Proceedings of the NACCQ 2000
Wellington NZ www.naccq.ac.nz

INFORMATION WARFARE
and its impact on the Information Technology Industry in New Zealand

Brian Main

The Waikato Polytechnic
Itbjm@twp.ac.nz

ABSTRACT

The term information warfare is used to cover a broad spectrum of offensive and defensive operations that include Electronic Warfare, Cyber-Terrorism, Hacker Warfare, Soft Warfare, and Psychological Operations.

The objective of this paper is to draw attention to the threat that Information Warfare poses to the New Zealand Information Technology industry and to stimulate interest in offering a course of study on the topic at Diploma and/or at fourth year Degree level. Such a paper would be based on courses currently offered in universities overseas and could include a comprehensive and coherent treatment of offensive and defensive Information Warfare operations in terms of actors, motivations, targets, methods, technologies, outcomes, policies, and laws.

Keywords

Information Warfare, New Zealand, Information Technology Industry, Electronic Warfare, Cyber-Terrorism, Hackers, Cyber-Criminals, Soft-Warfare, Psychological Operations, Script Kiddies, intellectual property, Economic Espionage, Intelligence Community,

"A popular Government, without popular information or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or perhaps both. Knowledge will forever govern ignorance; And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives."

James Madison to W. T. Barry
4 August 1822

1. INTRODUCTION

This paper will introduce the concepts and components of Information Warfare (IW), identify those groups who indulge in it and discuss their motivations. The paper will go on to assess the threat that these groups pose to New Zealand interests and then conclude with some observations and recommendations.

Information Warfare (IW) involves operations that target or exploit information media to win some objective over an adversary or to create a mischief. Publicity over Y2K concerns have, if nothing else, raised the consciousness of New Zealanders about our nation's dependence upon computer driven systems. It is now clear that computers pervade every aspect of New Zealand life, ranging from defence and the national economy to the kitchen and the bathroom.

Although in recent years information warfare has captured the attention and the imagination of government officials, defence analysts, and some elements in the information technology industry, it has not been the concern of industry and commerce or the general public. New Zealand's Y2K preparations revealed our dependence

upon computer-based systems and our vulnerability to their failure. Yet it took the "Love Bug"(1) to alert the public in general, and commerce in particular, to the potential threat posed to information security by hackers and terrorists. Hackers and information terrorists, armed with little more than a PC and a mouse can hack into computer systems and potentially cause national blackouts, disrupt the telephone service, crash an automatic banking system and destroy an air-control system. Their targets are limited only by their imagination, and their potential for disruption is seemingly limitless. Ultimately they could collapse the New Zealand economy.

New Zealand's dramatic increase in the use of the Internet in general and of e-commerce in particular (2) has created additional vulnerabilities. Although so far

New Zealand web sites have, in the main, escaped the attention of most hackers, other nations have not been so lucky. Over three consecutive days, commencing on the 7 February 2000, malicious hackers crippled nine popular commercial Web sites.

These Web sites included ZDNet, the E*Trade Group, Amazon.com, CNN.com, Yahoo, eBay, and Buy.com.

2. WHAT IS INFORMATION WARFARE?

It has been argued that as a separate technique of waging war, Information Warfare does not exist. There are, instead, several distinct forms of IW, each laying claim to the larger concept. (3) This argument goes on to identify seven forms of information warfare that involve the protection, manipulation, degradation, and denial of information that together embody what is described as information warfare. These seven forms include:

- Command-and-control warfare, which strikes at the enemy's head (Command) and neck (Communications).
- Intelligence-based warfare, which consists of the design, protection, and denial of systems that, seeks sufficient knowledge to dominate the battlespace.
- Electronic warfare, radio-electronic and cryptographic techniques.
- Psychological warfare, in which information is used to change the minds of friends, neutrals, and foes. Soft-war is a particular electronic application.
- Hacker warfare in which computer network systems are attacked.
- Economic information warfare which involves blocking information or channelling it to pursue economic dominance.
- Cyberwarfare in which cyberspace is blocked, corrupted, or destroyed.

