CRITICAL INFRASTRUCTURE ATTACK
An Investigation of the Vulnerability of an OECD Country[1]

Dr Adam Cobb
Australian Parliamentary Fellow, Information and Research Services, Department of the Australian Parliamentary Library, Canberra, Australia

ABSTRACT

This paper takes Australia as a case study and asks specifically where, how, and why Australia's critical infrastructure might be at risk. By examining the core elements of the National Information Infrastructure (NII), such as power distributions systems, telecommunications and financial networks, it is possible to gauge whether the system is vulnerable. The evident vulnerabilities are then juxtaposed against a selection of threats, thereby creating a risk assessment. The paper will end with suggestions as to future policy options available to the Australian Government. It should be noted however that this paper does not claim to provide an exhaustive survey of either vulnerabilities or threats. The criteria for selection were focused on the most serious threats and vulnerabilities that were evident in the open source literature at the time.

INTRODUCTION

There are risks as well as benefits associated with information technology. For example, the use of networked computers for criminal purposes is a significant and growing phenomena which is already costing Australia millions of dollars. A 1997 Australian Government law enforcement survey reported significant increases in both the sophistication and number of external attacks on Australian companies in the past 18 months financial systems and confidential corporate data were the two most frequently attacked information types (....) a number of respondents (...) expressed concern as to the vulnerability of their financial systems to attack (OSCA, 1997, para. 4.09)

Regrettably, the risks are not limited to crime. They span the spectrum from accidents to malicious attacks. Accidents include natural disaster, unanticipated problems (such as the Year 2000 Bug or Y2K problem), technical faults, and user error. Threats include, dis-information, hate/revenge (personal or work-related), crime, commercial or military espionage, state and non-state based terrorism, and information warfare.
In early 1998, both Queensland and Auckland, New Zealand, were afflicted with severe blackouts as key choke-points (or nodes) in the electricity distribution networks collapsed. As the Auckland crisis proved, contemporary cities quickly grind to a halt when electricity, telecommunications and financial networks are out of action. But think of the consequences of nation-wide computer breakdowns that could happen on 1 January 2000. Everything from your family video and microwave, the world wide Global Positioning Satellite (GPS) system, and nuclear power plants in the former Soviet Union are at risk. The Australian Government Minister responsible for fixing the Year 2000 bug estimates the cost of fixing government mission-critical systems alone at $600 million (Fahey, 1998). Being an advanced economy, with a well-educated workforce, extensive infrastructure, a strong and growing service sector, and high levels of overseas trade and finance, Australia provides a good example of the opportunities and problems faced by a typical OECD

country in the information age. This paper takes Australia as a case study and asks specifically where, how, and why Australia's critical infrastructure might be at risk. By examining the core elements of the National Information Infrastructure (NII), such as power distributions systems, telecommunications and financial networks, it is possible to gauge whether the system is vulnerable. The evident vulnerabilities are then juxtaposed against a selection of threats, thereby creating a risk assessment. The paper will end with suggestions as to future policy options available to the Australian Government.
It should be noted however that this paper does not claim to provide an exhaustive survey of either vulnerabilities or threats. The criteria for selection were focused on the most serious threats and vulnerabilities that were evident in the open source literature at the time.

The potential for critical information infrastructure systems failure is a matter for a ***joint*** private sector and whole-of-government approach—as it spans all those aspects of national life that depend upon interlinked information systems. It would therefore be prudent to attempt to anticipate the risks of both accidental and malicious system failures and plan for protecting the National Information Infrastructure.

INFORMATION WARFARE AND NATIONAL SECURITY

Much of the literature on information infrastructure vulnerabilities arises out of a new subject area in strategic studies—'information warfare'. It is a new and highly contested field of enquiry and in one variant refers to the ability of a military force to protect its own knowledge and information systems while at the same time attacking those of an adversary. While a concern with infrastructure is nothing new to the military strategist, new technologies have changed the way infrastructures operate, thereby demanding their re-examination in the strategic context. The same can be said of traditional approaches to military technology.

