

E-Government

**Protecting New Zealand's Infrastructure
From Cyber-Threats**

8 December 2000

EXECUTIVE SUMMARY

This report discusses the extent of protection of New Zealand's critical infrastructure from information-related threats, such as are posed by unauthorised access to computer systems, viruses and damage to telecommunications links. A recommended strategy to bring levels of protection in line with international practice is presented.

Critical infrastructure is that which is necessary to deliver services whose absence would adversely affect New Zealand's national or economic security, or have adverse effects on a large proportion of the population.

Much of this infrastructure is in private ownership, some is owned by State-Owned Enterprises, and some is owned by (or under the control of) government departments and other agencies. Whatever the ownership, it is appropriate for the Government to assure itself that infrastructure critical to New Zealanders is being adequately protected.

This report provides a list of information-related threats and discusses the extent to which various parts of New Zealand's critical infrastructure are seen to be vulnerable to these threats. It is not exhaustive or detailed; rather it serves as a signpost to issues that need to be watched. Owners of critical infrastructure have already performed a formal risk analysis for their Year 2000 readiness, and some maintained and extended this as an ongoing process. This report recommends, among other things, that all critical infrastructure owners be encouraged to maintain risk assessments covering information related threats for their infrastructure.

Certain risks are highlighted below: the relocation of critical banking facilities offshore; the management of power distribution networks; the vulnerability of offshore telecommunications links; and denial of service attacks on the Internet. This is not to imply that those responsible for these areas are in any way delinquent, or that unacceptable risks are being taken, but rather that there are complex threats and vulnerabilities that merit further investigation.

Banking Facilities

Banks have always been highly conscious of the need for security. All banks and interchange facilities spoken to were confident about the security of their core systems and Internet sites.

The main area of concern identified is the desire of some New Zealand banks to move their retail processing offshore. At least one has already done this and others are reportedly considering the move. The Reserve Bank of New Zealand is planning to move the computers for its real time gross settlement system to Australia. This system manages the relative position of all New Zealand banks and is core to the banking system. The computers for the Austraclear system, currently operated by the Reserve Bank, are also being moved to Sydney. Austraclear is the main means of settling debt securities transactions in New Zealand and is crucial to the New Zealand financial markets. Billions of dollars flow through it daily.

There are two main risks in the movement of banking systems offshore. Firstly, adverse events in Australia, such as industrial action, would be outside any New Zealand control yet could have a highly adverse impact here. Secondly, trans-Tasman telecommunications circuits or their local (Australian) links to the computer systems, although much improved in robustness and diversity, might fail leaving New Zealand disconnected from its banking system.

Power Distribution

Electricity is transmitted from generators around the country and delivered to local distribution networks by Transpower New Zealand Ltd, a state-owned enterprise. Transpower has two fully staffed operational Centres providing full operational backup and one, normally unstaffed, management support centre that can provide additional resources in the event of a widespread disaster. Operation of the national grid does not have heavy reliance on external telecommunications suppliers since Transpower owns a significant proportion of its communications links.

Transpower takes its responsibilities in respect of continuity of supply extremely seriously. However, with the increasing reliance on information technology to manage the power distribution network there may be a need for greater central focus on the IT security aspects of network design. In recognition of this issue Transpower has recently established an executive level committee to drive security in all parts of its network, and is drawing on work done in the US to consider information-related threats and vulnerabilities to its operations.

The project team has been unable to gather any information about the protection of electricity lines companies' infrastructure assets. Given that there are several such companies, each with an effective monopoly in their respective areas, there would appear to be scope for industry co-operation to provide mutual assurance of infrastructure security.

Offshore and Inter-Island Telecommunications Links

These links primarily use submarine cables. Cables are long and exposed to damage by shipping, as has occurred recently on a cable affecting Australia. Perhaps uniquely for a developed nation, New Zealand is dependent on the continuous availability of offshore telecommunications links, because key parts of its banking system are moving or have moved to Australia.

The latest cable, Southern Cross, being commissioned as this report was being prepared, is designed to be far more reliable than the older ones, partly because it offers at least two paths between any pair of locations. If the trans-Tasman part of the cable were severed, data would flow between New Zealand and Australia through Hawaii. Once this cable is fully commissioned the risk of isolation will be greatly reduced.

Inter-island telecommunications cables are particularly vulnerable. Presently there are only two, which are laid reasonably close together across the sea-bed (rather than buried) in relatively shallow water. They have been damaged more than once. There is a microwave backup, but it lacks sufficient capacity to replace the cable. Loss of inter-island telecommunications would have a very serious impact on New Zealand.

Resource consent is currently being sought for two separate high capacity inter-island cables to be buried in the sea bed along different routes. It is hoped that they will be commissioned in 2001. Once implemented, these will greatly improve the security of inter-island communications.

Denial of Service Attacks on the Internet

Denial of service attacks, in which a target computer is flooded with requests it cannot meet, are becoming a common feature of the Internet. As their name suggests, these attacks result

in the services normally offered by the target computer becoming unavailable. They also result in degraded or denied service to other customers of the same Internet Service Provider as the target and may cause wider degradation of service on the New Zealand Internet. The addition of new offshore bandwidth in the form of the Southern Cross cable may exacerbate this problem since it permits a greater volume of requests to be used by an attacker.

Tracing a denial of service attack to its ultimate source is difficult and requires considerable detective skills as well as the cooperation of many different Internet Service Providers globally while the attack is under way. Defending against them is technically difficult. Denial of service is currently the most worrying attack type on the Internet. This is a volatile area, and one which needs up to date information and a reasonable degree of cooperation to manage.

Conclusion and Summary of Recommendations

The Government cannot afford to ignore the security of New Zealand's critical infrastructure, or to leave it to solely to commercial pressures. It needs to take a role in at least monitoring, and ensure that the expertise and knowledge necessary to manage risks in this environment are available to New Zealand infrastructure providers.

The recommendations of this paper are set out on page 24. In summary, they are aimed at:

- building New Zealand capability and knowledge in respect of security and incident handling;
- deterring attacks through legislation and enforcement;
- promoting standards for risk management and security in infrastructure; and
- requiring government agencies to adopt appropriate information technology security measures.

CONTENTS

Executive Summary	2
Banking Facilities	
Power Distribution	
Offshore and Inter-Island Telecommunications Links	
Denial of Service Attacks on the Internet	
Conclusion and Summary of Recommendations	
Introduction	6
Critical Infrastructure	
New Zealand's Critical Infrastructure	8
Ownership of Infrastructure	
Risks in Critical Infrastructure	
IT Threats to Critical Infrastructure	
Vulnerability of Infrastructure to IT-Borne Attacks	
Availability of IT Security Staff	
Legal Issues	
The Current State of Infrastructure Protection in New Zealand	15
Finance and Banking	
Transport	
Electric Power	
Telecommunications and the Internet	
Oil and Gas	
Emergency and Government Services	
Water	
Infrastructure Protection Programmes in Other Countries	22
Summary of other National Programmes	
United States of America	
United Kingdom	
Australia	
Canada	
Recommended Strategy	24
Recommendations	
Glossary	26
Appendix I - Bibliography	29
Web Sites Researched	
Appendix II – Contributors and Consultations	31
Project Team	
Experts Group	
Consulted	

INTRODUCTION

In December 1999 the Chief Executives Group on Information Management and Technology provided you with a briefing¹ on issues emerging under the banner of 'electronic government' ('e-government'). On 1 May 2000 Cabinet approved an E-Government Vision Statement² and allocated to the State Services Commission the lead responsibility for oversight and coordination of the e-government programme. An E-Government Unit was established within the Commission to discharge this responsibility.

