INFORMATION WARFARE AND ETHICS

M.J.Warren W.Hutchinson

School of Computing
Deakin University,
Geelong, Victoria,
Australia.

School of Management Information
Edith Cowan University,
Perth, Western Australia.

Email contact: mwarren@deakin.edu.au

ABSTRACT

This paper examines the ethics of the practice of information warfare at both the national and corporate levels. Initially examining the present and past actions of individual hackers, it moves to the more organised, future military and economic warfare scenarios. It examines the lack of legal or policy initiatives in this area.

INTRODUCTION

During the last ten years there has been a growth of Information Systems and related Internet technology within the developed world. In recent years the Internet has grown from a solely military/academic network to one that can be used by business or individuals. In the years since the first WWW applications were developed, there has been an explosion in the global use of the Internet. In that time we have seen the development and growth of electronic commerce and the first steps towards the development of a global information society (Warren & Hutchinson, 2000).

We have seen a rise in computer misuse at a global level and also the development of new policies and strategies to describe organized computer security attacks against the information society – these strategies are described as being 'information warfare'. This is very different to the traditional view of attack against computers by the individual, determined hacker, a cyber warrior with a code of conduct to follow.

COMPUTER HACKER

The definition of the 'computer hacker' has been the subject of many debates in computing circles. Caelli et al (1989) provide two definitions of the term:

- Those who take a delight in experimenting with system hardware, software and communication systems
- Unauthorised users who try to gain entry into a computer, or computer network, by defeating the computers access (and/or security) controls.

In the contemporary world, the latter interpretation is by far the more common (although persons belonging to the former category of hacker would seek to more accurately define the latter group, particularly those with a malicious intent, as 'crackers'). Hackers are by no means a new threat and have routinely featured in news stories during the last two decades. Indeed, they have become the traditional 'target' of the media, with the standard approach being to present the image of either a 'teenage whiz kid' or an insidious threat. In reality, it can be argued that there are different degrees of the problem. Some hackers are malicious, whilst others are merely naïve and hence, do not appreciate that their activities may be doing any real harm. Furthermore, when viewed as a general population, hackers may be seen to have numerous motivations for their actions (including financial gain, revenge, ideology or just plain mischief making). However, in many cases it can be argued that this is immaterial as, no matter what the reason, the end result is some form of adverse impact upon another party.

Issues of computer abuse became apparent in the sixties when the first computers were created and used. The levels of computer crime reported in the sixties and seventies, seem very small when compared to today as shown by Table 1 (Parker, 1976):

Year	Number
1962	2
1963	1
1964	11
1965	8
1966	2
1967	4
1968	12
1969	15
1970	33
1971	54
1972	67
1973	69
1974	59
1975	43

Table1: Number of Security Incidents in the USA

Donn Parker (Parker, 1976) highlighted that the individuals involved in computer crime in the 1960's and 1970's were employed as key punch operators or clerks in EDP organisation s and the crimes were crimes of opportunity. In the 1980's with the development of cheaper home micro and the introduction of modems a new generation of younger computer users were developed. One of the features of this younger group was a keen interest in the technologies that lead to the development of hackers.
Steven Levy's book *Hackers: Heroes of the Computer Revolution* (Levy, 1984) suggests that hackers operate by a code of Ethics. This code defines main key areas:

- **Hands On Imperative**: Access to computers and hardware should be complete and total. It is asserted to be a categorical imperative to remove any barriers between people and the use and understanding of any technology, no matter how large, complex, dangerous, labyrinthine, proprietary, or powerful.
- **"Information Wants to Be Free"** "Information wants to be free" can be interpreted in a number of ways. Free might mean without *restrictions* (freedom of movement = no censorship), without *control* (freedom of change/evolution = no ownership or authorship, no intellectual property), or without *monetary value* (no cost.)
- **Mistrust Authority.** Promote decentralisation. This element of the ethic shows its strong anarchistic, individualistic, and libertarian nature. Hackers have shown distrust toward large institutions, including, but not limited to, the State, corporations, and computer administrative bureaucracies.
- **No Bogus Criteria:** Hackers should be judged by their hacking, not by 'bogus criteria' such as race, age, sex, or position.
- **"You can create truth and beauty on a computer."** Hacking is equated with artistry and creativity. Furthermore, this element of the ethos raises it to the level of philosophy.
- **Computers can change your life for the better.** In some ways, this last statement really is simply a corollary of the previous one. Since most of humanity desires things that are good, true, and/or beautiful.