Information warfare has also been associated with the so-called 'Revolution in Military Affairs' (RMA). While the RMA is a highly contested concept, its supporters argue that new military applications of very high technology provide modern defence forces with a revolutionary tactical and strategic advance on past means of using military force[2]. In this new world, stealth technology, surgical precision, long range and stand-off platforms are integrated by networks of sensors, computers and command and control systems that give a 'God's eye view' of the battle space[3]. No longer a three dimensional world of land, air and sea, the battle space integrates these with two 'new' dimensions - space and cyberspace - where the conduct of war depends on compressing time and distance. The RMA is also concerned with developing new organisational structures to assist in optimising new technologies, and in this respect has been referred to as a Revolution in Management Affairs[4].

This development comes at a time when three other trends are converging. First, organised violence increasingly concentrates on civilian targets. The focus of war since the last century has shifted from being the preserve of governments and the armed forces to involve entire civilian populations. Likewise, the spectre of terrorism concentrates on 'soft' targets. Second, out of desperation, revolutionary powers have often used new technologies in innovative ways that have given them, initially at least, a decisive advantage in war.

This century has observed incredible changes in technology for war-fighting purposes, from horse-drawn artillery to nuclear intercontinental ballistic missiles. As a rule, revolutionary powers have been much more imaginative than *status quo* powers in their development of doctrine and organisational structures coupled with new technologies. Prior to the outbreak of WWII, General Douglas Haig, the British architect of trench-warfare in WWI, stated emphatically that the coming war would be quickly won at its outset by a decisive cavalry charge. In 1939, there was rough parity between Allied and Nazi tanks, radios and aircraft. It was the combination of these technologies with new tactics that enabled the Germans to achieve stunning victories in 1939-40. 'Blitzkrieg' combined the tank with radio, airpower, and mobile infantry, in military formations (Panzer Divisions) using new doctrine unthought of by Haig and his contemporaries.

Third, the end of the Cold War, like the end of WWI, has created a period of strategic uncertainty. With high levels of unemployment, disillusionment with traditional forms of politics and deepening divisions along racial and ethnic lines, growth of anti-immigration movements, widespread job insecurity, high levels of financial speculation and an inability of conventional policy prescriptions to address any of these issues, the international political economy in some mature economies is beginning to demonstrate parallels with the inter-war years. As E.H. Carr convincingly argued of the period 1919–1939, the failure of the democracies to understand and overcome the destructive excesses of the policies that led to the Great Depression, left a policy vacuum that the totalitarian powers eagerly filled (E. H. Carr 1939, 1942, 1945). There are also parallels in the military–strategic context. As in the inter-war period, new technologies currently exist in the form of 'information weapons' but, as yet, no one has formulated the comprehensive doctrine or organisational structure necessary to bring 'info-blitzkrieg' into being. As the economic outlook continues to decline for many mature economies, which also happen to be *status quo* powers, the chances are that revolutionary powers will seek to champion their alternative either by demonstration, or worse, by force.

There is a Revolution in Military Affairs (RMA) in so much as traditional military weapons, platforms and sensors will become much less important in proportion to the growing centrality of the information dependence of civil society. This development is ushering in a new era where protection of critical infrastructure will be the key to economic success and national security. History shows that at turning points in the past, unsatisfied powers have seized the initiative—commercial, military or ideological. In the turbulence of contemporary global politics and economics, those that seek new alternatives to old dilemmas will gain a decisive advantage. The RMA's of the past have involved new weapons, strategies and organizations. The revolutionary concept of the 21st century will bypass traditional weapons and focus conflict on the heart of civil life—the information systems upon which societies depend.

National security involves much more than military defence. At a minimum, it is fundamentally about the survival of society. Pushing the definition a little further, it is concerned with the creation of the necessary political, economic, social, and environmental conditions within which society might flourish (Cobb, 1996). Clearly, an attack on the non-military NII, upon which economically developed societies so heavily depend, will be an attack on the security of that society. Indeed, in some respects, such an attack could be far more harmful to the stability and capacity of a society to function than an attack on the armed forces of the state, because it disrupts or destroys the most fundamental

infrastructural elements upon which modern society depend. It is the electronic equivalent of total war.
Consequently, the spectre of information-based conflict is the most significant threat to national security since the development of nuclear weapons over fifty years ago. Like nuclear weapons, information-based weapons relocate the strategic centre of gravity from military forces to direct attacks on civilian targets. While the use of nuclear weapons post-1945 came to be considered unthinkable, it is conceivable that information-based weapons will be used to target and destroy information dependent nations.