Although historically it is true that all these forms of IW have been weakly linked, the Persian Gulf War, the first Information Age War, deployed them in an integrated way never experienced before, and forever galvanised them into a coherent and powerful weapon system. (4)

The components of information warfare range considerably in maturity from the historic to the fantastic, and up to the end of the Cold War were confined to military and intelligence operations. However, since the end of the Cold War sophisticated Military technologies and expertise have become available on the open market and are being used together with operating methods, hitherto confined to intelligence agencies, to attack commercial enterprises.

3. WHO ARE THE PLAYERS AND WHAT ARE THEIR MOTIVATIONS?

Those who indulge in Information Warfare can be divided into four main categories: the hackers, the criminals, cyberterrorists, and the intelligence community.

3.1 The Hackers

This group comprises mainly of teenagers, for the most part, young males. Teenage boys, and some girls, have always been driven by a desire for adventure, danger, and excitement, so it is not surprising that they find computer systems an irresistible playground. Modern technology offers endless opportunities for exploration and presents countless challenges. Commonly referred to as Hackers, these youngsters, armed with little more than a PC and a modem, can play in a cyber realm of fantasy while hiding behind a cloak of anonymity.

Young Hackers are motivated by a variety of factors, including thrill, challenge, pleasure, knowledge, recognition, power, and friendship. In the words of a hacker interviewed in 1990: (5)

> "Hacking was the ultimate cerebral buzz for me. I would come home from another dull day at school, turn my computer on, and become a member of the hacker elite. It was a whole different world where there were no condescending adults and you were judged

by your talent. I would first check in the private bulletin boards where other people who, like me, would hang out, see what news was in the community, and trade some info with people across the country. Then I would start actually hacking. My brain would be going a million miles an hour and I'd basically completely forget about my body, as I would jump from one computer to another trying to find a path into my target. It was the rush of working on a puzzle coupled with the high discovery many magnitudes intensified. To go along with the adrenaline rush was the illicit thrill of doing something illegal. Every step I made could be one that would bring the authorities crashing down on me. I was on the edge of technology and exploring past it, spelunking into electronic caves where I wasn't supposed to be." (6)

Most Hackers range in age between 15 and 24 and only 5% are female. (7)

Hackers fall into two groups: script kiddies and real hackers.

- **Script Kiddies** are mostly teenage boys who use powerful software tools and little skill to perpetrate some of the most destructive attacks on the Internet and do little to cover their tracks. Matt Yarbough, a former U.S. cybercrimes prosecutor now in private practice says. "Script Kiddies are point-and-shoot hackers....When they get into systems, they don't know what they're doing, and that makes them more dangerous than a lot of real hackers...[they're like] a bull in a china shop." (8). Over three consecutive days, commencing on Monday 7 February 2000 malicious hackers crippled nine popular commercial Internet sites. These attacks started on Monday with Yahoo. Tuesday saw Buy.com, Amazon.com, eBay, and CNN.com, under attack. And Wednesday, technology site ZDNet and online trading site the E*Trade Group sites suffered attacks. On the 15th April 2000 a 15-year-old Canadian boy who goes by the name "Mafiaboy" was arrested in connection with the February attacks on major Web sites. Mafiaboy has been charged, under Canadian criminal law, with two counts of "mischief to data". This 15-year-old is alleged to have claimed credit not only for the CNN.com attack but also E*TRADE and several smaller sites. (9)
- By contrast **real Hackers** are more experienced youths who write the software tools that the Script Kiddies use. They hide in systems and spy on data and quietly hide their tracks. The hacker community disdains the teenage vandals, says Brian Martin, a security consultant involved with attrition.org, a clearinghouse of hacking-related information.

"A hacker is interested in learning and exploring.... The key is that they understand the tools they use, and in most cases write them. Script Kiddies blindly download those tools, have no comprehension of what they do, how they do it or the fundamental reasons they work..." he says. (10) Yet hackers feed the Script Kiddies by making the tools they use to break into systems. Hackers defend their activities by claiming that security professionals can analyse those tools and use them to identify insecurities among corporate and government Internet sites and create more secure systems. This is true, but that is no more a justification for hacking than housebreaking can be justified on the grounds that it alerts the house-dweller to secure their property.