During the 80's and 90's this pure vision of what hackers are was changed by the development of new groups within various aims and values. Mizrach (1997) states that the following individuals currently exist in cyber space:

- **Hackers** (Crackers, system intruders) - These are people who attempt to penetrate security systems on remote computers. This is the new sense of the term, whereas the old sense of the term simply referred to a person who was capable of creating hacks, or elegant, unusual, and unexpected uses of technology.
- **Phreaks** (Phone Phreakers, Blue Boxers) - These are people who attempt to use technology to explore and/or control the telephone system.
- **Virus writers** (also, creators of Trojans, worms, logic bombs) - These are people who write code which attempts to a) reproduce itself on other systems without authorisation and b) often has a side effect, whether that be to display a message, play a prank, or destroy a hard drive.

- **Pirates** - Originally, this involved breaking copy protection on software. This activity was called 'cracking'. Nowadays, few software vendors use copy protection, but there are still various minor measures used to prevent the unauthorised duplication of software. Pirates devote themselves to thwarting these and sharing commercial software freely.
- **Cypherpunks** (cryptoanarchists) - Cypherpunks freely distribute the tools and methods for making use of strong encryption, which is basically unbreakable except by massive supercomputers. Because American intelligence and law enforcement agencies, such as the NSA and FBI, cannot break strong encryption, programs that employ it are classified as munitions. Thus, distribution of algorithms that make use of it is a felony
- **Anarchists** - are committed to distributing illegal (or at least morally suspect) information, including, but not limited to, data on bomb making, lock picking, pornography, drug manufacturing, and radio, cable and satellite TV piracy.
- **Cyberpunk** - usually some combination of the above, plus interest in technological self-modification, science fiction and interest in hardware hacking and 'street tech'.

Mizarch (1997) determined that new groupings with cyberspace had altered the initial code of ethics, and that the code of Ethics in the 1990s was more concerned with:

- **"Above all else, do no harm"** Do not damage computers or data if at all possible.
- **Protect Privacy** People have a right to privacy, which means control over their own personal (or even familial) information.
- **"Waste not, want not."** Computer resources should not lie idle and wasted. It's ethically wrong to keep people out of systems when they could be using them during idle time.
- **Exceed Limitations.** Hacking is about the continual transcendence of problem limitations.
- **The Communication Imperative.** People have the right to communicate and associate with their peers freely.
- **Leave No Traces.** Do not leave a trail or trace of your presence; don't call attention to yourself or your exploits.
- **Share!** Information increases in value by sharing it with the maximum number of people; *don't hoard, don't hide.*
- **Self Defence** against a Cyberpunk Future. Hacking and viruses are necessary to protect people from a possible Orwellian '1984' future.
- **Hacking Helps Security** This could be called the 'Tiger team ethic': it is useful and courteous to find security holes, and then tell people how to fix them.
- **Trust, but Test!** You must constantly test the integrity of systems and find ways to improve them.

This newer code of ethics is more based upon the view that Hackers are helping in the development of the Information Society and adding to its distinct nature. The ethics of imposing these values on others who are unwilling 'victims' does not seem to be questioned.

INFORMATION WARFARE

The advent of the contemporary concept of 'information warfare' (see Schwartau, 2000, 1994; Denning, 1999; Waltz, 1998) has raised the tampering of computer systems to a new dimension. The individualistic, anarchistic, and rather naive actions of young hackers has been replaced by the determined, methodical, and organised workings of states, corporations, and criminal gangs. Initially, the term 'information warfare' was concerned with damaging a country's National Information Infrastructure (NII) (Schwartau, 1994). For the purposes of this paper, the NII is defined as the physical and virtual backbone of an information society and includes, at a minimum, all of the following (Cobb, 1998):

- government networks-executive and agencies;
- banking and financial networks-stock exchanges, electronic money transfers;
- public utility networks-telecommunication systems, energy and water supply (military and civil), hospitals, air traffic control and guidance systems, such as the Global Positioning Satellite system and the Instrument Landing System both common to commercial aviation ;
- emergency services networks (including medical, police, fire, and rescue);
- mass media dissemination systems-satellite, TV, radio, and Internet;
- private corporate and institutional networks, and

- educational and research networks.