Information-based conflict foreshadows a new kind of conflict, where the overt, physical assault is replaced by ubiquitous, anonymous, and ambiguous subversion of society. No longer a matter of clearly defined spatial limits where an 'enemy' is clearly an outsider, such subversion can come from within or without. An information assault on the diverse and complex roots of society cannot simply be addressed by a compartmentalised bureaucracy designed to address the nineteenth century problems of gunboats and cavalry-divisions. A holistic, integrated approach is required. While few ever realised it in the past, security has always been indivisible. It will be ever more so in the future, especially in the context of securing the information and infrastructure systems upon which society, domestic and international, depend.

While a new concern for infrastructure security may have been born out of the RMA, it is not and should not be the preserve of the military strategist. As this paper seeks to demonstrate, warfare is just one of a number of potential risks Australia faces in the early 21st Century.

THE NATIONAL INFORMATION INFRASTRUCTURE (NII)

What is the National Information Infrastructure?[5] For the purposes of this paper, the NII is comprised of systems whose incapacity or destruction would have a debilitating impact on the defence or economic security of the nation. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. According to function, they can be arranged thus:

- *Core state functions:* executive government, and essential agencies such as defence, intelligence, foreign affairs and trade, finance, social security, national and state emergency services.

- *Core utility functions:* power grids, telecommunications, petrol refineries, gas and oil storage and transportation systems, transportation and traffic systems (air traffic control, GPS systems, meteorological support), and water supply.

- *Core commercial functions:* banking and financial services, mass media, business systems and communication networks.

The NII runs on the telecommunications network, and is linked to the Global Information Infrastructure (GII) via submarine cable and satellite. It is also dependent on a constant supply of energy and thus elements of the NII dependent on one another. In the next

section a detailed examination of vulnerabilities in select NII systems is presented before examining the potential threats against these systems.
Computers cannot operate without power; nor can telecommunications, the financial network, or defence communications—all areas prone to information attack and discussed below. Moreover, the interdependency of these parts of the NII complicates efforts to defend them. Growing complexity and interdependence, especially in the energy and communications infrastructures, create an increased possibility that a rather minor and routine disturbance could cascade into a regional outage. Technical complexity may also permit interdependencies and vulnerabilities to go unrecognised until a major failure occurs.

VULNERABILITIES IN THE NATIONAL INFORMATION INFRASTRUCTURE

Energy

Energy distribution in the state of New South Wales (NSW) is the responsibility of TransGrid. According to TransGrid's annual general report, the company's 'high voltage electricity transmission network is large by world standards, involving approximately 11 500 km of transmission lines and 73 substations... [and six area headquarters at] Tamworth, Newcastle, Orange, Metropolitan Sydney, Yass and Wagga' (TransGrid, 1996):

> Information systems and communication links [are] also required to enable TransGrid to manage its market operation responsibilities. The real time nature of electricity delivery involves continuous changes to achieve balance between supply and demand. Accordingly, prices, generation dispatch instructions, market information and other matters are determined each half hour leading to the need to frequently update and communicate a large amount of data. **In short, the market in its present form could not operate without computerised information systems and communication links** (TransGrid, 1996: p. 20, emphasis added).

The entire NSW power grid including generators, distribution and the six area headquarters are controlled from the System Control Centre at Carlingford, a Sydney suburb. There are two central power sources feeding the state. One is the coal-powered Hunter Valley system, situated north of Sydney. The other is the Snowy Mountains Hydro Scheme, situated just outside Canberra and south to the border with Victoria, and comprising six main power stations located at dams in the region. The power generated from this region is channelled through one key point, Yass, before it can reach Sydney. The Hunter system does, however, provide an alternative supply, with additional diversity of routes into Sydney. Nevertheless, with the Snowy Scheme out of action, the subsequent pressures on the Hunter would probably overwhelm the system.