Unfortunately, a "hacker's culture" has developed. Hackers operate and hang out on Internet Web sites, e-mail distribution lists, chat channels, FTP (File Transfer Protocol) sites, newsgroups, and computer bulletin boards. They also publish magazines, most of which are electronic. Hackers use these facilities to learn their art, exchange ideas, trade tips and software tools, and plan attacks. One can learn how to break into computer systems, evade detection, steal phone services, listen to private calls and even how to crack a TV scrambler.

Hackers exploit weaknesses in laws as well as vulnerabilities in technology and human frailty. Juveniles are generally immune from prosecution, and in some countries hacking is not a crime. In New Zealand the minimum age a person can be prosecuted for offences other than murder and manslaughter is 14 years, compared to 18 in the US. However unlike the US, the UK, Australia, Canada and Singapore, computer hacking as such is not illegal in New Zealand. In November 1998 a New Zealand hacker erased some 4,500 "Ihug" web sites. The Ihug server was based in California and Auckland-based internet service provider (ISP) the Internet Group hosted the sites. There were no backup facilities and, unless the owners of the web sites made their own copies, the web pages were lost permanently. (11) It was reported that Ihug were considering extraditing the hacker and prosecuting him in the United States as New Zealand law was "inadequate to deal with Cyber-vandalism". However the hacker, tagged "Sharkdogg", was only a 15-year-old, too young for prosecution in the U.S. (12).

The New Zealand Law Commission, in their Report 54: Computer Misuse, tabled in the House of Representative on 13th May 1999, strongly recommend

that four new offences dealing with computer misuse should be added to the Crimes Act 1961.

The new offences recommended by the New Zealand Law Commission are:

- Unauthorised interception of data stored in a computer.
- Unauthorised access to data stored in a computer.
- Unauthorised use of data stored on a computer.
- Unauthorised damaging of data stored in a computer (13).

Most hackers eventually become distracted by other challenges, the opposite sex for example, and by the time that they reach the age of 18, they have moved on to other adventures(14). Those hackers who continue tend to drift into serious acts of fraud and sabotage and are supported by an entire underground culture. Almost every day we hear of hackers trafficking in stolen credit card numbers ("carding") and pirated software ("warez"). Such people drift into the professional ranks of "Cyber-criminals".

3.2 Cyber-Criminals

This group includes individuals and organisations that are motivated by money. Their criminal activities include intellectual property crimes and fraud.

Crimes against intellectual property include piracy and theft of trade secrets. Although many people pirate software and other copyright materials for their own use, there is a substantial criminal element that seeks to profit from the mass production and sale of pirated goods. The stakes are incredibly high. According to the Intellectual Property Alliance (API), U.S. copyright industries lost between US$18 billion and US$20 billion in revenue in 1996 to pirates. Yet these figures pale into relative insignificance when one reviews the impact of Industrial Espionage. The American Society for Industrial Security (ASIS), in a survey that they conducted over 1997/98, revealed thefts of information related to research and development, manufacturing, marketing plans, and customer lists that exceeded US$250 billion (15). New Zealand has a significant number of trade secrets too, and as a country that relies on foreign trade for survival, their loss to trading competitors could have a devastating impact on the national economy.

The Risk Elements: The same ASIS survey also identified the groups that posed the highest risk to the security of corporate trade secrets. These included former employees, temporary staff, current employees, vendors, suppliers, and consultants. Other identifiable threats include hackers, domestic and foreign competitors and foreign intelligence services (16).

New Zealand law does not explicitly address the theft of trade secrets. Prosecutors are forced to apply laws designed for other purposes making convictions more difficult to obtain. In 1996, the U.S. Congress passed the Economic Espionage Act of 1996. This Act was designed to provide more robust protection of trade secrets at the federal level. The law makes it illegal for anyone to knowingly steal or otherwise fraudulently obtain a trade secret, to copy or distribute a trade secret, to receive or buy a trade secret, or to attempt or conspire to commit one of these acts in order to benefit a foreign government, instrumentality, or agent or convert the trade secret to the economic benefit of anyone other than the owner. New Zealand needs such an Act.

