour and climb trees!” The other gasps, “I don’t have to outrun the grizzly bear (pant, pant). I just have to outrun *you.*”

Organizations must make themselves unattractive targets for espionage and sabotage.

5.4 Increase Military Education and Planning for Information Warfare

The United States National Defense University already has programs in Information Warfare. Canada and other countries should follow suit. Officer training should include a thorough grounding not only in classical military applications of information technology but also in the symptoms of information warfare attacks. Computer countermeasures such as anti-virus precautions, proper quality assurance standards during software development, and anti-penetration techniques should be taught with a conscious awareness of how military systems could be compromised using information technology. Even off-the-shelf software or systems written by consultants could be conduits for information warfare attacks. The military must learn about these threats and be prepared to counter them.

5.5 Encourage Cooperation Between Military and Civil Authorities

Just as emergency preparedness in the world of bridges and roads naturally involves close cooperation between civilian and military authorities, so should emergency preparedness in the world of gateways and networks. Each level of government, each sector and department, should have its Computer Emergency Response Teams (CERTs). These CERTs should cooperate at every level, sharing information and techniques, coordinating their efforts to prevent widening rings of damage from information warfare attacks, and working effectively with their military counterparts.

Winn Schwartau was a guest of honour at the Second International Conference on Information Warfare in Montreal in January 1995. As he wrote in the January 1995 issue of *Security Insider Report,* he chatted with several military officers at the conference. "If Qaddafi (Libya) blew up the Statue of Liberty, what would our response be?" His interlocutors said, "We would... ah, respond." Schwartau went on to question them about escalating levels of attack and then asked, "Let's say that Qaddafi hacked his way into a US computer system and broke it. That is, a complete denial of service. Then what?" The military officers were less certain: "We would probably respond, maybe militarily, but that is a real policy choice." Finally, Schwartau asked, "Fine. Now let's say that the French did the same thing. They hack their way into our financial computers, and as a result, we suffer a major bank collapse. Does that event trigger a military intervention or response?" Apparently the officers were taken aback at this scenario.

Military thinking must include a thorough understanding of all the ways that a foreign enemy can harm a country. And that means understanding the value and vulnerability of civilian information technology. I would like to see military specialists in information warfare taking time to work in commerce, industry and government to gain hands-on knowledge of the role of information technology. I would like to see civilian information technology specialists, including especially technical and managerial employees from telecommunications companies, encouraged to participate in a new kind of military reserve: a Computer Corps specializing in detecting and correcting deliberate damage to information systems, whether military or civilian. I would like to see civilian police authorities cooperating with CERTs and the military Computer

Corps to strength the nation's defences against deliberate attack on the information infrastructure of our society.

5.6 Set National Priorities to Include Information Security

Robert David Steele, another keynote speaker at the Information Warfare Conference last January [1995], has spoken out forcefully on the need for national governments to pay attention to information security. Mr Steele is President of Open Source Solutions, Inc. (Oakton, VA) and has been working on a convincing the government of the United States to establish what he calls a National Information Strategy. His draft proposal presented to the Senate of the U.S. includes the following key points:

- National Information Strategy to be coordinated by the President of the U.S.
- Chief Information Officers to be appointed for federal government and every state.
- National Information Foundation to report to the Chief Information Officer of the U.S.

His proposal includes the following paragraph:

> C4 (Command & Control, Communications and Computer) Security. The substantive elements of this program--connectivity, content and coordination--are all heavily dependent on a relatively fragile national C4 infrastructure. It is the intent of this Act to ensure that all civil communications and computing pathways, including our financial, health care, governance, public information, and defense pathways, are developed in such a way as to maximize their survivability and reliability in the face of attacks by individuals, groups and hostile nations familiar with the critical vulnerabilities of our civil and military C4 infrastructure.

5.7 Encourage Mandatory Reporting of Information System Attacks and Failures

We currently lack a clear picture of the state of information technology security in government, industry and private life. As part of a nascent national information strategy, all organizations should share details of every compromise of system security they experience. There should be mandatory reporting coupled with strict protection of sources; a government organization, law enforcement authority, or quasi-autonomous non-governmental organization should receive reports of data leakage, virus attacks, programmatic damage, eavesdropping and electromagnetic interference. It would be impossible and unnecessary to try to force individuals to report their experiences with home computers, but such reports should be encouraged. The agency entrusted with such reports must maintain strict controls over the data to prevent damage to the organizations reporting their own victimization; data could reasonably be anonymized at the time of entry to preclude even inadvertent disclosure of embarrassing details. However, such a national database of computer incidents would be invaluable in evaluating which security measures work and which don't work. With a growing database of knowledge, it should be possible to improve security measures and also to provide hard evidence and case studies to help convince managers to pay attention to security.