This report is presented in accordance with Output 3.1.6 of the 2000/2001 State Services Commission Purchase Agreement:

Report assessing current infrastructure protection for government and recommending a strategy to improve it.

The term *infrastructure* is broad. This report considers only the infrastructure necessary to deliver services whose loss would have great impact on New Zealand or a significant section of the population, referred to as *critical infrastructure*.

The focal issue is the protection of the IT systems upon which each of the critical infrastructure components relies for its operations. To safeguard the infrastructure, information assurance measures need to be applied to the systems, viz.: critical data must be protected from improper disclosure (confidentiality), the data and systems must not be open to unauthorised manipulation or change (integrity), and the systems and data must remain always accessible by the infrastructure owner and users (availability). The critical infrastructure must be protected from cyber-threats, i.e. threats borne by electronic means, such as attacks by "hackers"³ or computer viruses, or on other threats to electronic communications, e.g. damage to submarine cables. This paper does not provide the solutions to this problem; rather it provides a top-level assessment of vulnerabilities of the critical infrastructure to cyber-attack, and identifies areas for further action or consideration.

Critical Infrastructure

By *critical infrastructure* this report means infrastructure necessary to provide critical services. Critical services are those whose interruption would have a serious adverse effect on New Zealand as a whole or on a large proportion of the population, and which would require immediate reinstatement.

Analysis of overseas studies⁴ and the New Zealand situation shows that critical infrastructure may be defined as the assets and systems required for the maintenance of:

- governance including law and order and national and economic security;
- telecommunications and the Internet;
- energy including electricity generation and distribution and the distribution of oil and gas;

¹ Briefing to Minister of State Services, 9 December 1999

² E-Government – A Vision for New Zealanders, 2 May 2000

³ The term *hacker* originally referred to a clever programmer, and is still used to mean this by some. This report uses the more widely used sense of computer intruder.

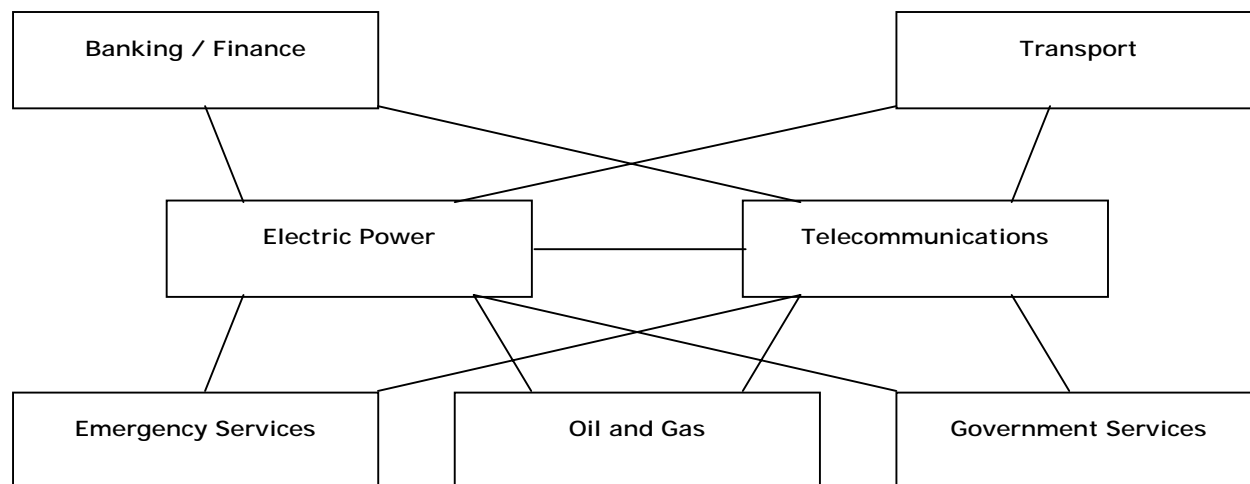
- finance and banking;
- transport including air, land and sea; and
- emergency services.

Some of the infrastructure required to deliver critical services is directly concerned with the transmission and manipulation of information (e.g. the telecommunications network). Other infrastructure areas make extensive use of networked information technology (IT) in their management and control systems. In principle, such areas of infrastructure are subject to IT-borne threats. Infrastructure operators are aware of this and, to varying degrees, have taken steps to mitigate the risk of infrastructure failure due to these threats.

⁴ E.g. President's Commission on Critical Infrastructure Protection – Critical Foundations: Thinking Differently, Oct 1997

NEW ZEALAND'S CRITICAL INFRASTRUCTURE

The following diagram shows how the various critical infrastructures depend on each other. Most systems assume the continuing supply of power and telecommunications.



Ownership of Infrastructure

The ownership of critical infrastructure is diverse.

- Central government departments own items such as the computers running the SWIFTT benefits payment system.
- The Defence and Police forces have computer systems and communications networks.
- Hospitals use computer systems for accounting and administration.
- The Reserve Bank currently operates banking settlements systems.
- State-owned enterprises such as Transpower and Airways own critical networks.
- Much critical infrastructure is in the private sector, including telecommunications and local electricity distribution.

The situation is more complex than the above would suggest. There are many different models for infrastructure-owning organisations to have parts of infrastructure outsourced or managed by another company. Furthermore, although some infrastructure providers have IT or telecommunications networks, these are in many cases dependent on circuits provided by a telecommunications carrier such as Telecom or Telstra Saturn.

While the government does not own or directly control much of the critical infrastructure of New Zealand, it does have a role in assuring itself that this infrastructure is adequately protected. Infrastructural businesses differ from others in that customers' interest in their continued ability to supply may exceed the commercial interests of the business to do so. This is especially a concern where the infrastructure business is a monopoly provider, since the competitive pressure to maintain service is reduced or absent. A hypothetical example

would be a power company that risked infrastructure failure through under-investment of funds and time in engineering while choosing instead to focus on an area that might increase profitability.

Risks in Critical Infrastructure

Given the concerns expressed above over the adequacy of commercial incentives in respect of infrastructure security, Government needs to consider how it can assure itself that sufficient risk management is being undertaken. A reasonable approach is to establish the extent to which infrastructure owners use risk management methods.

Best practice risk management starts with a formal model of risk and mitigation. There are a number of formal risk assessment models available. The following diagrams show a summary of risk assessment and mitigation as applied to the critical infrastructure. These models are adapted from Australian and New Zealand Standards.