The National Capital, Canberra, is serviced by one main substation. That station is in turn connected to only two other substations, located at Yass and Cooma. Within Canberra, most major government agencies depend on two smaller substations located in the city (City East zone and Kingston zone) and there are precious few transformers available in reserve to service the city. The computers operating the power grid can be accessed via a number of routes, including the direct dial-in diagnostic system used by technicians to monitor, detect and fix problems across the breadth of the grid. From the point of view of security, these are serious vulnerabilities. Few sections within even the Department of

Defence, for example, have an alternative energy supply to the city grids. Similarly, the joint force commanders are all located in Sydney and rely on the city's power supply as well as public communication links between themselves and ADHQ in Canberra.
As the explosion at the Longford gas refinery in Victoria in 1998 vividly demonstrated, energy distributions systems are vital to the national economy. Recent estimates suggest Australia lost up to 1% of GDP as a consequence of the Longford incident. Australia's major cities are serviced by two or three natural gas fields via extremely long pipelines that are computer controlled. Two key pipelines feeding both Sydney and Adelaide originate from the Moomba (SA) oil and gas fields. Similarly, Perth is fed from the far north west of WA by two lines, Brisbane is dependent on one line, while Melbourne relies on lines emanating from the Bass Strait platforms. In all cases, the pipelines span thousands of kilometres over uninhabited sections of the outback or under the ocean. The lines are policed in terms of physical protection. For example, one of the roles of the RAN's patrol boat flotilla is to very publicly patrol the Bass Strait oil rigs. Yet the line and the computer systems that operate them are not policed at all. The accident at Longford could have been just as easily triggered by accessing the SCADA system (Supervisory Control and Data Acquisition) running the plant.

Telecommunications

There are two major telecommunication service providers in Australia, Optus and Telstra. Telstra operates an extensive network of coaxial cable, microwave radio, optical fibre, digital radio concentrators, mobile phone cells, submarine cables and submarine fibre cables (Telstra, 1996). There are dedicated trunk switches in every capital city in a static hierarchy configuration. Routes are tested in a routine order, with the most direct route selected first. It is possible for calls between cities to bypass major hubs only if all lines through the hub are in use. Each hub is linked with other capital cities by two geographical routes and each capital city trunk switching centre should have access to the other capital cities without physically routing via a common building in the city.
While there is some redundancy on the eastern seaboard, there are also a number of important choke-points. For example, the exchanges in Katherine (NT), Woomera (SA), and Ceduna (SA), link central and western Australia to the east. Both microwave and fibre lines pass through these exchanges. If these critical nodes were attacked all terrestrial communications between the west and east would be severed. Add the exchange at Camooweal (QLD), and the entire centre of the continent would be severed from the outside except for direct satellite links and HF radio. With the exchanges gone, these remaining systems would be overwhelmed by the demands of regular telephonic and data traffic that daily cross the continent.

Australia is also a critical node in the international fibre network. Calls in and out of Australia via submarine cable and satellite are all processed through two buildings in Sydney: the Paddington exchange and the Telstra facility at Oxford Falls. Aside from Australia, there are three potential single points of failure in Asia: Japan, Hong Kong and Singapore. All South East and North East Asia connect onto this submarine fibre corridor. Links to the outside world pass from Japan to the US, and from Singapore to India and onwards to Europe via Suez. The only other separate submarine fibre links to the US and Europe pass through Australia. Within the Asian submarine cable corridor, between the two key nodes of Japan and Singapore, Hong Kong is a critical node. If it were disabled,

Asia would be isolated on the north-south axis. Were Singapore and Japan taken out of service the only remaining international links pass via Australia. Consequently, Australia is a vital international node.

The satellite communication network comprises two systems, one international (INTELSAT) and one domestic (Optus satellites). Both Optus and Telstra operate separate INTELSAT gateways at Oxford Falls in Sydney, part of an international network of nearly 400 earth stations in over 150 countries. In addition, Optus operates an INTELSAT earth station at Lockridge in Perth, as does Telstra at Gnangarra in WA. The Telstra facility is also a major link in the international satellite control network.