5.8 Establish International Agreements on Jurisdiction Over Attacks in Cyberspace

Finally, a systematic effort similar to the Law of the Sea process must be established to define multinational agreements covering computer crimes. Jurisdiction over computer crimes should rest with the federal authorities in the country where the victimized systems are physically located; extradition should be enforced by the authorities where the accused perpetrator has been arrested. Standards of evidence will have to be established; for example, norms for accepting and safeguarding digital evidence will have to be uniform across cooperating jurisdictions. Telecommunications carriers and international value-added networks will play important roles in such cooperation and must be included in the process of policy development.

6 Concluding Remarks

With every development in technology has come new forms of crime and of war. As we move into the twenty-first century, we must take the growing dimensions of cyberspace into account in our defensive strategies as individuals, as members of organizations, and as citizens. With our rapidly growing use of cyberspace, we will experience growing conflict over values: norms that evolved in the world of mail, newspapers and television will collide with those from the world of electronic messaging, newsgroups and multiuser dimensions. As in all human arenas, some of the norms evolving in cyberspace seem to have their roots in alienation and sociopathy. We can hope to protect ourselves in the future not only by countering attacks but by reducing the frequency of such attacks. It is time for society to discuss, determine and express collective values in cyberspace.

Chapter Notes

1. Most of these titles are available from the NCSA in Carlisle, PA (call 717-258-1816):

   Bologna, J. (1993). *Handbook on Corporate Fraud: Prevention, Detection, Investigation.* Butterworth-Heinemann (Boston). ISBN 0-7506-9243-X. xii + 308. Index.

   Card, O. S. (1991). *Xenocide.* Tor Books / Tom Doherty Associates (New York). ISBN 0-812-50925-0. xiii + 592.

   Cheswick, W. & S. Bellovin (1994). *Firewalls and Internet Security: Repelling the Wily Hacker.* Addison Wesley (Reading, MA). ISBN 0-201-63357-4. xiv + 306. Index.

   Haugh, J. J. R. E. Burney, G. L. Dean & L. H. Tisch (1992). *Toll Fraud and Telabuse: A Multibillion Dollar National Problem.* Telecommunications Advisors Inc (Portland, OR). ISBN 0-9632634-2-0. 399 + 431 pp.

   Hafner, K. & J. Markoff (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier.* Simon & Schuster (New York). ISBN 0-671-68322-5. 368 pp. Index.

   Schwartau, W. (ongoing). *Security Insider Report.* Monthly newsletter on infosec and the computer underground. Inter.Pact, Inc. / 11511 Pine St. N. / Seminole, FL 34642. Tel. 813-393-6600.

   Schwartau, W. (1994). *Information Warfare: Chaos on the Electronic Superhighway.* Thunder's Mouth Press, New York. ISBN 1-56025-080-1. 432. Index.

   Schwartau, W. (1991). *Terminal Compromise* (novel). Inter.Pact Press (Seminole, FL). ISBN 0-962-87000-5. 562 pp. Available as shareware on a disk as well as in print.

   Toffler, A. & H.Toffler (1993). *War and Anti-War: Survival at the Dawn of the 21st Century.* Little, Brown and Company, Boston. ISBN 0-316-85024-1. xiii + 302. Index.

   Stallings, W. (1995). *Network and Internetwork Security: Principles and Practice.* Prentice Hall (Englewood Cliffs, NJ). ISBN 0-02-415483-0. xiii + 462. Index.