Fraud: Crimes of electronic fraud include telemarketing scams, identity theft, stealing telecommunications services, and bank fraud. In the U.S. telemarketing fraud is estimated to cost consumers US$40 billion a year (17). It is difficult to assess the extent of telemarketing fraud over the internet in New Zealand as all known cases originate overseas and citizens lose the protection offered by the Consumer Guarantees Act 1993 and the Fair Trading Act 1986. Most crimes of this type in New Zealand go unreported.

State of the Art: The technical resources used by companies that specialise in economic espionage and fraud spring increasingly from the most sophisticated military technologies and copy operating procedures confined, up to now, to intelligence agencies. So how did these companies acquire this technology and expertise?

In the decade that followed the end of the Cold War significant changes in Russia impacted on the KGB 'Komitet Gosudarstvennoy Bezopasnosti', which means Committee for State Security. The 8th and 16th Directorates, roughly representing the Russian equivalent of the U.S. NSA (National Security Agency) and the British GCHQ (Government Communications Headquarters), became an independent agency, the Federal Agency of Government Communications Information (FAPSI, as a Russian acronym). Although the FAPSI is directly subordinate to the President of Russia, it got caught up in a wave of privatisation and was partially privatised. Some of the leading FAPSI experts left the agency and founded private security companies, taking some of the best officers, at all levels, along with them. These companies cater mainly to Russian private financial institutions and provide a wide range of security services. Yet they are fully capable of carrying out any defensive and offensive operations. The technology and know-how that was historically in the hands of a small number of intelligence experts in a few countries is now in the market place, and the economic conditions in Russia make

a sizeable cash offer, from well funded organised crime syndicates and terrorist groups, tempting.(18).

3.3. Cyber-Terrorists

Terrorism is the use or threat to use violence to intimidate or coerce societies or governments. Motivated by ideology or political objectives, it is conducted by individuals or groups. The February 26, 1993, bombing of the World Trade Centre in New York revealed a new breed of terrorist. Unlike the tightly disciplined cells that dominated terrorism hitherto, they function in a loosely organised ad hoc manner. This new breed is prepared to strike far from their homelands.

Radical Islamic movements have mushroomed not only in the Muslim world, but also among Muslim immigrants in the West. Ironically, they are drawn to the West by economic opportunities and political freedoms, yet they reject Western values and what they consider to be its degenerate culture of materialism and secularism. Radical Islamic movements outlawed in their own countries have found sanctuary in the West where they are free to express their political views (19). Many of this new breed of terrorist have turned to the armoury of information warfare to pursue their objectives. Amongst this group is the cyber-terrorist.

" Cyber-terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by subnational groups or clandestine agents" (20). In a closed briefing before the U.S. Congress in the summer of 1998, Central Intelligence Agency (CIA) head George Tenet warned that "...at least a dozen countries are working on information warfare programs intended to give them the capability to attack another nation's computer systems". Tenet had a sobering conclusion: computer-controlled financial, water, sewage, power, and telecommunications systems are vulnerable (21). New Zealand utilities are no less vulnerable to attacks from terrorists or hostile countries. Who then protects the national infrastructure?

3.4. The Intelligence Community.

Information warfare covers operations undertaken by states and by nonstate players against states. These include foreign intelligence operations, war and military operations, acts of terrorism, and netwars. The first responsibility of any government in a democracy is the security of its citizens. That security cannot be taken for granted and most nations have some form of arrangement in place to warn the administration about threats that could endanger their people, and can, take steps to minimise them. New Zealand is no exception and has a small group of intelligence agencies that form our intelligence community.

