Conflict and the Computer:

Information Warfare and Related Ethical Issues

Sam Nitzberg

ABSTRACT: Information warfare, the engaging of computers in conflict, provides new avenues for investigation regarding their use in industrial espionage, accomplishing political ends, and warfare. Issues to address in understanding the use of computers in any conflict include the motivations for such conflict, the nature of warfare, what a party might choose to accomplish in any such conflict, and the nature of defense in information warfare. Naturally, there are consequences to any conflict, and the nature of information warfare deserves to be considered from the perspective of its ethically-related issues.

1 Introduction

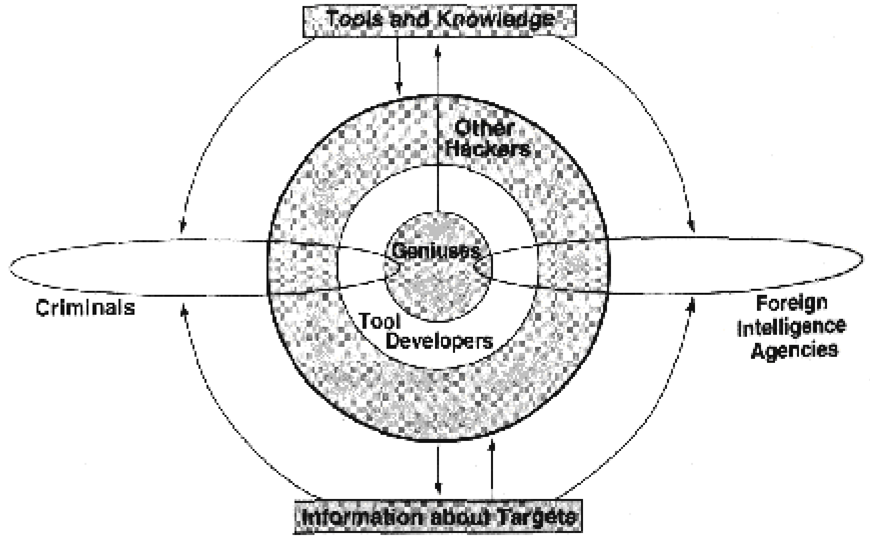
This paper discusses information warfare and ethical issues by providing an overview to the subject of information warfare, and a brief discussion of warfare and historical notions of just war. Following this, issues are discussed which describe significant areas of interest to both the "underdog" and the "fat cat," those either seeking or holding power, respectively, through the use of information warfare. A brief guide follows recommending how an organization (small or large) may defend itself in light of the material presented, along with an appropriate conclusion.

Information warfare concerns the use (and abuse) of computers and high-technology appliances to undermine the computing resources of an adversary. This may be done to obtain information from an enemy, cause havoc among a nation by disrupting its information infrastructure or industry, or to spread propaganda when other means might not be practical. One popular view decomposes information warfare and information warfare incidents into three classes: personal information warfare, corporate information warfare, and global information warfare[Schwartau,1995]. What distinguishes the three categories is whether the subject of the attack is an individual, business enterprise, or government, respectively. Information warfare is closely related to infrastructural warfare, which involves the disruption of a government without necessarily causing direct loss of life. As more computers connect to systems used by society as a whole, the capability to use computers to engage in infrastructural warfare will only increase.

The engineer has historically been of significant value to those engaged in warfare. Some of the more famous examples of technology advancing the state or understanding of warfare include Leonardo DaVinci's war machines [Doeser,1994], the use of computers in performing calculations in developing the hydrogen bomb, breaking of the enigma code in Bletchely Park, and in Aiken and Jon Von Neuman's automated generation of ballistic tables.

Today, computers are commonly used to effect computerized command and control systems for the modern, digitized battlefield. At their core, computers were developed, and remain today, as weapons. Not long ago, an incident came to light where Dutch hackers had obtained sensitive information including order-of-battle data by penetrating systems belonging to the Coalition Forces during the engagement of the Persian Gulf War. This information was offered to sale to the Iraqi government, which feared a ruse due to the value of the information, and declined to engage in any sort of transaction for the offered intelligence [AP].