2. Internet news group c4i-pro
   The c4i-pro (C4I Professionals) mailing list covers topics of interest to those following developments in information warfare. Here is the list description:
   This mailing list was created for use by anyone interested or involved in the area of Command, Control, Communications, Computers and Intelligence (C4I). Its purpose is to serve as a central point or clearinghouse for (unclassified/non-sensitive) information and activities of interest to members of the C4I professional community. This includes military and government civilian members (both in operational, acquisition and policy

positions), C4I contractors and members of the academic community worldwide. Topics of discussion are envisioned to include:

Conference/meeting announcements
Exercise announcements (e.g. JWID)
Lists of C4I resources on the net
C4I thesis ideas and proposals
C4I lessons learned
Generic discussion on such C4I topics as:
- C4I theory
- C4I systems design and acquisition
- C4I system models and simulations
- Information technology security and protection
- C3 countermeasures
- Current C4I topics and issues
- Space and Electronic Warfare (SEW)
- Information Warfare/C2 Warfare
- Cyberwar and Netwar
- C4I equipment effectiveness

The c4i-pro list is managed by students and faculty of the Naval Postgraduate School's (NPS) Joint C4I Systems curriculum. The NPS is the U.S. Navy's graduate education university. More than 1800 students from all four U.S. Services and over 40 countries are studying for graduate degrees in a variety of curricula. The Joint C4I Systems curriculum provides U.S. students from all four services the opportunity to obtain a masters of science degree in systems technology. For more information on the NPS or the C4I curriculum, see our WWW home page described below or contact Ernie Beran at eberan@nps.navy.mil or Dan Boger at dcboger@nps.navy.mil.

To subscribe to the list, send e-mail to majordomo@stl.nps.navy.mil with the single-line message

subscribe c4i-pro <your e-mail address>

where < and > are not included in the message. Thus I subscribed using

subscribe c4i-pro 75300.3232@compuserve.com

3. Information warfare reading list.

Lt. Robert Garigue of the Canadian Department of National Defence published a reading list on information warfare in the c4i-pro news group. It provides a wealth of further reading and I have reprinted it here as published.

Date: Tue, 21 Mar 95 21:00:22 +0000
From: garigue@ncs.dnd.ca
To: 75300.3232@compuserve.com, c4i-pro@stl.nps.navy.mil
Subject: IW Bibliography - public sources

As there has been quite a debate as to the definition of IW I submit to the group the small bibliography that I have put together on the subject. They are all from open sources so there is not problem debating the definitions that are found in these documents. You will rapidly realise that there is no such thing as a final definition about something that Karl Popper would clearly class as a world 3 "construct".

If any one wants to add to the biblio send me a note of your documentation or thesis.

This could go into a FAQ

INFORMATION WARFARE - BIBLIOGRAPHY
March 9/95

Advance Planning Briefing for Industry, "Winning the Information War", United States Army Communications-Electronics Command, Fort Monmouth, New Jersey. Symposium held May 11-12, 1994, Ocean Place Hilton Resort and Spa, Agenda and Description of Sessions, 10 pages.

Arquilla, John and Ronfeldt, David, "Cyberwar is Coming!", Article copyrighted 1993 by Taylor & Francis, Bristol, PA, originally published in the Journal Comparative Strategy, Volume 12, no. 2, pp.141-165.

Busey IV, Adm. James B., USN (Ret.), "Information Warfare Calculus Mandates Protective Actions", Presidents Commentary, Signal, October 1994, Official Publication of AFCEA, p.15.

Cook, Lt. Col. Wyatt C., "Information Warfare: A New Dimension in the Application of Air and Space Power", 1994 CJCS Strategy Essay Writing Contest Entry, Lt., 37 pages.

Defense Information Systems Agency, "Defensive Information Warfare (DIW) Management Plan", 15 August 1994, Version l.2, 4 sections and Appendices.

DeLanda, Manuel, "War in the age of Intelligent Machines", Zone Books Swerve edition New York 1991

FitzGerald, Mary C., "Russian Views on Information Warfare", Army, Vol. 44, No. 5, May 1994, pp.57-60.

Franks, Frederick M.. Jr., "Winning the Information War: Evolution and Revolution", Speech delivered at the Association of the US Army Symposium, Orlando, Florida, February 8, 1994, Copyright City News Publishing Company Inc., 1994, 11 pages.

Garigue, Robert. "On Strategy, Decisions and the Evolution of Information Systems". Technical Document. DSIS DND Goverment of Canada.1992

Information Society Journal The, Volume 8, Number 1, 1992, Published Quarterly by Taylor & Francis, Printed by Burgess Science Press, Basingstoke, England.

Johnson, Craig L., "Information Warfare - Not a Paper War", Special Report, Journal of Electronic Defense, August '94, pp.55-58.