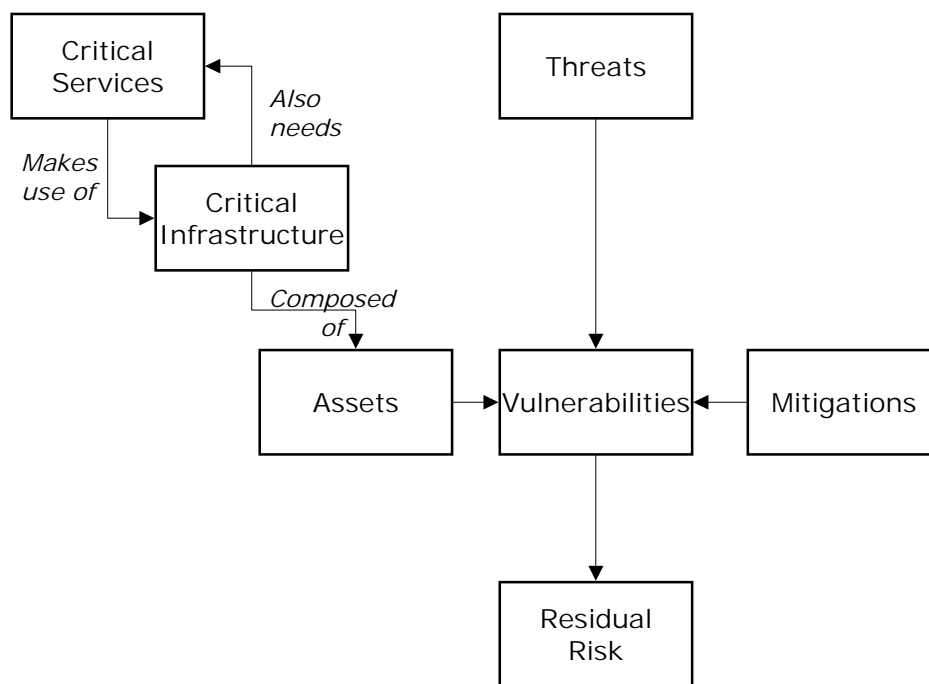


Figure 1 - Infrastructure Threats and Vulnerabilities

This diagram shows the critical services depending on infrastructure, some areas of which themselves depend on other services. The components of the infrastructure, referred to as assets, are subject to vulnerabilities. Vulnerabilities may be exploited by threats. The action of a threat on a vulnerability may be mitigated through various strategies.

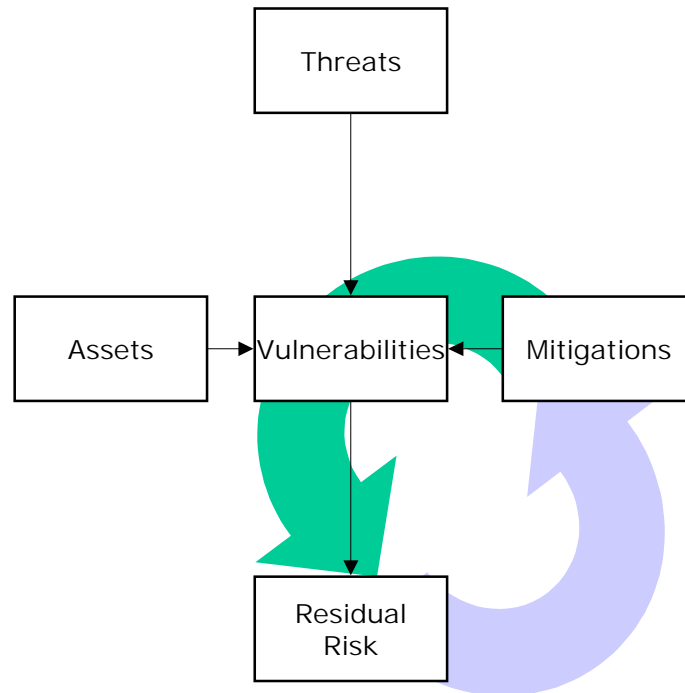


Figure 2 - Risk Mitigation Cycle

After risks have been mitigated there is always some residual risk, which needs to be assessed. If it is found unacceptable further mitigation measures will need to be applied.

Risk has two components: the consequence, or impact of an event; and the likelihood of the event. Because infrastructure is obviously valuable, physical risks have generally already been considered and some measure of protection applied. The risk of damage to infrastructure from physical threats therefore tends to have a low likelihood, albeit a high consequence. This report, however, focuses on the more rapidly developing and less immediately obvious risks that are associated with the growing dependence on IT.

IT Threats to Critical Infrastructure

IT threats (i.e. threats which do not include physical attack) to critical infrastructure may be categorised both by the motivation and resourcing of the attacker or other threat agent, and by the means of attack.

Threat agents could be:

- staff making mistakes;
- disaffected staff or contractors;
- recreational hackers;
- individuals seeking personal gain, e.g. through theft or extortion;
- agents of organised crime, competing commercial interests or issue groups; or
- agents of foreign governments.

These vary in the extent of knowledge and resource.

The types of IT-borne attack include:

- denial of service attacks via the Internet;
- hacking or cracking, whether leading to systems damage or breach of confidentiality;
- malware - programs with covert malicious intent, including viruses, worms, and trojan horses;
- malicious or inadvertent damage by insiders; and
- the unlawful interception of messages (or actual theft of laptop or other computers).

Since the Internet has become so ubiquitous in developed nations, most IT-borne attacks have been carried out over the Internet. Internet based attacks have certain characteristics which explain their prevalence and impact:

- Internet attacks involve action at a distance, in many cases crossing national borders, which offers the attacker a degree of anonymity and reduces the likelihood of punishment. This reduces the deterrent effect of legislation⁵.
- Like other IT-borne threats, Internet attacks often involve the use of computers for automatic repetition of some process, such as the use of dictionary searching tools to crack passwords, or viruses that replicate themselves without limit. This factor can leverage one individual's cleverness into an attack on infrastructure that has global impact. The size of the impact in this scenario bears no relation to the quantum of resources available to the attacker.
- Once written, automated attack tools⁶ become widely available on the Internet, and may be used by individuals who do not understand the tools or the consequences.

The Internet provides a wealth of opportunity for attacks on systems connected to it.

Vulnerability of Infrastructure to IT-Borne Attacks

Any area of infrastructure that uses IT-based control systems is vulnerable in principle. The greatest area of risk, in terms of the adverse consequence that could result, is any potential for unauthorised access to the IT systems used to manage infrastructure networks.

Where access is restricted to secure locations, the vulnerabilities are those of physical security and the risk that staff will do something malicious or mistaken.

Access through telecommunications (i.e. dial-up) to unstaffed network management facilities (e.g. electricity substations) is used by some infrastructure providers for efficient and prompt fault resolution. This introduces a new range of vulnerabilities, since there is a need for authentication of callers to the facility. The authentication system needs to be of strength

⁵ New Zealand is unusual among Western countries, in that it currently does not have legislation directed against hacking. A Bill to address this is before the House.

⁶ The authors of such tools are not necessarily malign or reckless, since they are in many cases intended for legitimate uses such as assessing one's own network for vulnerabilities.

commensurate with the risks posed by unauthorised access. The authentication system itself needs timely maintenance to ensure that, for example, resigning employees have their access revoked.

Interconnecting systems with the Internet provides benefits in terms of cost savings and functions that can be offered. Large infrastructure providers typically have their corporate business networks connected to the Internet, and have some kind of links between these and their network management systems. While awareness of Internet threats is high in many providers, it is hard to guarantee that unauthorized access to network management facilities is impossible.

Homogeneity of IT Systems

In information technology, New Zealand follows global trends in the choice of equipment and standards. Over the last decade the diversity of IT in wide use has decreased. This has happened because of:

- a desire for common open standards on the part of IT purchasers, partly as a measure to prevent vendor lock-in and monopoly pricing;
- the overwhelming success of the Internet, due in part to the quality and openness of the engineering on which it is built, effectively displacing other ways of connecting computer systems; and
- the exit of smaller computer manufacturers with unique equipment from the market (mainly for the reasons above) and the trend for specialised equipment to increasingly be based on off-the-shelf computers and operating systems.