The Australian domestic satellite fleet was sold to Optus communications in January 1992 as an integral part of the Optus licence bought from the federal government for $800 million. 'Although they are hidden from view, Optus' satellites are a surprisingly common part of the day to day lives of Australians and Australian businesses' (Optus, 1996, p. 10). In the same publication, Optus states that their satellites carry the following types of information:

- Parts of the Optus and Telstra telephone systems
- Extensive management data nets for banks
- Remote oil and gas pipeline monitoring
- Ground to air communications and air traffic control systems
- Secure defence signals
- Mobile satellite communications (Optus B systems only)
- The Internet, and
- Radio and TV services (Optus, 1996, p. 10).

The primary Optus satellite operations control facility is located at Belrose, a northern suburb of Sydney, with a backup facility in the Perth suburb of Lockridge. A broadcast operations centre and satellite network services centre are also co-located at the Belrose facility. From Belrose, the satellites can have their position in orbit or their direction altered (as is necessary to maintain geostationary position with antennas pointed in the right direction). It is also possible to access and manipulate the signals sent and received via the Optus satellites from Belrose, and to monitor the traffic that passes through all Optus spacecraft. There is no encryption on the control channel of the two A series. Anyone with the proper equipment could easily put the A's out of action. Clearly, Belrose is a highly critical node, with redundancy provided at only one other well-known location in Perth.

Finance

The central bank, the Reserve Bank of Australia (RBA), is responsible for the overall stability of the financial system. It is banker to the banks, and the main banker to the Commonwealth Government, and some state governments. As well as supervision of banks[6] the RBA is responsible for the accounts used for 'settlement of interbank obligations arising in the payments system' (Bank for International Settlements, 1994, p. 22). In other words, clearance of its customers' cheques and electronic funds transfers are the RBA's responsibility. The RBA operates the Reserve Bank Information Transfer System (RITS) which is a *real time* gross settlement system for all accounts held by the bank (Bank for International Settlements, 1994, p. 22). A range of associated organizations work with the RBA to ensure the smooth running of interbank, securities, equity, futures, and options, clearance and settlements. The RBA is either a shareholder or has representatives on these bodies. The clearance process involves consolidation of information on debts and credits and establishment of the net position between institutions. Settlement refers to 'payment or receipt of value of net obligations established in the clearing process' (Linklater, 1992: p. 196).

The clearance process is managed by the Australian Payments Clearing Association (Ltd), which is a limited liability company. 'Net obligations arising from the clearing of instruments in this system are settled across accounts at the Reserve Bank of Australia' (Bank for International Settlements, 1994, p. 13). APCA have outsourced their operation to the Society for World Wide Interbank Financial Telecommunication (SWIFT), based in Brussels (further discussion of SWIFT below). This means that every day Australian banks clear their netted position with one another via a computer in Brussels which then transmits the final result to the Reserve Bank computer in Sydney for settlement on the accounts held by APCA members (e.g. Australian banks). The RBA computer is located at Head Office (at Martin Place, Sydney), and is linked on-line with the Reserve Bank's state branches in each capital city (except Darwin).

The banks have just 45 minutes for the clearance and settlement process—from 0800 to 0845 on each day of trading. The remaining 15 minutes before 0900 allow the RBA to intervene, if necessary, as banker of last resort in cases where a bank cannot honour its commitments arising out of the clearance process. Forty-five minutes is not much time to act if something goes wrong. The domestic banking system could not survive more than a few days if this delicate system was disrupted.

In many cases with domestic personal banking electronic transactions, network members agree their net obligations bilaterally and notify their positions to the Reserve Bank. Consequently, all major banks have central data processing centres connected to one another and the main system at the Reserve Bank. Similarly, all ATMs and EFTPOS systems are linked by one of two national networks using common systems architecture (Bank for International Settlements, 1994, passim). Notably, for reasons of 'efficiency' the central data processing centres are few in number. Problems have already been recorded where such centralisation has caused major disruption. For example, in the early 1990s, the Melbourne ANZ bank data centre was disabled when the electricity line from a tram came into contact with the bank's tin roof as a consequence of a road accident[7].