Information warfare is concerned with the full spectrum of offensive and defensive operations such as electronic warfare, cyber-terrorism, psychological operations and so on (Main, 2000). Mainly it has been associated with the so-called 'Revolution in Military Affairs' (RMA). In some respects IW is a sub-set of the RMA, which is also concerned with the military application of new technologies to the 'battlespace' (Cobb, 1998), such as stealth, precision guided munitions, and advanced surveillance capabilities.

Because of this military aspect of information warfare, its ethics have been associated with those of warfare. It is a development of the nature of warfare. The development of 'total war', arguably started in the actions of Napoleon but certainly present in the Second World War, has been extended by the advent of information warfare. The distinction between military and civilian targets has been blurred. The Kosova conflict illustrated this. The bombing of a television station as a part of the Serbian military machine displayed the importance of information in modern conflict (Ignatieff, 2000). At the state level, there is a tendency to attempt to develop 'information superiority' over every competitor. International and national legal systems still have to catch up with this trend.

There are ethical implications between developed and less developed countries. In terms of information warfare, each society has its advantages and vulnerability. For instance, the USA has an enormous advantage in digital facilities from fibre optic communications to satellites and sophisticated software production. However, this advantage also adds vulnerability, as digital systems are susceptible to attack. The infrastructure of a 'networked' society (eg power, water) is very exposed.

Developing countries at a lower level of development have an advantage of slower communication and processing systems, but this lack of sophistication lessens the vulnerability to an information attack.

The advantages of developed societies in the information 'struggle' can be summarised as:

- Advanced infrastructure
- Have the intellectual property rights to most advanced developments
- Advanced technologies
- Have control of large corporations
- Advanced networked society possible, reliant on technology but infinitely flexible
- Capable of information dominance strategy
- Dominate perception management industries, eg media

The advantages of developing nations can be summarised as:

- Lack of vulnerable electronic infrastructure
- Low entry costs to get into electronic systems development
- Web based systems know no geographic boundaries (in theory), hence neither does 'place' of company
- Networked society based on 'clans', difficult to penetrate
- Cheap labour, often with an educated elite, eg India

The implications of interstate behaviours have yet to be fully worked out. Of course, it is questionable whether 'ethics' *per se* are relevant in an environment where international law (which *should* reflect ethical issues) and national self interest dominate.

Information warfare has also spilled into the corporate arena. Adams (1998) emphasises the movement of state aggression from military to economic. However, this conflict can be said to have also moved to corporate to corporate conflict, and even corporate to individual. The use of information warfare techniques can be seen as just another factor of business behaviour. Grace and Cohen (1998) illustrate the dilemma in business of behaving ethically. They argue that, all too often, arguments are polarised into two choices: behave unethically or fail. For many organisations, business is a form of competitive warfare. Hence, techniques applicable to the military and intelligence services (information warfare) are viewed as feasible choices, although Grace and Cohen assert that it is wrong to assume that competitor's tactics are designed to destroy rivals. However, they do argue for an "international legal and normative infrastructure...The point is often lost in analogies with war, however, is that a great deal of this infrastructure already exists in private and public international law" (*ibid*, p.181). Whilst this may be the case for general business practices, the advent of cyber-space has created problems of definition and jurisdiction.

However, over the last few years, legislation in America, Europe, and Australia has allowed intelligence and law enforcement agencies to perform these operations. For instance in 1999, the Australia Security and Intelligence Organisation (ASIO) was allowed (with ministerial approval) to access data, and generally 'hack' into systems

(Lagan and Power, 1999). Therefore, legal hacking is the province of the authorities. Hardly, an ethical, public stance to take. In fact, it just emphasises the efficacy of information warfare techniques to others.