Johnson, Frederick C and Painter, Floyd C., "The Integration of Warfare Support Functions", Technology Analysis, Warfare Integration, C31:1988, pp.176-182

Kelly AFB, Tex., "EW Expands Into Information Warfare", Electronic Warfare, Aviation Week & Space Technology/October 10, 1994, pp.47-48.

Lum, Zachary A.,"Linking the Senses", Journal of Electronic Defense, August '94, pp.33-38.

Luoma, William M., "Netwar: The Other Side of Information Warfare", 8 February 1994, A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations, 42 pages.

Roos, John G., "Info Tech Info Power", Armed Forces Journal International, June 1994, pp.31-36.

Science Application International Corporation (SAIC), "Planning Considerations for Defensive Information Warfare - Information Assurance -", 16 December 1993, 61 pages.

Sovereign, Michael G. and Sweet, Ricki Dr., "Evaluating Command and Control: A Modular Structure", Technology Analysis, Evaluating C2, C:31 1988, pp.-156-161.

Schwartau, Winn. "Information Warfare - Chaos on the electronic superhighway " Thunder's Mouth Press, New york . 1994

Toffler Alvin & Heiddi "War and Anti War" 1992

//----------
// Robert Garigue |garigue@dgs.dnd.ca
// Strategic Information Technology Specialist |Vox 1 613 992 6855
// Office of the Assistant Deputy Minister-DIS |Fax 1 613 992 1469
// Department of National Defence

4. NCSA Information Warfare Conferences

The National Computer Security Association sponsors an annual International Conference on Information Warfare. The First was held in Montreal, September 15, 1993; the Second, in Montreal January 18-19, 1995; the third, in Washington, DC on 6-8 September 1995. The complete Call for Participation for the Third International Conference as published on the Internet follows:

From: <winn@Infowar.Com>
Date: Wed, 28 Jun 1995 13:37:24 -0400
Subject: IW 95

InfoWarCon '95
Third International Information Warfare Conference
Confronting Chaos in Cyberspace
Personal, Corporate and National Perspectives
Schedule: June 26, 1995
Sheraton Stouffer's, Arlington, VA

Sponsored By:
National Computer Security Association
Winn Schwartau, INFORMATION WARFARE, Interpact, Inc.
Robert Steele, President, Open Source Solutions, Inc.

Wednesday, September 6, 1995
Registration and Cocktail Reception: (Casual) 17:00-20:00

DAY I: Thursday, September 7, 1995

7:00 - 7:45 Continental Breakfast Sponsored by IBM, Corp.
7:45 - 8:00 Introductory Remarks: Peter Tippett, President, NCSA
8:00 - 8:30 Keynote Address
Speaker of the House, Newt Gingrich (Invited)

"What Is Information Warfare?"

The morning's discussions will be moderated by Information Resources Management College, School of Information Warfare & Strategy, National Defense University. There is no consensus as to what Information Warfare means; everyone has a different definition and application which often suits specific agendas. The morning sessions are to provide attendees with a current review of what Information Warfare means to different people.

8:30 - 9:00 "Threat Analysis: The Intelligence Perspective",
Admiral William Studeman, Asst. Director, Central Intelligence

9:00-9:30 "The Government Perspective"

How does the government view Information Warfare as the NII and GII become realities? Increasing reliance on technology brings new risks and vulnerabilities along with opportunities. What plans are in place to insure American competitiveness?
- Bruce McConnel, Office of Management and Budget (Invited)

9:30 - 10:00 "The Military View"
The military traditionally defends US interests overseas. What is the role of the military in cyberspace where borders are meaningless? How do Information Warfare paradigms fit into the the future plans of the armed services?

- Ambassador H. Allen Holmes, Asst. Secretary of Defense (Invited)

10:00 - 10:30 Morning Coffee Break, Sponsored By: _____

10:30-11:00 "The Financial View"

Technology is the underpinning of the world's economy. Systems availability is key to stability and national economic security. As global economies continue to inter-integrate, major challenges arise. How will we address them?

- Roger Pagak, National Security Advisor to the Secretary of Treasury (Invited)

11:00-11:30 "The Commercial View"

What are the organizing principles for information security and the design basis of information systems and networks? The DII is mandated to provide information services to the war-fighter. The NII initiative is enhancing the economic posture of the US. The infrastructures are inter-related and the loss of either capability could have devastating effect on the economy and security of the United States. The GII will necessarily find similar challenges where all nations must develop a viable means of cooperation. This presentation outlines high level approaches to successful implementation.