Many other significant transactions pass through the RBA's computer. For example, the Government Direct Entry Service is owned and operated by the RBA. The system electronically disperses government payments to over 600 financial institutions, which in turn distribute government payments into the accounts of millions of Australians—which include, *inter alia*, public servants, those on social security benefits and members of the armed forces. In 1993, this system conducted up to 3 million transactions a day (Bank for International Settlements, 1994, p.10).
This is a key weakness in the system. If, for example, in the lead-up to major conflict, an adversary could disrupt government payments to the armed forces and their families, it would seriously affect the morale of the forces and society generally. This kind of disruption has been foreshadowed in the past with grave political consequences. The 1975 Federal Budget crisis which threatened Supply, quickly turned into a constitutional crisis, in part because of the fact that the incumbent Government was facing a hostile Senate that could have prevented the Government from paying the armed forces (and others). With all of the government's payments passing through just one computer, the financial security of millions of Australians as well as national political and economic stability is seriously vulnerable.

Risk Assessment

A **risk assessment** juxtaposes existing vulnerabilities against likely threats to determine what is most likely to happen. Like most OECD countries, Australian NII vulnerabilities are confronted by a range of dangers, both unintentional and intentional. Accidents include natural disaster, unanticipated problems (such as the Year 2000 Bug or Y2K problem), technical faults and user error. Threats include dis-information, hate/revenge (personal or work-related), crime, commercial or military espionage, state and non-state based terrorism and information warfare.

Threats, such as terrorism, are not necessarily more dangerous than accidents, if the likelihood of a terrorist act actually occurring (other things being equal) is very low. In some cases, the probability of an event occurring is remote but the consequences so grave that such a threat must be given a high priority.

Two points must be emphasised here. The consequences of a failure of the NII would be very severe indeed. Therefore, action is required regardless of any threat probability assessments. Once probability is added in - it will be clear which risks will require the most urgent action. Second, in some instances in the Australian context, there exists a combination of high levels of vulnerability, a high probability of an event occurring and associated severe consequences. A threat hierarchy exists where these three factors overlap.

This paper's risk assessment suggests a *hierarchy* of threats facing Australia's critical infrastructures. In descending order of probability and consequence of seriously damaging Australia's national security, wealth, and international standing, they are:

- Year 2000 incompatibility
- Information-terrorism at the Sydney 2000 Olympics
- Major crime activity
- Natural disaster
- State and non-state terrorism (excluding the Olympics)
- Information warfare—civilian systems, and
- Information Warfare—military systems

Year 2000 Bug

The greatest risk regarding Australia's NII appears to emanate from an unintentional but nevertheless ubiquitous 'threat'. The Year 2000 computer incompatibility problem affects all computers everywhere, as well as embedded chips. Not only would Y2K failures impact upon individual computers and networks, their effects would concentrate on the same critical choke-points in the NII identified above, as any malicious attack. Similarly, a cascading collapse could occur—spreading out from problem systems into the general network community—threatening systems that have been Y2K 'immunised'.

Not only would Y2K 'attack' all the vulnerabilities identified in the NII *simultaneously*, the *probability* of a Y2K event is *guaranteed*. Come 1 January 2000 it is a certainty that some kind of crisis will develop—the only question concerns the extent of the ensuing dilemma. The unintended or unimagined consequences of multiple interdependent systems collapse would cripple the nation more swiftly and comprehensively than any military attack ever could.

In essence, the problem is that most hard/software has been programmed in a shorthand that only uses a two-digit year reference e.g. DD/MM/YY. These two-digit dates exist on millions of data files, in millions of applications, and in a wide variety of operating codes and hardware systems. In 2000, computers will not be able to decipher whether it is 1800 or 2200, thereby sending all manner of code, programs, applications and calculations haywire. The problem affects most computers and software embedded in electronic equipment. Correction requires the inspection, evaluation, alteration and testing of literally millions of lines of computer code—it is complex, time consuming and costly.

A great part of the danger lies in the timing and magnitude of the problem. On 01/01/00 every computer system that has not been fixed will experience some difficulty. Indeed, when it comes to interdependent computers and networks, it will only take one non-Y2K compliant link to threaten the entire chain. There is a very high risk that critical infrastructures that rely on networked computers will face serious, if not catastrophic, failure. Because it will all happen at the same time right across the country (and indeed internationally within 24 hours), it is impossible to predict the scope of the impact. Its scale, however, will be unprecedented.