These trends have led to a situation in which almost all computer networks use Internet protocols, almost all Internet routers are made by Cisco, most server computers use a version of Microsoft Windows or a flavour of Unix, desktop computers almost all use a version of Microsoft Windows, and where specialist machines such as are those in the power grid are increasingly controlled through widely understood machines of the types above. This is not meant to imply that these products are inherently less secure than alternatives. However, while homogeneity of systems leads to benefits in terms of efficiency and ease of use, it also makes all computers more vulnerable to attack. This is because having a large number of users increases the chance that lurking security problems are discovered and exploited, and because of the number of machines that can be compromised when problems do come to light.

The process of convergence to common IT standards may not be complete. Telephony, which is already dependent on digital technology, may move to use Internet protocols and Internet-style routers instead of the specialist switches and PABXs currently used. The Ministry of Social Policy has recently installed just such a system across all Department of Work and Income branches. This does not imply such a move is inherently risky, indeed it should pay dividends in terms of efficiencies and greater effectiveness. However, it is part of the general convergence of many kinds of technology to a few types whose details are very widely known.

Complexity

Continued technological development involves increasing complexity. Although the diversity of building blocks of IT systems is decreasing, the complexity of the blocks

themselves is increasing very quickly. Each generation of computer chips has several times more transistors than its predecessor, and each new version of Microsoft Windows adds millions of lines of program code. More and more of these elements are interconnected in novel ways to offer greater levels of automation and control.

In this environment it is hard or impossible to test every possible combination of circumstances and user input. Commercial pressures tempt developers to ship products with known problems (some of which are security related), leaving solutions to the problems for product updates. Consequently problems, including security problems, are often found with widely used systems.

Availability of IT Security Staff

Securing computer systems and maintaining their security requires considerable expertise. Retaining staff with this expertise is difficult. Because of the premium these people can attract, they are often contractors or consultants. Anecdotal evidence suggests that IT skills in general, and IT security skills in particular are becoming scarce in New Zealand. There is a similar view in Australia. In an attempt to address this shortfall the Commonwealth Government is considering promoting specific centres of excellence in some universities.

With IT security skills in demand in the US and Europe they will always command a premium in New Zealand and Australia. The challenge for infrastructure owners is to manage risk in this environment. Government can help through initiatives to pool knowledge and expertise.

Legal Issues

Criminal Law

Globally, there are two main areas of criminal law which relate to hacking or other IT-borne attacks: so-called *cybercrime*, where electronic means are used to commit a non-IT crime such as theft; and the making of unauthorised computer access itself a crime.

There are international moves to agree definitions of cybercrime and to facilitate pursuit of offenders across international boundaries. The EU is attempting to negotiate such a treaty among its members. If it succeeds, other jurisdictions may well try to harmonise legislation. The New Zealand Police has also been considering cybercrime through its membership of the Australasian Centre for Policing Research.

Most developed nations have now enacted legislation making unauthorised access to computer systems a crime. New Zealand has yet to do this, although a Bill is before the House (the lack of such a statute may harm New Zealand's international reputation if not rectified soon). Enacting this legislation will make it easier to pursue New Zealand residents who break into computers, and also will make it more likely that requests by New Zealand law enforcement agencies for assistance to track computer vandals in other jurisdictions will meet with favour.

As currently framed⁷, the Bill before the House does not address denial of service attacks. This type of attack, discussed elsewhere in this paper, is an increasing problem on the Internet in New Zealand and overseas. There is a risk that New Zealand's legislation will remain out of step with other countries and with the real world if no attempt is made to make

⁷ Crimes Amendment Bill No. 6 as amended by Supplementary Order Paper No. 85

denial of service attacks a crime. Ministry of Justice officials are aware of this issue and are considering further amendments to the Bill to take it into account.

Disclosure

Gathering reliable numbers about incidents of this nature is hard since companies are understandably reticent about making disclosures that might harm customer confidence or shareholder value. There is sometimes a public perception that the public sector is more susceptible to IT related attacks than the private sector, but this may be due to the greater requirements for information disclosure in the public sector.

Without reliable figures planning protective strategies is difficult. A solution to this might be some trusted group that maintained an incident database in a suitably anonymised form.

Liability

Companies that own infrastructure would be unlikely to be liable in a legal sense if their infrastructure failed, unless it could be shown that they had failed to operate in accordance with widely accepted relevant standards.

An exception is the banking industry. As a condition of a banking licence, the directors of a bank are required to attest to prudent operation of their bank. This may make them personally liable in the event of failure.

THE CURRENT STATE OF INFRASTRUCTURE PROTECTION IN NEW ZEALAND

Finance and Banking

The New Zealand finance and banking sector contains retail banks, other financial institutions and purely infrastructural organisations. Retail banks are licensed by the Reserve Bank of New Zealand, which imposes various conditions on their operation. Each bank runs its own retail account processing system. Most maintain accounts with the Reserve Bank from which they pay each other during the course of each day. Interchange and Settlements Limited (ISL) operates payment “switches” which route transactions from one bank to another. Similarly a company called ETSL operates the main EFTPOS switch.

The players in the New Zealand wholesale financial markets, who include offshore banks and investment funds managers as well as the New Zealand retail banks, use a system called Austraclear to exchange New Zealand dollar debt securities and wholesale cash transactions. Austraclear is currently operated by the Reserve Bank. Billions of dollars flow through it daily.

Banks have always been highly conscious of the need for security. All banks and interchange facilities spoken to were confident about the security of their core systems and Internet sites.

The main area of concern identified is the desire of some New Zealand banks to move their retail processing offshore. At least one has already done this and others are reportedly considering the move. The Reserve Bank of New Zealand is planning to move the computers for its real time gross settlement system to Australia. This system manages the relative position of all New Zealand banks and is core to the banking system. The Reserve Bank also plans to move its Austraclear computer systems to Sydney.

There are two main risks in the movement of banking systems offshore. Firstly, adverse events in Australia, such as industrial action, would be outside any New Zealand control yet could have a highly adverse impact here. This is not to argue that the labour markets or other factors in the two countries render disruption more likely with systems being offshore. Rather, the New Zealand Government would be less able to manage an extreme situation involving critical New Zealand infrastructure if this is located offshore than it would otherwise be.

Secondly, trans-Tasman telecommunications circuits, or their local (Australian) links to the computer systems, might fail leaving New Zealand disconnected from its banking system. Even with the much improved robustness and diversity of trans-Tasman links this represents a greater risk than running systems onshore, since there will always be greater capacity and robustness between, say, Wellington and Auckland than between Wellington and Sydney. A similar argument to the one above applies in respect of the domestic Australian links necessary to connect the computers to the trans-Tasman cables.

The Reserve Bank leases its trans-Tasman circuits from diversified carriers, and has back-up arrangements for satellite links should the cable be seriously disrupted. Additionally, the Bank has formal business continuity plans for loss of communications and these are tested six-monthly. The BCPs are based on reverting to alternative modes of operation, with a bottom line being continuity of service to customers in the event of communications failures.

The RBNZ is moving to interdependency with international banking, a move that the rest of the New Zealand banking sector also appears to be adopting. Notwithstanding the

apparently solid business continuity planning processes established and tested by the banking and finance sector, the move offshore does increase the reliance on extended telecommunications paths and perhaps raises issues of sovereignty. Stringent risk assessment processes need to be implemented to ensure that the telecommunications and sovereignty risks do not outweigh any operational gains.