The diagram below represents a model of the hacker community at large [Winkler, 1997]. An interesting consideration I would add is that, contrary to what is indicated in the diagram, the groups containing Foreign Intelligence Agencies and Criminals are not necessarily mutually exclusive in their memberships. By their definitions and charters, most intelligence organizations conduct operations in other n untries which, by their definitions, are illegal in the target nations. Additionally, there is the rare case in which a member of an intelligence agency could act in a criminal manner, unrelated in any fashion to duties related to actual intelligence activity.



The Hacker Community

Some hackers view their endeavors as being "value-free," without distinguishing between good and bad hacking. One popular view among hackers is, "Breaking into a computer should not be a crime! No one gets hurt and we all learn something. But hurting people with the data or hurting the computer should be illegal. Having a negative impact should be illegal. You have a lot of benign people going to jail … They're not real criminals. They are explorers who are being persecuted for thinking [Schwartau, 1995]." A more accurate view of the hacker ethic might be "Don't get caught," along with the caveat, "and if you do get caught, cash in and make money." Works such as *Out of the Inner Circle*, and *Masters of Deception: The Gang That Rules Cyberspace* relate stories of hackers who were caught and either went on to publish their stories, or become engaged in security consulting[Landreth, 1985 ; Slatalla, 1995].

At a recent Signals Symposium, a senior U.S. Army officer indicated that the teenage hacker is just as deadly an opponent as a Force XXI soldier assaulting a position. The role of the computer as a weapon in and of itself magnifies the consequences of a teenager - or for that member, any Underdog, who may surreptitiously obtain access to computerized weapons systems. In traditional warfare, even when corporations are targeted as enemies, the players are tangible: there is a significant risk of a party getting caught and facing severe penalties. In information warfare, poorly equipped and funded actors (participants in intelligence parlance) can remain anonymous and create great harm.

The opportunity to cause great harm and remain anonymous heightens the need for individuals and organizations with computing resources to maintain an ethical balance to their operations. While countries develop with the rule of law, computing environs often develop with no significant authentication mechanisms, security policies (roughly analogous to laws), enforcement mechanisms, or borders. The interesting question regarding the integrity of computer networks, is often not so much a question of what keeps the networks and their users together, but what keeps them from breaking apart.

2 Warfare

The Clausewitzian premise, that war is something waged by the state for political ends can be considered naive, if not incorrect . Those who have waged war do not always include states proper, but have included many sorts of social entities: barbarian tribes, the Church, feudal barons, free cities, and private individuals

[Creveld, 1991].

Due to their growing presence, computers will be increasingly used by organizations to defeat or undermine their adversaries (real or perceived). Naturally, anyone using technology to defeat or injure a foe will feel justified in their actions (as did the "Unabomber" who used his technically sophisticated, hand-crafted bombs to injure and kill individuals as his way of protesting technology). The philosophies of Roman just war, medieval just war, and current international law all acknowledge circumstances in which it is ethically sound to engage in war:

"It will be remembered that medieval and early modern just war theory, following Roman law and practice, recognized three kinds of justifying cause for war:defense, retaking something wrongly taken, and punishment of evil. Positive international law formally recognizes only defense; yet in practice the concept of defense has been stretched to include the other two, as in the Falklands war of 1982 (retaking something wrongly taken) and the justification of "defensive" nuclear retaliation (punishment of evil). The logic of these international law developments is straightforward, however: if there is no higher judge of justice than the nation-state, then its integrity against attack must be paramount, and defense of that integrity against attack must be the only generally acceptable justifying cause for use of military force. Both as an elaboration and regularization of the just war tradition (in the case of the jus in bello) and as a truncated statement of it (in the case of the jus ad bellum), international law on war remains a major stream of development of just war tradition [Kelsay, 1995]".