The Information Warfare Challenges of a National Information Infrastructure
Ronald A. Gove, PhD., V.P. SAIC

11:30-12:00 "Information Revolution" and "Information Powershift"

The sudden empowerment of the individual in the Post Cold War World changes the view of traditional national security. Info-states arise, and global uncertainty increases. The speakers will address the fundamental paradigm shifts that arise as nations transform themselves into knowledge based societies.

Chair: John Peterson, President, Arlington Institute
- Elin Whitney-Smith, Institute for Change and Learning, George Washington University
- Tamara Luzgin, SPO Information-Based Warfare Modeling Naval Research Laboratory

12:00 - 13:30 Sponsored Lunch: Luncheon Speech 12:30 - 13:00

"Information Terrorism," a special video presentation by Paul Strassmann, former Chief Information Officer, Xerox Corporation and former Director of Defense Information
This exciting presentation will be followed with an audience Q&A session.

13:30-14:30 Breakout Sessions:
Class I Meet The Hackers Panel

The underground, denizens of Cyberspace, the first information warriors. Meet them, hear what they have to say about their electronic wanderings. An open, interactive discussion.

Moderated by: Ira Winkler, SAIC
- Chris Goggans, founder Legion of Doom
- Phiber Optik, convicted felon, member Masters of Destruction (Invited)
- Emmanuel Goldstein, Publisher 2600: The Hacker Quarterly

Class II: "Industrial and Economic Espionage - An Update"

What's new in the world or private spying? Front line experts will what's better and what's worse. Who's spying on whom? What are they looking for? What are their techniques and tools? What can you do to protect your organization from being a victim?

Chair:- Jim Settle, Director, I-NET, Inc., former head of Natl. Computer Crime Squad, FBI (The Commercial Perspective)
- Larry Watson, Supervisory Special Agent, National Security Division, DECA Program, FBI
- Bob Friel, Special Agent, Electronic Crimes Branch, Secret Service

Class III "Denial of Service on Information Systems"

Confidentiality and Integrity, two of the three pinions of security have been technically solved with advanced encryption techniques. The third aspect, Availability remains unsolved because of daunting technical problems. What do DOS attacks look like? From the Civil-Cyber Disobedience to Accidental Acts God or Man, a failure of key system components can trigger a domino-like chain of collapses. This session examines the vulnerability of current US infrastructures and the application of such techniques in offensive military applications.

Chair: Larry Merritt, Technical Advisor, Air Force Information Warfare Center
Maj. Gerald R. Hust, USAF (Invited)
"Taking Down Telecommunications"
Maj. Thomas E. Griffith, Jr. USAF, (Invited)
"Strategic Attack of National Electrical Systems.

14:30 - 15:30 Break Out Sessions

Class I "Building a Commercial War Room"
The 'Third Wave' Approach to Managing Information Warfare

Maximizing the flow and control of information is key to competitiveness - whether it be on the battlefield or in the marketplace. An innovative tool and approach to planning and managing information in these very intense, time-sensitive environment is the advent of "war rooms." These are dynamic facilities which are optimized to channel the collection, analysis and dissemination of information. 'War rooms' can be static or field-portable and vary in ergonomic layout and technical capability.

This session will provide case studies on the use of war rooms in government and industry. State of the art automated war rooms will be described which feature the projection of computer-generated information. Tools and practices for knowledge discovery, processing and dissemination will help you understand how you go about planning and building a competitive intelligence War Room?

Chair: Steve Shaker, War Room Research
- Mark Gembecki, Technology and Security Oversight Consultant, US Dept. of State
- Dr. Robert Beckman, Alta Analytics, Inc.
- Stewart Silverstone, Graphical Linguist

Class II "Practicing Defensive Information Warfare"
Military lessons for the private sector

This exciting session will show what the military has learned about 'real time' security testing, new security policies and constant testing and vigilance The military has developed an arsenal of tools for penetration and monitoring and alerting users about intrusions. Commercial attendees will learn what life is like without these mechanisms, and how much dramatically more secure they can be with them - with a low increase in overhead. What steps are required to build a defensive posture, and just how much defense is enough?