The New Zealand Intelligence Community: The four agencies that make up New Zealand's intelligence and security community are:

- The New Zealand Security and Intelligence Service (SIS).
- The Government Communication Security Bureau (GCSB).
- The External Assessments Bureau (EAS), which is part of the Department of the Prime Minister and Cabinet.
- The Directorate of Defence Intelligence and Security (DDIS).

The GCSB and the DDIS, together with the Armed Services, possess most of the information warfare assets that New Zealand employs.

The GCSB is responsible for signals intelligence (SigInt.), that is the interception and analysis of foreign communications and other signals such as radar. GCSB also provides advice and assistance to Government on the security of New Zealand's official communications and information technology systems (INFOSEC) (22).

The majority of New Zealand's information warfare assets are devoted to **Electronic Warfare**. Electronic Warfare has three components, Electronic Support Measures, Electronic Countermeasures, and Electronic Counter Counter Measures.

Electronic Support Measurers (ESM) includes:

- **Monitoring** the Electro-magnetic frequency spectrum listening for radio, radar, and other signals that may contain useful intelligence. Once a signal of interest is located it is recorded and analysed for any intelligence that it may contain. This is referred to as Signals Intelligence or Sig Int;
- **Locating** the geographic position of the site emanating the signal. This is called Direction Finding or DF;
- **Jamming** involves disrupting the enemy's, communications, air-defence, and weapons systems, by jamming them with high-powered signals etc;
- **Deception**, which can involve joining an enemy communications network or intercepting a signal, reprocessing it and then passing it on through the enemy communications system as if it was a legitimate message, also called **Cooking;**
- **Electro-magnetic bombs** that include radio frequency (RF) Electro magnetic impulses that can

damage or destroy the electronic componentry of a computer that is not connected to a network (23).

- **Computer viruses** that include, Worms, Trojan Horses, Logic Bombs, and polymorphic viruses.

Electronic Counter Measures (ECM) includes: Encryption, frequency-hopping, burst-transmissions, reducing transmitter power, employing directional antennas, and eliminating spurious Electro-magnetic radiation which is referred to as **Tempest**.

Electronic Counter Counter Measures (ECCM), which includes cryptographic code breaking and generally stopping the enemy from doing to you what you are doing to them.

4. THREAT ASSESSMENT

While the possibility of a serious threat to New Zealand's physical security is unlikely, recent events relating to the "love Bug" have demonstrated how vulnerable we are to an electronic attack. Although New Zealand itself is currently an unlikely target for terrorists, foreign interests resident in New Zealand are. In 1999, there were 392 international terrorist attacks. Of these 392 attacks, 169 were directed at U.S. interests (24). As the U.S. tightens its security systems, terrorists will seek "softer" targets. American and British companies and other interests resident in New Zealand may well become a target.

Organised crime may also see us as easy prey as other Western countries tighten up their systems. The absence of an appropriate Economic Espionage Act in New Zealand will make us more attractive as it reduces the chance of a prosecution.

Hackers may find more challenges in attacking the large U.S. and European sites, but New Zealander's complacence will furnish them with countless "zombies" (compromised computers) in New Zealand with which to perpetrate their "denial of service" attacks on sights elsewhere.

Script Kiddies will attack us by default as they did with their "Love Bug", the "Melissa" virus and the February DOS attacks.

The threat of massive damage to e-commerce in particular would be reduced if New Zealand possessed **Computer Emergency Response Teams (CERT)**, similar to those operation in the U.S. These teams are available 24 hours a day 7 days a week to react immediately when a cyber attack is detected. There is an Australian CERT based at the University of Queensland that is active in New Zealand. However, because of the distances involved and the scope of their capabilities their service to New Zealand customers is limited.

"**Complexity and complacency are the enemy of security"**, according to Auckland security consultant, Peter Benson. Complex systems are dangerous; they offer too many opportunities to the experienced hacker (25). "Ninety five per cent of security exploits happen through known exploits", Mr Benson says. "The key to security is vigilance and diligence. Vigilance in identifying what's happening in the industry, the political environment and the technical environment, and guarding around it, and diligence in ensuring that when exploits are published your systems are patched". The February **"denial of service"** (DOS) attacks that many large companies, such as ZDNet, E*Trade Group, Amazon.com, CNN.com, Yahoo, and eBay, experienced came about through the use of **"zombies"** around the world being synchronised into flooding targeted sights with traffic. Mr Benson says New Zealand companies need to **"wake up and smell the daisies....** The biggest problem is lack of awareness or denial that these things could happen here" (26).