3 The Underdog, or

Perception, benefits, and consequences of information warfare for those wanting power

Once upon a time, one of the most feared disadvantages in the weapons race between the United States and Soviet Union was the "Missile Gap," the disparity between Soviet and American missile strength and numbers. This matter has bloomed into the current situation, where the American and collective Soviet governments (arguably) have more than a sufficient numbers of missiles for their needs. Cryptography and security form a new pair of gaps the Underdog may use to its advantage.

The "cryptography gap" encompasses a host of concerns which perplex free governments. With advances in mathematics and software since the 1960s, software and hardware can be at anyone's disposal at virtually no cost. While personal privacy has been one of the greatest goals of free government, there is a price to be borne by governments for the guarantees of privacy offered by the newer software packages - the governments may be generally unable to access records related to crimes, insurgency, or personal data. A government may seize all records belonging to a revolutionary group, and still learn nothing. Software is even available which allows computers to place telephone calls over the Internet, using strong encryption to protect the calls by making them indecipherable to anyone who may listen in on the connection. Due to the low cost and high compatibility of modern cryptographic software, and the widespread presence of computer and telephone networks with which to exchange messages, cryptography is one of the most cost-effective instruments available to those making any grand plans towards coups d'état.

For the individual or small organization, it is generally not too difficult a matter to overcome the security of a large computing environment; this brings us to the subject of the "security gap." Large environments, without proper precautions and disciplined policies, can quickly grow to resemble Swiss cheese when examined from a security perspective. Automated network tools can be used to analyze computer networks from either inside a corporation's own networks or from the Internet. The common lack of computing security policies or computing security infrastructure leave companies wide open to attack; an aggressor often only needs to find one good security hole to effect his will against an enterprise. This imbalance provides the Underdog with very cost-effective options when implementing information warfare methodologies to effect change or conduct a mission/operation.

One reckless method of affecting systems is through the deployment of computer viruses. Viruses are self-replicating programs which are automatically copied between computers without the knowledge of the operators. Under some set of conditions, these programs generally perform some function which causes harm. An ex-author of computer viruses, who went by the name Hellraiser and founded an electronic-format magazine on how to develop computer viruses has moved on, "The stuff we did was terribly wrong and terribly evil, and I'm probably going to Hell for it [Wired,1997]." Most viruses are developed as some sort of prank or exercise, but they have also been used as modes of political expression. The Tiennamen Square Virus is transferred (through disks) between computers and activates on the anniversary of the Chinese government's crackdown on the democratic protesters. Unfortunately, however, once the virus was released "into the wild," it could propagate and infect any systems - even those belonging to democracy loving students anywhere throughout the world. Properly designed, a computer virus could target and hurt an adversary. Half of the vital chemical weapons logs kept during the Persian Gulf war may have been lost due to a computer virus [APP,1997]. If some characteristic were known of an enemy's systems - for example, if they had certain data or files present, a virus could be programmed to activate only on systems with that particular characteristic. Note that an enemy need not be a military adversary, but could include political organizations, corporations, or even non-profit service organizations.

Due to societies' increasing dependence upon computers for day-to-day transactions and necessary services, computers will be increasingly targeted by organizations seeking to harm the Fat Cat, discussed later, especially as an extension of infrastructural warfare methods. Warnings have already been issued that terrorist organizations may be looking to expand their capabilities to include information warfare expertise, especially as negotiations and diplomatic approaches to their needs progress, and non-lethal operations become increasingly desirable means for achieving their ends. A hacker group, the Hong Kong Blondes, has already temporarily disabled a Chinese communications satellite and has provided a warning to China that there will be increasingly severe attacks if there are any human rights crises in Hong Kong[Wired,1997].

One factor often overlooked in the engagement of warfare or conflict is the consequences to the adversary. Due to the wide and sweeping capacity of computers to operate systems critical to society and necessary for life (such as medical, traffic, and air-control systems), the aggressor must take special note to consider the consequences of any actions taken against computing platforms. The aggressor should not seek to perform reckless harm. While it may be convenient to consider it fundamentally wrong to inflict harm in any context, there are precedents for just war, and it is very difficult to conceive of any job or operation which, taken in the proper context, is totally free of producing harm. One mere practical joke, the Internet worm unleashed by Robert Morris, produced very definite harm by disabling a large number of computer systems.