Chair: Bob Ayers, Defense Information Systems Agency
- Col. John Sheldon, DISA
- Capt. Kevin J. Zeise, USAF, Chief Countermeasures Development, Air Force Information Warfare Center

Class III "Terrorism and Counter-Terrorism"

Terrorist attacks against the US are now occurring on our home ground. What can the modern terrorist do which will meet his goals of sowing fear and distrust? Experience from both the European perspective and the European Space Initiative (their NII) and the American side will demonstrate how infrastructures such as power grids, communications and transportation systems are attractive targets for the terrorist minded Information Warrior. What are we doing in planned response?

Chair: John Sullivan, FBI (Invited)
- SOCOM Rep. (Invited)
- Neal Pollard, "Computer Terrorism and the Information Infrastructure"

15:30-16:00 Afternoon Coffee Break Sponsored By: _____

16:00-17:00 "Hackers: National Resources or Criminal Kids "
DEBATE

Germany uses professional hackers for their domestic industrial and economic advantage. What about the US? The kindest words ever uttered by Mich Kabay, PhD, about hackers is, "Amoral, sociopathic scum." Robert Steele, President of Open Source Solutions sees them as national resources, to be cultivated as a tool for US economic security. Do they have a value in the protection of the US infrastructure, or can their specific expertise be found elsewhere? After short opening statements, the audience will be encouraged to ask provocative questions.

Moderated by Winn Schwartau, President, Interpact, Inc.
Robert Steele, President Open Source Solutions.
Mich Kabay, PhD, Director of Education, NCSA

17:00 - 19:00 Cocktail Reception, Hors d'oeuvres, and Band
Sponsored By: _____

Most speakers will be available for more intimate groups chats, and authors will be available to sign books. Great opportunity to pursue those ideas with people from different disciplines.

19:00 - 21:00 Birds of a Feather Dinners

"Dutch" dinners give attendees the chance to dig into more and more depth in areas of their particular interest.

* * * * *

DAY II: Friday, September 8, 1995

7:00 - 8:00 Continental Breakfast Sponsored by: _____
8:00 - 8:30 Keynote: "War and Anti-War in the 21st. Century"
Alvin and Heidi Toffler (Invited)

8:30 - 9:30 "Should the US Spy on the World?"

The US has been the target of economic and industrial espionage by militarily allies and 'friendly' competitors such as France, Japan, Korea, Israel, Germany, Taiwan among others. With an estimated intelligence budget of $30 Billion and arguably the most proliferate and advanced technologies, should we turn our spying 'eyes' on our global neighbors for the benefit of American economic security? Or, are Mom and Apple Pie Americans above that?

Chair: Mark Thompson, TIME Magazine (Invited)
- William Colby, former Director Central Intelligence (Invited)
- Thomas Fedorek, Managing Director, Kroll Associates (Invited)

9:30-10:00 "The First Information War: Revisiting Desert Storm"
Lessons in CyberWar for the Commercial Sector and the Military

The US plans a new military strategy of "information war" that assumes an assured ability to dominate knowledge. Knowledge war is absolutely dependent upon spectrum superiority and inviolate software. But, converting cheap and widely available commercial information technology into military capability risks ceding strategic advantage to low-tech adversaries, and, the paradox of a superbly equipped offensive force that also is the most vulnerable to the weapons of information warfare. Desert Storm and other recent military expeditions are examined in the light of evolving definitions and strategies of Cyberwar.

- Alan D. Campen, Col. USAF (Ret.), Contributing Editor, "The First Information War." Former Director of Command and Control Policy to the Undersecretary of Defense.

10:00-10:30 "CORE WARS: Information Trade Wars"
Practicing Information Warfare in Cyberspace"

As fought today on the Internet, Core Wars represent the purest intellectual tests of pure strategy, tactics and capability. Battalions of software programs must genetically breed themselves for combat knowing that they will go up against fierce competition. Video examples will be used to portray how Core Wars is a working model for Information Warriors on the front lines. New models of Information Trade Wars expand this work as "info-nations" need to develop means to maintain global competitiveness.

Stuart Rosenberg, University of Cologne, Germany
Jo Seiler, University of Cologne, Germany

10: 30 - 11:00 Morning Coffee Break Sponsored By: _____
11:00 - 12:00 Breakout Sessions

Class I "Well Managed Propaganda"

The media is a powerful filter by which citizens and the government collect most of their information. Was the media a puppet of the US in the Gulf War? Does aggressive PR makes media policy? How can the media be used, or protect itself from being used? How can people's perceptions be manipulated to specific advantage?