5. CONCLUSION

New Zealand Parliament must enact the recommendations in the **Law Commission's Report 54**: Computer Misuse and in addition develop a new Act that specifically addresses **Economic Espionage.**

New Zealand Polytechnics and Universities should follow the lead of the U.S., the U.K., and Australia and establish Computer Emergency Response Teams (CERT).

The Government Communications Security Bureau's Information Security mandate should be extended to include advice to e-commerce and other civilian organisations, and allow them to establish a CERT Centre and play a national role in co-ordinating Computer Emergency Response Teams.

Polytechnics and Universities should develop a programme of study on Computer Systems Security at Diploma and/or fourth year Degree level. Such studies could be based upon courses currently offered on this and related topics at Universities in the U.S. The programme could include a comprehensive and coherent treatment of offensive and defensive Information Warfare operations as applied to Computer Systems in terms of actors, motivations, targets, methods, technologies, outcomes, policies, and laws.

New Zealand information technology specialists must recognise that vigilance and diligence are the key to information security and that complexity exacerbates security hazards. Where possible "keep it simple" **(KIS)**

6. ENDNOTES

1. Barton Chris, **Lightning cyber hit**, The New Zealand Herald, Weekend Herald, Section A, 6 May 2000, p.1. A **"worm",** referred to as **The Love Bug virus**, was reported on the Internet at 2 p.m. on Thursday 5 May 2000. The "worm", spread by e-mail, struck businesses, organisations and individual users of Windows-based PCs worldwide. Most damage came from the flood of e-mails generated by the worm, causing mail servers to be overloaded and shut down. It also destroyed music and picture files on infected computers. The most worrying aspect of the Love Bug was the speed at which it spread around the globe. New Zealand's Telecom Internet Service Provider (ISP) Xtra was deleting the virus at a rate of 2 a second by Saturday 6 May. Amongst the victims of this self-replicating virus, were:

Britain: The House of Commons, Barclays Bank, Britishtelecom, the BBC and News International.

Europe: Denmark's Parliament, ministries and major television companies.
Switzerland's Government and several banks.
Germany estimated that up to 80 per cent of computers were hit.
The virus also hit several unnamed European publishing companies
that lost digital photo archives and a Central European radio station which lost its music library.

United States: The officers of Microsoft, Ford, Archer Daniels Midland, Vodafone, AirTouch, and the Mayo Clinic medical centre in Minnesota. In addition, The Pentagon, The CIA and the White House were attacked although no classified systems were penetrated.

Damage in the tens of billions, of dollars from lost data, interrupted work, and the cost of fixing the problems are already reported.

2. There are 120 Internet Service Providers (ISPs) in New Zealand, New Zealand Herald, Thursday April 20, 2000, P. B3. The National Business Review (NBR) reported that, according to Intel, electronic commerce will be worth US$1 trillion by 2002, NBR, February 26 1999.