A great many tools which may be used to attack computers are available for free. These include:

- Network Scanning Tools
- Password Cracking Tools
- Denial of Service Tools
- Cryptography Tools

These tools may be used to identify the vulnerabilities present in computers attached to a company's or government's computer networks, crack and defeat password systems, effectively deny an organization's computers the ability to provide the services which it is required to perform, and establish private communications respectively.

With these tools, any small, loosely-knit computing interest may become a formidable adversary, and there is a demand for mercenaries, computer security guns for hire. An example of such a gun for hire is the Hanover Hacker described in *The Cuckoo's Egg* by Clifford Stoll. The Hanover hacker had links to both the East German Stasi and the KGB[Schwartau, 1995].

Attacks may be launched from any location with a telephone and a modem. In all actuality, attacks may be launched from Internet cafés with anonymity, and if one is in a location without either Internet cafés or telephones, a satellite phone will work nicely. A number of steps may be taken to anonymize attacks using computers, but borders matter little.

Hackers can use their skills towards their ends, which may range from trivial to political in scope. By undermining the security of a web server, they may access any legitimate organization's web page and change its contents. Similar attacks are occurring with increasing regularity, and before and after versions of web pages which have been attacked are available for viewing online [2600,1997]. In some cases, the hackers have squandered their opportunity to effect change or promote any political view. One such case is that of the hacked CIA's home page, which was modified to include a link to "naked women." In other cases, effective use has been made by the hacking of the Republic of Indonesia's web page, which was modified on more than one occasion to include anti-Indonesian, pro East Timor propaganda, and the attack upon the Kriegsman fur company web page, where anti-fur rhetoric and pleas to harass the staff of the company were placed on-line. The World Wide Web has been used to perpetrate hoaxes; in one such hoax, an Internet web page was established claiming proof that airliner TWA800 (a civilian airliner which crashed in the shore off of the Long Island Coast) was shot down by an anti-aircraft missile. In fact, there was no such evidence; but, had this information been placed on the U.S. Department of Justice home page (which had been hacked previously), the Justice department's reputation and credibility could have been severely compromised.

Governments in exile could find computers to be very effective tools in their campaigns for legitimacy. Computers may be used to disseminate cryptographic keys to ensure private communications, to establish password-protected and secure pages for operatives to obtain their assignments, to distribute propaganda, and to collect data on their adversaries, by obtaining both publicly available information (such as is available on web sites), as well as by using covert computer-based means for information gathering. Experienced computer security specialists or hackers may also be able to effectively cover their tracks in a number of cases. The computers can present a "sanitary" battleground on which to conduct operations.

4 The Fat Cat, or

Perception, benefits, and consequences of information warfare for those having power

The Geneva convention, and its interpretations allow for different treatment for soldiers, who are protected under its terms, and spies, for whom it offers no such protection. The question of how civilians caught during conflict using computer warfare methods against companies or governments must be addressed. A member of a given country's legitimate armed forces may use information warfare methods against another nation and be apprehended; in such a case, the soldier would be afforded protection under the Geneva convention. On the other hand, should an individual not affiliated with armed services, or in the employ of a nation be apprehended, that person could easily be regarded as a spy, and be subject to harsher treatment.

Nations and large enterprises can monitor information systems under their domain. During WWII, wire services were known to produce copies of their communiqués to the U.S. War Department. Presently, certain governments maintain the right, if not the capacity, to monitor Internet connections[Case, 1997 ; Zixiang, 1997]. One theoretical model even outlines how computers could be used to monitor both voice and video in their vicinity [Nitzberg,1996]. While such capabilities may be to the advantage of large corporations or governments, there are a great number of terrible deficits that they must face. More advanced nations (and their industry) are more vulnerable to having their technology exploited than less technologically sophisticated ones. Their banking, power, communications, and military infrastructures may all be attacked through technological and computing platforms.