Transport

The only significant section of national transport infrastructure potentially vulnerable to information-related threats is the air traffic control system. This is operated by the Airways Corporation, which is a state-owned enterprise. The major vulnerability is loss of telecommunications which are, in the main, provided via leased bearers. However, most communications links can use multiple routes. Further back-up using satellite capacity is under consideration. Airways Corporation also has a strong service level agreement with its telecommunications provider.

Airways' main operations centre is located in Christchurch. Also in Christchurch, but in a separate building are Airways' research and development facility, software development facility and a simulator system which can assume most of the functions of the main operations centre. Airways' control room at Ohakea provides contingency back-up for Christchurch although extra staffing at Ohakea would be required. (This might be an issue if staff could not be relocated from Christchurch, e.g. after a major earthquake there.) All Airways' computer systems are locally maintained so there is no remote access to any of its systems. All IT staff undergo security checks. The Internet is not used operationally other than for e-mail with some secondary sites.

Two strengths of Airways' systems are business continuity planning and audit. All operational equipment has at least one back-up system, and rigorous BCPs have been developed. Strong security audit regimes are in place: the Civil Aviation Authority undertakes an annual audit of centres and regions; internal audits are undertaken annually by each Airways business unit; and ISO 9001 certification audits are undertaken by Quality Assured Services. Airways has also put considerable urgency into development of full risk analysis processes and risk analysis is part of the internal audit process.

There is good recognition of infrastructure vulnerabilities in the New Zealand aviation industry, and no major area of concern has been identified.

Electric Power

The electric power industry in New Zealand comprises a number of generators, the national power grid operated by Transpower, local infrastructure ("lines companies") and the various power retailers.

The generators mostly have a number of power stations of different types. While it is quite possible to imagine that these have vulnerabilities, no one generator, or particularly no one power station, is crucial to ensuring continuity of supply. If any one generation company were to fail totally, under most circumstances New Zealand would have enough power. The issue of protection therefore becomes one of commercial prudence for each company, and need not be examined further here.

The retailers, while they market and account for power, do not own the infrastructure – the local lines – which is used to deliver it. Damage to their computer systems and records would

harm only their own businesses and they have every commercial incentive to ensure that this does not happen.

Failure of the core networks of Transpower or the lines companies would cause loss of supply. This is not to imply that they are in any way suspect; rather that Government has a greater interest in their continued delivery.

The Transpower network comprises various switching points and substations interconnected by transmission lines, including the inter-island link. This network is managed through remotely controlled equipment placed throughout the network.

Transpower has two fully staffed operational Centres providing full operational backup and one, normally unstaffed, management support Centre that can provide additional resources in the event of widespread disaster. Operation of the national grid does not depend heavily on external telecommunications since Transpower owns 60-70% of its telecommunications links. In an extreme situation, if the network were unable to be managed actively, it would continue to deliver power unless there were a major change in demand or supply.

Transpower takes its responsibilities in respect of continuity of supply extremely seriously. However, with the increasing reliance on information technology to manage the power distribution network there may be a need for greater central focus on the IT security aspects of network design. In recognition of this issue Transpower has recently established an executive level committee to drive security in all parts of its network, and is drawing on work done in the US to consider information-related threats and vulnerabilities to its operations.

The project team has been unable to gather any information about the protection of electricity lines companies' infrastructure assets. Given that there are several such companies, each with an effective monopoly in their respective areas, there would appear to be scope for industry co-operation to provide mutual assurance of infrastructure security.

Telecommunications and the Internet

New Zealand has a number of companies offering telecommunications and Internet services. The major telecommunications companies ("telcos") operating in New Zealand offer robust domestic voice and data networks.

New Zealand's international telecommunications pass through one of three submarine cables, or go via satellite. Submarine cables are vulnerable to damage by anchors and fishing gear and to sabotage. The cables were laid some years apart. Each successive cable has many times the capacity of its predecessor. Failure of the highest capacity cable would thus have a severely detrimental effect on New Zealand's connectivity with the rest of the world.

The newest cable, Southern Cross, takes the form of a ring connecting New Zealand, Australia and North America. If part of the ring is severed, traffic will be routed through the remaining segments to ensure that connectivity is not lost. To reduce the risk of damage, in water depths of less than 1,500 metres Southern Cross cables are buried beneath the sea-bed. Southern Cross is designed to have a much higher reliability than older cables. The likelihood of total failure of Southern Cross must be seen as very low. As Southern Cross becomes fully commissioned through 2001 the risk of a major loss of offshore telecommunications will decrease significantly.

The movement of banking systems to Australia (discussed elsewhere) greatly increases the impact of any failure of international telecommunications. This threat has to be seen as one of low likelihood (that sufficient cables are damaged to disconnect the banking system) but high impact – failing to process bank transactions would have a severe effect on many individuals and the economy as a whole.

Inter-island telecommunications currently pass through two Cook Strait cables owned by Transpower. They are periodically subject to damage by fishing vessels. Despite legislation to protect the cables, no one has ever been prosecuted for this damage. Furthermore both cables are laid reasonably close to each other across the sea bed and use the same landing points. To mitigate the risk of cable failure, Transpower has made arrangements for priority access to a specialist cable repair vessel. However there would still be a delay of days or weeks after breakage before repair could be completed. There is a backup arrangement for inter-island communications using a microwave link, but this does not have adequate capacity to provide normal service if both cables were unavailable.

Resource consent is currently being sought for two separate high capacity inter-island cables to be buried along different routes in the sea bed. It is hoped that they will be commissioned in 2001. Once implemented, these will greatly improve the security of inter-island communications.

The Internet

The Internet is increasingly both an important business tool and an infrastructure for commerce. It is central to the whole notion of e-government.

The Internet's importance impels businesses to connect their systems to it. There are, however, significant security risks in interconnecting business systems and the Internet.

It is the nature of the Internet to be open to all, highly decentralised, and to allow (or even encourage) very rapid technical innovation. These attributes, while they have facilitated the explosive growth of the Internet, also lead to significant threats to machines connected to it. The vulnerabilities described below do not just apply to Internet business, but to all businesses with an Internet connection.

Security weaknesses are frequently discovered in hardware and software in common use. These vulnerabilities are often published on the Internet, together with “exploits” – detailed instructions (or actual code) that uses the vulnerability to demonstrate a security breach. Updates to resolve security issues (called patches) are generally, but not always, made available by software vendors soon after the publication of vulnerabilities. As soon as a vulnerability for a specific piece of software is published, computers using that software and attached to the Internet have to be regarded as insecure until the software has been patched.

The existence of software with known vulnerabilities running on machines connected to the Internet is exploited by individuals (“hackers”) who for whatever reason like to compromise computer security. Sometimes hackers just look at systems they have penetrated, other times they cause damage by changing or deleting files. Hacking into web servers to deface web sites is quite common, and has been done to many organisations including the CIA. Web site defacements are currently running at about 20 per day across the whole Internet⁸, with an increasing trend. Having a high public profile, particularly one concerned with security,

⁸ <http://attrition.org/mirror/attrition/stats.html>

increases the attempts made to deface a site. All organisations with web sites need to remain vigilant about the security of their machines and monitor them for any evidence of break-ins.