At the local Australian and international level is the problem with the whole area of computer crime and the ambiguity of the law in this area. This is also confused by the potential international legal implications of foreign attacks. For instance, in the state of New South Wales, the *Crimes Act 1900 (NSW), Section 310* states it is illegal to 'destroy, erase, insert, or alter data in a computer system...or interfere with, interrupt, or obstruct the lawful use of a computer' (Internet Law Bulletin, 1998, p.14). However, it is rare for these offences to be detected, prosecuted, or proven. Morth (1998) further argues that although this form of information warfare may be illegal in international law, it is only states that are covered by this, not individuals or companies (for which there is no international law in this area).

The perception of information warfare at the state or corporate level is to obtain as much benefit as possible and cause as much damage as possible to the 'enemy'. Thus the intent is usually destructive; this is very different to the hacker code of ethics. The reason for this is the emergence of cyberspace attack as the critical ingredient in a new witch's brew of strategic conflict capability. Information warfare tools and techniques allow the potential to destroy communications, information dissemination, and the functioning of critical equipment with no reference to geography or an ability to *physically* destroy anything in the conventional sense. Such a capability poses a whole new kind of threat to international stability (Molander and Siang, 1998). This destabilising potential can equally have an organisation or individual as its targeted victim.

CONCLUSIONS

Information warfare has shifted the ethical issues from a naive group of technically, oriented, young individuals (hackers, etc.) to the organisational arena. The implications of this shift from the relatively benign impact of individual behaviour to that of organised groups has raised the magnitude of the ethical issues surrounding them. They need to be considered at both the legal and policy making levels of national, international, and corporate institutions before practices become entrenched or cause irreversible damage. But how feasible in reality would this approach be. The impact of hackers could be the destruction of a few number of information's system, the impact of Information Warfare could be the widespread destruction of a entire countries information systems network, the ethics behind these viewpoints and actions are completely different.

REFERENCES

Adams, J. (1998) *The Next World War*, Hutchinson, London

Caelli, W., Longley, D., Shain, M. (1989) **Information Security for Managers**, Stockton Press, New York, USA.

Cobb.A. (1998) **Australia's Vulnerability to Information attack: Towards a National information Policy** Strategic and Defence Studies Centre working paper #310, Australia National University, Australia.

Denning, D.E. (1999) **Information Warfare and Security**. Addison-Wesley, New York.

Grace, D., Cohen, S. (1998) **Business Ethics – second edition**, Oxford University Press, Melbourne.

Ignatieff, M. (2000) **Virtual War**, Chatto & Windus, London.

Internet Law Bulletin. (1998). 'Guilty Plea on Inserting Data Charge'. **Internet Law Bulletin**, **1**(1).

Lagan, B., Power, B (1999) ASIO Cleared to Hack into Computers, **Sydney Morning Herald**, 26 March, 1999.

Levy, S (1994). **Hackers:Heroes of the Computer Revolution**. Unknown, ISBN 0385312105.

Main, B. (2000) Information Warfare: and its Impact on the Information Technology Industry in New Zealand, **Proceedings of the NACCQ**, Wellington, New Zealand.

Mizrach S (1997) **Is there a Hacker Ethic for 90s Hackers?** URL: www.infowar.com Molander R, and Siang S (1998). The Legitimization of Strategic Information Warfare:Ethical Consideration, **Professional Ethics Report, XI**(4).

Morth, T.A. (1998) 'Considering our Position: Viewing Information Warfare as a use of Force Prohibited by Article 2(4) of the U.N.Charter', **Case Western Reserve Journal of International Law**, **30**(2,3), pp. 567-600.

Parker, D. (1976) **Crime by Computer**, Charles Scribner Sons, USA.

Schwartau, W. (2000) **Cybershock**. Thunder's Mouth Press, New York, USA.

Schwartau, W. (1994). **Information Warfare: Chaos on the Electronic Superhighway**. Thunder's Mouth Press, New York, USA.

Waltz, E. (1998) **Information Warfare – Principles and Operations.** Artech House, Norwood.

Warren, M., Hutchinson, W. (2000). **Information Warfare: Fact or Fiction**. SEC2000, IFIP World Congress, Beijing, China.