The table below reports figures which reflect recent analyses of both civilian and DOD (United States Department of Defense) computer systems, and the rates at which they are attacked or probed[Gibbs, 1997].

While there is some debate as to how to properly measure and distinguish individual computer attacks and probes, these figures are generally well respected, and are useful in comparing the rates of the effectiveness of computer-based attacks against systems in both government and industry, and give a good indication as to the state of various organizations' security postures.

GOVERNMENT:	
Estimated number of hacker attacks on DOD in 1995: in 1996:	250,000 500,000
Estimated percentage that are successful:	65%
Estimated percentage detected by the DOD:	Less than 1
RESEARCH:	
Average number of potentially damaging hacker attempts on Bell Labs networks in 1992, per week	6 per week
Average number of less threatening attacks, per week	40
Average rate of attacks in 1996	No longer tracked.
COMMERCE:	
Percentage of banks in recent survey that report plans to offer Internet banking services in 1997:	36%
Percentage of existing bank web sites found to have potentially significant security holes:	68%
Percentage of Web sites selected at random with such holes:	33%

Table I - Breaking and Entering

Recent U.S. government estimates indicate that more than 120 countries presently have information warfare attack capabilities, with most planning to incorporate information warfare into their overall security strategy. Further, the results of an exercise performed for Office of the Secretary of Defense for Command, Control, Communications and Intelligence demonstrated the susceptibility to attack of train routing systems, military systems, including weapons systems, banking systems, telephone, and power systems in various countries[GAO,1996]. Together, these findings reveal a growing international threat to both government and corporate interests.

5 How an organization protects itself

An Organizational Security Process Model may be used in securing an organization's computing assets [Nitzberg,1997]. There are a number of available process models to choose from, but they should have certain aspects in common. Organizations should have a documented process model which will ensure their ability to maintain and revise their information security policies, identify known vulnerabilities in their computing platform, and factors which expose themselves to risk, and to regularly update their policies, procedures, and security countermeasures. Of paramount importance is security awareness training.

A number of organizations are taking steps towards spreading information related to ethics and security by way of education. The ACM (Association for Computing Machinery) sponsors its annual computing security day in order to promote an awareness of computing security and related issues. The ACM has adopted its own code of ethics for members, as has the IEEE (Institute for Electrical and Electronics Engineers) [ACM,1997].

Businesses are starting to include more computer security training and awareness than has been historically provided, but more training is needed. Universities have started to incorporate computer ethics into both their computer science and business curriculums. News stories have been addressing security issues and the consequences of recent system penetrations with greater frequency and detail than ever before. With the growth of each of these trends to disseminate information related to computer security and conflict will come added exposure to the computing populace of the ethical and very real consequences associated with subversions of computing security mechanisms and technologies.

In the United States there has been investigation into preventative measures to preclude an "electronic Pearl Harbor." One proposal assigns specific government agencies to be responsible for assisting various sectors in the American Information Infrastructure (which includes telecommunications, electric power, gas and oil, banking and finance, transportation, water, emergency services, and continuity of government related concerns and interests). The philosophy behind this approach is that national and economic security has become a shared responsibility between government and industry, and that the federal government must collect appropriate information and share it with industry, while the private sector must take reasonable actions to protect itself from hackers. This cooperation between government and industry is viewed as critical, as an attack against the United States may not be directed against its military organs. Still, debate continues regarding where the various responsibilities are to be drawn, as well as what costs should be borne by government and by industry[Harreld,1997]. Other nations will have to confront similar issues.

There are a large number of unknowns when dealing with computer crime, fraud, abuse, information warfare, and subterfuge. Governmental organizations often have funding or manpower problems, or may lack the experience needed to assist an organization. The courts often fall far behind technology, which is not a new phenomenon, nor is it a situation unique to the United States. Recently forming pacts and legal alliances between law enforcement and judiciary bodies from Canada, France, Germany, Great Britain, Italy, Japan, Russia, and the United States have the potential to allow quick investigation and uniform penalties for international criminal activity occurring global networks [Johnson]. There are opportunities, however, which must be taken advantage of, and which can be used to confront the unknowns. Organizations and business alliances can form their own computing intelligence groups to help them defend their systems; they can lobby and press for more meaningful laws and enlightened interpretations of legislation, and they can educate their personnel as to the risks inherent in the use of technology.