Viruses and similar programs attempt to spread copies of themselves widely. Some also cause deliberate damage, or more sinisterly seek specific information, which they then transmit to a remote Internet address. Most modern viruses use Internet email to spread themselves, and many use the specific automation features of Microsoft desktop products. The use of virus scanners is essential, as is keeping them up to date. The rapid spread of novel viruses (such as the “love bug”) can be controlled if systems administrators are notified immediately and take urgent action.

Another type of attack is the denial of service attack (DoS). This exploits features of the Internet protocols to overwhelm a target computer with a flood of requests it cannot meet, resulting in a reduction or loss of service from the target machine. This technique is often used against web servers. An extension of this technique is the distributed denial of service (DDoS) which uses the resources of a large number of machines which have been effectively commandeered, to attack a single target. Such attacks are difficult to defend against and almost impossible to trace back to their originator.

These attacks are becoming common against New Zealand targets. As well as effectively forcing their target off the Internet, DOS attacks result in degraded or denied service to other customers of the same Internet Service Provider as the target and may cause wider degradation of service on the New Zealand Internet. The addition of new offshore bandwidth in the form of the Southern Cross cable may exacerbate this problem since it permits attacks of much greater intensity.

Oil and Gas

There are a number of different companies involved in oil distribution in New Zealand. The main retailers are very competitive and are fully aware that any failure on their part would result in loss of market share as consumers switched to alternative suppliers. The Marsden Point oil refinery is shared by several oil companies, but this only provides a proportion of New Zealand’s petroleum products (since some are imported). Failure of the refinery for whatever reason would be subject to normal contingency plans for this event. The coastal tanker fleet is also shared, but is not thought to be vulnerable to IT based attack.

Gas is widely used for domestic heating and also supplies at least one power generation station. However it is questionable whether it can be regarded as critical. The commercial incentives on the companies providing gas services are regarded as sufficient to ensure that they protect their infrastructure adequately.

Emergency and Government Services

Defence

The New Zealand Defence Force makes extensive use of telecommunications, both national and international. For example, NZDF establishments throughout the country are interconnected over leased telecommunications bearers. Communications with deployed forces overseas, and communications with allied nations also generally use leased bearers. Considerable use is also made of the Internet for unclassified communications. But the NZDF also has its own integral communications capabilities with the capacity to provide ‘thin red line’ communications in the event of disruption of the national or international carriers and

has the tested capability to provide emergency communications for government in the event of civil or other disaster.

The NZDF has completed a risk assessment of its communications infrastructure and has established contingency plans. While these plans have not been specifically tested, the reality is that every exercise, operation or deployment routinely exercises the plans under normal operational circumstances.

In general terms, the NZDF is a self-contained force with the ability to continue operations, or to contribute to the national good, in the event of degradation of the infrastructure. As evidenced by the strategies of our partner nations, the NZDF needs to be closely involved in critical infrastructure protection planning.

Police

The New Zealand Police enterprise communications network has switch centres in Auckland, Wellington and Christchurch with sufficient redundancy to ensure that operations will be unaffected by the loss of any one centre. The backbone network uses shared sites although some sites are Police owned. The Police telephone system is outsourced.

A comprehensive risk analysis and BCP were completed as part of the Y2K programme. The BCP has now been rolled over into a corporate BCP and a formal risk assessment framework has been established. From the New Zealand Police perspective, the most critical infrastructure element is probably power.

Emergency (111) service is operated by a contractor to Telecom, which passes calls to police, fire or ambulance as appropriate. Police and fire share the emergency communications network, but ambulance services are disparate organisations so are not integrated. A key police development strategy is the implementation of a common network for all emergency services.

Like the NZDF, the NZ Police Force is self-contained with the ability to continue operations, or to contribute to the national good, in the event of degradation of the infrastructure. Police also needs to be closely involved in critical infrastructure planning.

Fire

The New Zealand Fire Service uses communications facilities which it shares with the New Zealand Police, and which are discussed under that heading. There are no significant concerns in this respect.

Revenue and Income Support

Inland Revenue Department and Department of Work and Income handle high volumes of time-critical financial transactions for Government. Disruption to these departments' core infrastructure might have adverse effects for many New Zealanders.

IRD has invested considerable effort to ensure that its services remain available. It has a strong security focus, and is aware of the vulnerabilities associated with Internet connection as it moves toward a greater use of e-business. Some IRD computer facilities are managed by external companies, but IRD maintains a detailed level of control over the use of the computers. Like most other large businesses, IRD requires telecommunications for its day to

day business, and has gone to lengths with its telecommunications supplier to ensure an adequate service level. IRD maintains and tests comprehensive business continuity plans.

To pay benefits and pensions the DWI relies on its computers, which are facilities managed by EDS. Critical systems are operated from the Upper Hutt data centre; there are backup computers in an Auckland data centre. DWI also depends on the data and telephony network provided by the Ministry of Social Policy, using Clear as a carrier. A high standard of IT security is provided for DWI by MoSP, but staff security and physical security are handled by a security function within DWI. There may be value bringing the responsibility for these functions together.

Water

Water is supplied by local authorities and is not part of a national infrastructure as such. The Parliamentary Commissioner for the Environment has recently released a report⁹ examining issues and risks around water supply. This notes a number of major challenges including a risk of infrastructure failure. However, this is not an information related risk and will not be investigated further for this project.

⁹ Ageing Pipes and Murky Waters

INFRASTRUCTURE PROTECTION PROGRAMMES IN OTHER COUNTRIES

Summary of other National Programmes

The elements of the critical infrastructure identified in this report are consistent with those identified in other national programmes researched. By their very nature cyber threats transcend national borders. Infrastructure elements operate beyond national borders, and so infrastructure protection must be considered on an international scale. It is important that New Zealand be aware of, and as far as reasonable participate in, the critical infrastructure protection initiatives of other Western nations.

United States of America

In July 1996 the President established the President's Commission on Critical Infrastructure Protection (PCCIP)¹⁰ to review and recommend a national policy for protecting critical infrastructures. The PCCIP Report¹¹ eventually led to the promulgation in January 2000 of the "National Plan for Information Systems Protection".

There is considerable infrastructure protection activity underway in the United States, both at the federal and state levels. There is significant effort undertaken at federal level to complete vulnerability assessments of critical infrastructure elements with these assessments including 'red teaming' or penetration testing. At state level Hawaii is particularly active and recently hosted a three day seminar on the protection of the electric power infrastructure.

Arguably the most effective protective measure implemented by the US has been the establishment of the National Infrastructure Protection Center (NIPC). The NIPC, which is hosted by the FBI, has widely representative staffing from other national agencies. It serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. It provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The main mission of the NIPC is to detect, deter, assess, warn, respond, and investigate unlawful acts involving computer and information technologies and unlawful acts, both physical and cyber, that threaten or target US critical infrastructures.

United Kingdom

Extensive activity on Information Age Government (IAG) is ongoing in the United Kingdom. Protection of the UK Critical Information Infrastructure (CII) is within the portfolio of the Home Secretary. An advisory committee, the IAG Champions, has drafted a policy for the protection of critical infrastructure and this is currently with the Home Secretary for consideration. BS7799 (equivalent to AS/NZS 4444)¹² is being advocated as the standard for CII owners, and it is understood that the Cabinet Secretary has invited all departments to advise by 31 December 2000 their plans for adopting/satisfying this standard.