3. **Libick Wartin,** What is Information Warfare?, Institute for National Strategic Studies, National Defence University, Washington, D.C., August 1995, p.1.Electronic copy available at http: //www.ndu.edu/ndu/inss/actpubs/act003/a003ch00.html
4. **Summers Harry G. Jr.**, A Critical Analysis of the Gulf War, Dell Publishing, New York, 1992, p.1.**6.**
5. **Denning Dorothy E.,** Information Warfare and Security, AACM Press, New York, 1999, p.45.
6. **Denning Dorothy E.,** Concerning Hackers Who Break into Computer Systems, Proc. 13th National Computer Security Conf., pp.653-664, Oct. 1990.
7. **Chantler Nicola**s, Profile of a Computer Hacker, Faculty of Law, Queensland University of Technology, Australia, ISBN 096287000-2-1, electronic copy available at http://www.infowar.com.
8. **Segan Sascha,** Tracking Mafiaboy's Steps, ABC News.Com, 30 April 2000, pp. 1-2. electronic copy available at http://www.abcnews.go.com/sections/tech/DailyNews/webattacks000420.html
9. **Dube Jonathan, and Ross Brian**, 'Mafiaboy' Arrested, ABC News.com, 19 April 2000. electronic copy available at http://www.abcnews.go.com/sections/tech/DailyNews/webattacks000419.html
10. **Segan Sascha**, Ibid., p.2.
11. **The Wellington Dominion**, Hacker wipes out Web sites, 19 November 1998.
12. **The Wellington Dominion**, Teenage hacker faces extradition bid, 21 November 1998.
13. **Law Commission**, Report 54:Computer Misuse, 13 May 1999, para. 89. Electronic copy available at http://www.lawcom.govt.nz/pub_index.html
14. **Denning Dorothy E.,** op.cit., P.50.
15. **ASIS 1997/98** Trends in Intellectual Property Loss, American Society of Industrial Security, press announcement, 10 May 1998. Electronic copy available at http://www.asisononline.com. An earlier announcement on 16 January 1998 said the losses were estimated to be over US$300 billion. See also, ASIS Study Verifies Risks and Trends, Computer Society Security Alert, No. 184, July 1999, p.3.
16. **Annual Report to the U.S. Congress**, Foreign Economic Collection and Industrial Espionage 1996, May 1996, citing "Trends in Intellectual Property Loss", American Society of Industrial Security, International, March 1996.
17. **Schneider Howard,** "Telemarketing Scams Based in Canada Increasing Targets U.S. Residents", Washington Post, 24 August 1997. P.A21.

18. **Sheymov Victor,** "The Low Energy Radio Frequency Weapons Threat to Critical Infrastructure", a submission to the Joint Economic Committee, United States Congress, 20 May 1998, p.4. (Victor Sheymov defected to the U.S. from the Soviet Union in 1980. At the time he was a Major in the 8th Directorate of the KGB.) electronic copy available at http://www.house.gov/jec/hearings/intell/sheymov.html
19. **Phillips James**, "The Changing Face Of Middle East Terrorism", The Heritage Foundation, Backgrounder #1005, 6 October 1994, pp. 4-6.
20. **Pollitt Mark M.**, "Cyberterrorism-Fact or Fancy?", Proceedings of the 20th National Information Systems Security Conference, October 1997, pp.285-289.
21. **Nelan Terrence**, "Tools of the Terror Trade", ABCNEWS.com, 15 January 1999, p.3. electronic copy available at http://www.abcnews.go.com/sections/world/DailyNews/terror_tech991101.html
22. **The New Zealand Intelligence Service,** Produced by the New Zealand Security Intelligence Service, P.O. Box 900, Wellington, April 1998, p.8.
23. Leaving physical destruction of computers aside, information warfare attacks on computers can be classified as attacks through legitimate gateways of computers such as the modem and the keyboard (software attacks), or attacks through other than legitimate gateways (backdoor). Backdoor attacks are mainly perpetrated by utilizing radio frequency electromagnetic energy, and this type of attack can be devastating. Areas like air traffic control, commercial airlines, energy and water distribution systems are vulnerable to this type of attack because they are seldom part of a computer network and therefore regarded as secure. **Sheymov Victor**, Ibid., pp.1-3.
24. **Patterns of Global Terrorism: 1999**, The Year in Review, Department of State, Office of the Secretary of State, Office of the Coodinator for Counterterrorism, Department of State Publication, April 2000. electronic copy available at http://www.state.gov/www/global/terrorism/1999report/review.html
25. The Windows 2000 operating system is said to have between 30 and 45 million lines of code. Current bug rates for normal application software is up to one bug per thousand lines of code.
26. **Wright Heather,** "New Zealand Companies Not Exempt From Security Attacks", NZ INFOTECH WEEKLY, Ed.2, 1 May 2000, p.10.