6 Conclusion

Although there are a great number of players engaging in information warfare and computer conflict, methods by which computers may be effectively secured are known. Due to the growing intrusion of the computer into all realms of everyday personal and professional life, the ubiquity of computers, and the quickly shared knowledge of their vulnerabilities, companies and organizations can and must assure their own protection. This is not merely of pragmatic concern, but a moral responsibility and ethical mandate due to the severe consequences to stockholders and customers, and to populaces as a whole, due to the growing importance and reliance by societies upon computing systems.

7 References

2600 (1997), 2600: The Hacker Quarterly Web Page, http://www.2600.com/hacked_pages

ACM (1997), Association of Computing Machinery Code of Ethics, http://www.acm.org/serving

AP (1997), Associated Press (London), "Experts: Hackers Stole War Data, March 24, 10:18 PM EST.

APP, (1997) Chemical Data Wiped out by Computer Virus (Associated Press). Asbury Park Press, 28 February.

Case, D. (1997), Big Brother is Alive and Well in Vietnam - and he Really Hates the Web, Wired, November, 164-176.

van Creveld (1991), The Transformation of war, The Free Press- A Division of Macmillan, Inc., New York, 52.

Doeser, L. (1994), The life and Works of Leonardo Da Vinci, Shooting Star Press, 42-47.

GAO (1996) - General Accounting Office, Report to Congressional Requesters: Information Security - Computer Attacks at department of Defense Pose Increasing Risks, GAO/AIMD-96-84, May 1996. http://www.epic.org/computer_crim/gao_dod_security.html

Gibbs, W. (1997), Profile: Dan Farmer From Satan to Zen, Scientific American, April, 32-34.

Harreld, H. (1997), Feds, Industry at odds over data, duties, Federal Computer Week, Vol. 11, #35, 1.

Johnston, K. (1997), USA Today, Worldwide strategy set on fighting cybercrime, 1A.

Kelsay, J. and Johnson, J. (1995), Just War and Jihad: Historical and Theoretical Perspectives on War and Peace in Western and Islamic Traditions, Greenwood Press, 21.

Landreth, B. (1985), Out of The Inner Circle, Tempus Books of Microsoft Press.

Nitzberg, S. (1996), Emerging Issues Involving the Presence of Cameras and Microphones in the Computing Environment, SIGSAC-Security, Audit, and Control Review, ACM Press, Vol. 14, No. 3, 13-16.

Nitzberg, S. (1997), The Cyber Battlefield - Is This the Setting for the Ultimate World War?, Proceedings of the IEEE International Symposium on Technology and Society: Technology and Society at a Time of Sweeping Change,100-106.

Schwartau, W. (1995), Information Warfare: Chaos on the Electronic Superhighway, First Trade paperback edition, Thunder's Mouth Press, 207-209.

Slatalla, M. and Quittner, J. (1995), Masters of Deception: The Gang That Rules Cyberspace, HarperCollins Publishers.

Winkler, I. (1997), Corporate Espionage, Prima Publishing, 86.

Wired (1997), Hacking the Great Firewall, Wired, December, 120.

Wired (1997), Hellraiser Unplugged, Wired, December, 120.

Zixiang, T. and Mueller, M. and Foster, W. (1997), China's New Internet Regulations: Two Steps Forward, One Step Back, Communications of the ACM, Vol. 40, No. 12, 11-16.

8 Contact

Sam Nitzberg may be contacted at: Telos Corporation, 656 Shrewsbury Avenue, Shrewsbury, NJ 07702, USA; or, at: 241 Cummings Avenue, Elberon, NJ 07740 (USA). Sam Nitzberg's electronic mail address is sam.nitzberg@telos.com, and Sam may also be reached through his web page at http://www.iamsam.com.