Moderated by: Neil Munro, Senior Editor, Washington Technology,
- Vic Sussman, US News and World Report (Invited)
- Jim Roberts, SOLIC PSYOPS (Invited)

Class II "Threats To Electronic Commerce and Anonymous International Banking"

As the world increasingly relies on electronic commerce, every country, business and individual can be targeted or affected by financial system assaults. This session will examine these threats as well as promising safeguards and countermeasures. The threat of anonymous financial transactions is especially illuminating.

Chair: Mark Gembicki, Security Consultant, US Dept. of State
- Steve Diamond, V.P. Electronic Publishing Resources
- Eric Hughes, Financial Security Expert, co-founder Cypherpunks

Class III "The Legal Consequences of Information War"

What are the legal rights of Cyber-citizens in the US and how do those relate to the laws in other countries? What is the real criminal and civil recourse and remedies to combat industrial espionage? How do we legally handle non-physically violent attacks against the interest of the US on our own soil or overseas? Get the views of the experts.

Chair: - Daniel Kuehl, PhD, Professor, National Defense University
- Air Force General Counsel Representative (TBD)
- Scott Charney, Department of Justice

12:00 - 13:30 Lunch
12:30 - 13:00 Luncheon Speech:
"Export Control As A Proactive Defensive Information Warfare Mechanism"
Winn Schwartau, President, Interpact, Inc.

13:30 - 14:30 Breakout Sessions

Class I "An Electronic Bill of Rights"
Defining Privacy In Cyberspace

How do we as a nation balance the privacy rights of the individual against the legitimate needs of the state, and in sync with the policies of our global trading partners? The views from three differing positions will stimulate a healthy audience-panelist dialogue.

Chair: Andrew Grosso, Former Asst. US Attorney
- Scott Charney, US Department of Justice
- Cynthia Hogan, Democratic Counsel, Senate Judiciary Commitee (Invited)
- Jerry Berman, Executive Director, Center for Democracy and Technology (Invited)

Class II "Defending Against the Internet"

The chaotic ravages of the Internet constantly knock at the doors of anyone or any company is connected. What do you have to do to protect your information resources? What have others done? Is it enough and what does the future bode?

Chair: Kermit Beseke, President, Secure Computing Corp.
- John Nagengast, Deputy Chief of Network Security, National Security Agency (Invited)
- Robert Stratton, Security Services Manager, UUNet Technologies, Inc.

Class III Measuring Effectiveness of Theater IW/C2W Campaigns

Success in theater and JTF campaigns demands the full incorporation of C2W and IW. This presentation puts forth the latest research and techniques for modeling and evaluating the effectiveness (MOE) of simulations and real conflicts.

Chair: National Defense University
- Howard W. Clark and Sandra K. Wellfesh, Dynamics Research Corporation

14:30-15:00 Afternoon Coffee Break Sponsored By: _____

(The afternoon sessions will be moderated by National Defense University.)

15:00-15:30 "Protecting Information Resources in Cyberspace"
Lee Sutterfield, Division Chief, Engineering Analysis, Air Force Information Warfare Center

15:30-16:30 "What Is the Role of Government in defending National Economics?"

As evolving global conditions shift competitive value from military might to economic advantage, how should we redefine national security? The threats to the private sector increase and become more likely targets in information warfare of all three classes. What is, and what should the role of the military be in defending US interests both domestically and abroad? This session will provide plenty of opportunity for audience involvement.
- Assistant Secretary of Commerce Larry Irving
- Dr. Barry Horton, Maj. Gen. USAF (Ret.)
- Principle Dep. Asst. SecDef for C4I (Invited)

16:30 - 17:00 "The Future of Information Warfare"

Where do we go from here? After two intensive days of interaction, learning and listening, what's the next step? What do industry and the government have to do to better understand each other? What steps can each take to improve individual, corporate and national defensive postures?
Dr. John Alger, National Defense University

17:00 - 17:15 Closing remarks: Peter Tippett, President, NCSA
17:15 - 19:00 No-host reception.

To be kept informed about future Information Warfare conferences, join the NCSA by phoning 717-258-1816 or send the Membership Director e-mail at ssands@ncsa.com any time.