Robustness of service is a focal requirement of IAG, and the challenge is to accurately and quickly identify threats. Public attitudes to system failure will be unforgiving as was demonstrated by the recent passport problems where the inability of the systems to cope with requirements resulted in significant inconvenience (and cost) to many individuals. The 'Love

¹⁰ Executive Order 13010, 15 July 1996, Critical Infrastructure Protection

¹¹ Critical Foundations, Protecting America's Infrastructures, October 1997

¹² Information Security Management in two Parts: Part 1 is the code of practice for information security management, Part 2 is the specification for information security management systems.

Bug' demonstrated the fallibility of non-robust systems, and UK virus companies have now been tapped to provide immediate advice when they detect any security incidents.

The UK equivalent of New Zealand's Secure Electronic Environment (SEE) network extends throughout government, with most intra-government business now conducted over the network. Any potential for non-availability of this network is a real issue for government – it will become more so as IAG becomes a reality. There may be lessons here for the SEE project.

A close relationship has been developed with the private sector – both business and academic. For example, the Information Assurance Advisory Council established at Kings College London has a diverse membership and is an effective forum. Engagement of infrastructure owners is central to the CII programme with the approach being one of persuasion rather than regulation. The UK government views the establishment of Computer Emergency Response Teams (CERTs) as central to CII and would encourage the development of a CERT for each community of interest within the CII.

Australia

The Commonwealth government has recognised the need for infrastructure protection for several years. An inter-departmental committee was formed and led by the Attorney-General's Department. In December 1998 this produced a report recommending an ongoing effort to protect the National Information Infrastructure.

The committee recommended, among other things, that: a formal structure be established to coordinate infrastructure protection; AusCERT (Australian computer emergency response team) be funded; and that accreditation for IT security training be set up. In the 2000/01 commonwealth budget round information infrastructure received \$2m. This figure was intended for coordination and central funds; actual protection activities are to be undertaken by the agencies and companies owning the infrastructure.

The interdepartmental committee has continued and has been raising awareness among infrastructure owners, partly through a consultative industry forum involving the private sector. Recently the Attorney-General's department has recommended to the commonwealth government that general IT security promotion (i.e. non-critical infrastructure protection) be passed to the National Office for the Information Economy, an agency concerned with e-commerce and e-government.

Canada

A Critical Infrastructure Protection Task Force (CIPTF) was established in 1 April 2000 within the Department of National Defence, but reporting operationally to the Privy Council Office. Its mandate is to review critical infrastructures in Canada and develop a framework for future action in terms of protecting them. The CIPTF expects to present its report to Cabinet in early-2001.

A five-part strategy is being proposed based around strong interaction both with the private sector and with other international critical infrastructure programmes. It is likely that a new organisation for CIP will be established to lead and coordinate the national response. As an interim measure a pilot Government of Canada Information Protection Coordination Centre (GIPCC) has been set up to provide better coordination and management of cyber incidents affecting government departments and agencies. Pending establishment of the new organisation, the GIPCC has been temporarily located with the RCMP.

RECOMMENDED STRATEGY

The protection of critical national infrastructure from information related threats is an issue which merits taking notice, and is being taken seriously by other western nations. While owners of critical infrastructure in New Zealand are conscious of the need to protect it, this report has raised some concerns over specific issues. The recommendations below are aimed at providing infrastructure owners with the tools and information they need to protect against information related threats, and to promote cooperation toward a common view of infrastructure protection.

Recommendations

- a The E-government Unit should investigate the establishment of a New Zealand-based security monitoring and incident handling organization with the following functions:
- provide timely information to critical infrastructure owners and government departments about threats, actual attacks and recovery techniques
 - build local capability in incident handling and security research
 - monitor global security issues and gather IT security intelligence
 - build relationships with similar organisations, e.g. CERT.
 - promote cooperation among clients in respect of IT security
 - maintain statistics and incident databases
 - promote standards and tools for IT security and risk management
 - communicate to raise provider and public awareness of computer security issues
 - maintain a model security service level agreement for use in outsourcing arrangements
 - encourage production and adoption of relevant standards
 - facilitate independent security/protection audit capability,

Rationale: By providing a New Zealand based centre of expertise the IT security skills and awareness of infrastructure providers and government departments can be bolstered.

- b Government should consider harmonising computer crime legislation with that of other Western nations and participating in international cybercrime treaties. Furthermore, the Bill on this matter currently before the House should be extended to address denial of service attacks.

Rationale: There is currently little deterrent against casual attack on infrastructure. Improving our computer law will help. Furthermore, other jurisdictions are more likely to help with trans-border crime if New Zealand's legislation parallels their own.

- c The New Zealand Police should consider what is necessary to investigate computer break-ins and related attacks and prosecute perpetrators. This would involve:
- building investigative capability, while maintaining respect for privacy of Internet users; and
 - building relationships with law enforcement authorities responsible for pursuing malefactors across national borders and co-operating with other countries who wish to pursue here.

Rationale: There is currently little deterrent against casual attack on infrastructure. Improving our computer law will help. Furthermore, other jurisdictions are more likely to help with trans-border crime if New Zealand's legislation parallels their own.

- d Establish an ongoing cooperation programme between owners of critical infrastructure and Government.
- Invite Responsible Ministers to write to critical infrastructure owners asking them to declare their support or otherwise of relevant security standards.
 - Engage critical infrastructure providers at a senior level on the subject of IT threats to ensure that all infrastructure owners undertake and maintain formal risk analysis and management of information-related and physical threats.
 - Direct the State Services Commission to review the state of critical infrastructure protection after 12 months.

Rationale: This will seek and maintain the commitment of infrastructure-owning organizations to an adequate level of protection, and will show the government's commitment, on behalf of New Zealanders to the issue.

- e Invite Transpower to lead a power industry infrastructure protection group, possibly as part of the group in recommendation d, to provide knowledge and cooperation in respect of infrastructure protection among power industry players, particularly lines companies.

Rationale: This is a highly competitive and technically complex industry with many players, some of whom have effective monopolies over power distribution in large areas. There is little or no evidence of cooperation in security or infrastructure protection matters. Transpower is uniquely positioned to assist the industry.

- f Through the State Services Commission, direct government agencies to adopt specified appropriate IT security standards.

Rationale: As part of the movement toward e-government, the Government needs assurance that its own agencies are taking prudent steps to manage their own IT security. Though many of the large and critical agencies have already adopted relevant IT security standards, there are others who may lack understanding of the issues or technology.

GLOSSARY

Austraclear – an electronic system used to transfer cash and securities between financial market participants.

Automated Attack Tools – software which may be used to attack a remote computer over the Internet.

Bandwidth – the capacity of a telecommunications link in terms of the amount of data that can be passed through it per second.

CERT – an organisation which monitors IT security problems and assists with recovery from attacks. Originally Abbreviation for Computer Emergency Response Team. The original CERT is based in Carnegie Mellon University in the US, there are now a number world wide.

Cracking – see hacking.

Critical Infrastructure – Infrastructure necessary to provide critical services.

Critical Services – Those whose interruption would have a serious adverse effect on New Zealand as a whole, or on a large proportion of the population, and which would require immediate reinstatement.

Cybercrime – general term which can mean crime specific to computers or more mainstream crime in which computers have been used.

Data Centre – a building whose purpose is to house large computers. Typically these have strong physical security and backup power supplies.

Denial of Service (DoS) – a mode of attack across the Internet in which a target computer is overwhelmed by a large volume of requests it cannot meet, leading to it becoming effectively unavailable.

Distributed Denial of Service (DDoS) – like denial of service, but with much greater attack volume gained through the use of a number of commandeered computers.

Exploit – a penetration of security through a vulnerability in hardware or software.

Firewall – a special purpose computer intended to control access between the Internet and a private computer network.

Hacking – exploiting weaknesses in other people's computers to gain unauthorised access to them. (The definition of this term is open to debate. Some people use it mean clever programming with no connotation of breaking security and argue that the sense used here is an invention of the media.)

Hardware – physical parts of a computer or communications system, as distinct from software.

Information Age Government (IAG) - The United Kingdom equivalent of e-govt.

Internet – a global computer network which carries e-mail and the world wide web, among other things.

Internet Protocol (IP) – the precise way in which messages are passed through the Internet. All computers connected to the Internet use IP to communicate with each other.

Internet Service Provider (ISP) – a company that connects businesses and/or individuals to the Internet.

Mainframe – a very large computer, typically installed in a data centre (q.v.), used for high-volume high-security applications such as banking.

Malware – software with malign intent such as viruses, worms and Trojans.

National Information Infrastructure – Those parts of the infrastructure that provide transmission or manipulation of data, or make extensive use of networked IT in their management and control systems.

NT – see Windows.

Operating System – a program which control access to a computer and shares its resources among all the other programs it runs. Operating systems are large, complex programs with the potential for many security vulnerabilities. Examples are Microsoft Windows and Unix.

PABX – central component of a corporate telephone system which connects the extensions together and to the outside lines. Abbreviation for Private Automatic Branch Exchange.

Patch – a small change to software already distributed, usually to fix a problem in it. Applying patches as they become available is important to maintain security of computer systems.

Router – a piece of hardware that stands at a junction in a computer network and directs messages.

SCADA – a type of specialised hardware and software used to manage remote parts of power and other networks, particularly water, oil and gas. Abbreviation for Supervisory Control and Data Acquisition.

Secure Electronic Environment (SEE) – an e-govt project providing for the secure interchange of data between departments.

Server – a powerful computer which provides services such as document filing and printing to other computers. See also Web Server.

Social Engineering – posing as an insider or technician on the telephone to gather passwords or other sensitive information.

Submarine Cable – a telecommunications cable laid across or below the sea bed between continents or along coastlines.

Trojan – a malign computer program disguised as something entertaining or interesting. Example: an emailed program that tells jokes and also steals passwords.

Unix – a type of operating system (q.v.) often used for powerful computers and servers. There are many different varieties (or flavours) of Unix, including Linux, Solaris and AIX.

Virus – like their biological namesakes, computer viruses make copies of themselves onto as many computers as possible. Viruses sometimes have a specific malign intent, such as deleting files or sending information off site. Even if they do not, they use up computer and communications resources and a great deal of time of those staff whose job it is to get rid of them.

Vulnerability – a security weakness that might be exploited and would lead to adverse consequences.

Web Server – a server computer that operates one or more web sites. Web servers usually use one of two or three popular web serving programs and Unix or NT.

Windows – a family of operating systems from Microsoft. Versions include Windows 95, 98 and ME (Millennium Edition) which are aimed primarily at home machines, and Windows NT and 2000 which are aimed at corporate machines. Almost all desktop computers and many servers use one version or another of Windows.

Worm – see virus.

APPENDIX I - BIBLIOGRAPHY

- 15 July 1996 Presidential Executive Order 13010, Critical Infrastructure Protection
<http://www.ciao.gov/PCCIP/eo13010.pdf>
- October 1997 Critical Foundations: Thinking Differently, The President's Commission on Critical Infrastructure Protection
http://www.ciao.gov/CIAO_Document_Library/PCCIP_Report.pdf
- December 1998 Protecting Australia's National Information Infrastructure, Report of Interdepartmental Committee on Protection of the National Information Infrastructure, Attorney-General's Department, Canberra
<http://law.gov.au/publications/niireport/niirpt.pdf>
- 26 August 1999 Announcement by Attorney-General, Protecting Australia's Information Infrastructure
http://www.ag.gov.au/aghome/agnews/1999newsag/601_99.htm
- October 1999 Canadian IO Bulletin, Vol 2, No 4: Some Thoughts on Critical Information Infrastructure Protection, Holly Porteous, EWA-Canada
<http://www.ewa-canada.com/IOV2N4.htm>
- 9 May 2000 Announcement by Attorney-General, Budget Increases Safeguards to National Information Infrastructure
<http://www.ag.gov.au/aghome/agnews/2000newsag/2000newsag.htm>
- 7 January 2000 Defending America's Cyberspace, National Plan for Information Systems Protection V1.0, The White House
http://www.ciao.gov/National_Plan/national_plan%20_final.pdf
- June 2000 Ageing Pipes and Murky Waters, Urban water system issues for the 21st Century, Office of the Parliamentary Commissioner for the Environment,
<http://www.pce.govt.nz/Reports/Ageing%20Pipes%20and%20Murky%20Waters.pdf>
- 18 August 2000 The Cyber-Posture of the National Information Infrastructure, Willis H Ware, RAND
<http://www.rand.org/publications/MR/MR976/mr976.html>
- October 2000 The Virtual Horizon: Meeting the Law Enforcement Challenges, Police Commissioners' Conference Electronic Crime Working Party, Australasian Centre for Policing Studies, Report Series No 134.1

Web Sites Researched

www.attrition.org	Records website defacements and other attacks
www.ag.gov.au	Attorney-General, Australia
www.ciao.gov	Critical Infrastructure Assurance Office
www.citu.gov.uk	Central IT Unit, Cabinet Office, UK
www.ewa-canada.com	Electronic Warfare Associates-Canada Ltd
www.globalcomms.co.uk	Global Communications, London
www.iagchampions.gov.uk	Information Age Government Champions
www.nipc.gov	National Infrastructure Protection Center
www.nist.gov	National Institute of Standards and Technology
www.pce.govt.nz	Parliamentary Commissioner for the Environment
www.pcis-forum.org	Partnership for Critical Infrastructure Security
www.rand.org	RAND
www.sans.org	System Administration, Networking, and Security Institute
www.witsa.org	World Information Technology and Services Alliance

APPENDIX II – CONTRIBUTORS AND CONSULTATIONS

Project Team

Colin Jackson (Project Manager)
Mike Spring

Experts Group

This was a group of technical experts selected for their expertise and knowledge.

Tone Borren (Chair)
Andrew Mason
Mike Pearson
Eric Evans
Michael Newbery
Frank March
Bernard O'Brien
Jay Garden

Consulted

Airways Corporation
ASB Bank
Cisco
Civil Aviation Authority
Clear Communications
Debt Management Office
Department of the Prime Minister and Cabinet
Department of Work and Income
Enternet
Government Communications Security Bureau
Information Technology Association of New Zealand
Inland Revenue Department
Interchange Settlement Ltd
Internet Society of New Zealand
Ministry of Fisheries
Ministry of Economic Development
New Zealand Defence Force
New Zealand Fire Service
New Zealand Police
New Zealand Security Intelligence Service
Reserve Bank of New Zealand
Telecom New Zealand
Telstra Saturn
Transpower
Vodafone
WestpacTrust
Xtra

In addition contacts were made with various government bodies in Australia, Canada, the United Kingdom, and the United States.