Not only are key civilian infrastructures dependent on computers and networks, so are nuclear warheads, missiles and reactors, for example. At a recent conference in Canberra[8], the author asked the Chief of the United States Air Force, General Michael Ryan, whether

US strategic nuclear forces were fully protected from Y2K. He gave reassurances that all required 'patches' have been put in place. 'The USAF will fly on the 1st of January 2000' he said. However, media reports cast doubt on the ability of Russian and former-Soviet strategic nuclear forces to keep up with Y2K threats. For example, *The Sunday Times* recently reported that western intelligence sources have warned political leaders that there could be 'a giant Chernobyl' if Y2K issues are not addressed within both military and civilian nuclear systems in the former Soviet Union (*The Australian,* 1998 (a), p. 1). The same paper reported President Clinton's new Y2K adviser, John Koskinen, who suggested even US systems were not as safe as General Ryan claimed. Mr Koskinen is quoted as saying that 'it needs to be worried about… if the data doesn't function… they [US warheads and missiles] actually [could] go off' (*The Australian,* 1998 (b), p. 7).
The military is not the only concerned group. The Australian Stock Exchange revealed it has spent '$12.5 million already to safeguard its systems from the millennium bug'. It is asking Australian companies to 'outline how much exposure the company has, what measures have or are being taken and the overall cost of addressing the problem' (*The Australian,* 1998 (c), p. 1).

The responses to the ASX letter inquiring into Y2K compliance makes interesting reading, especially with regard to critical infrastructure systems. The ASX Managing Director, Richard Humphry, said that 'I haven't yet received from any State government any assurance written or verbal, that [the] utilities will be okay by 2000' (*The Australian,* 1998 (d), pp. 56-7). Indeed, the Chairman of the ASX, Maurice Newman, who was appointed by the Australian Prime Minister to chair the Federal Government's Year 2000 steering committee, has predicted a global recession in 2000 (*Business Review Weekly*, 1998, pp. 40–8). He has also highlighted problems with staging the Olympics and the risk of major failures in critical infrastructures (*Sunday Telegraph*, 1998, p. 1). As the reports from top government advisers above suggest, Y2K is the greatest threat to critical civilian infrastructures.

Threats

Having established a very significant unintentional threat in the form of the Y2K problem, it is now necessary to consider the hierarchy of potential malicious threats. None of the vulnerabilities discussed above will be important if there is not a significant threat posed to Australia. It must also be remembered that there must be four core elements in identifying likely threats: motive, opportunity, capability and willpower.
In terms of a malicious attack, the NII can be attacked in a number of ways. There is a lot of animated talk of 'electronic Pearl Harbours' in the mainstream information warfare literature (Schwartau, 1994). Attacks on the NII are not as easy to organise as such comments suggest, but they are a lot easier than one might imagine. It all depends on the target and the scale of attack envisaged.
Mass attack on the NII where *all* core systems are *totally* incapacitated will not be possible without detailed planning, intelligence, and highly-skilled personnel, mostly available only to advanced states. The fact is that the incredible array of systems and their myriad interlinkages that constitute the NII provide a form of security in their very diversity. It would not be possible to completely disable these systems without detailed knowledge of their weaknesses and the location of critical nodes within and between them. Then only a well-timed and coordinated strike might have a total effect.

As discussed below, the consequences of attack may increase where system redundancy has been degraded due to commercial imperatives to cut operating costs, centralise critical nodes, minimise maintenance schedules, and use common 'off the shelf' hard/software solutions. Nevertheless, mass attack is unlikely. If significant intelligence and planning assets were deployed for the purposes of mass information attack it would certainly be by a state and only in conjunction with other more traditional forms of organised violence. Consequently, existing intelligence and other defence assets should detect and give warning of an impending attack. However, in the event of military action, attacking core NII sites and information nerve centres would greatly aid strategic surprise and the aims of conventional warfare.

This does not mean that Australia is invulnerable. On the contrary, an attack on critical nodes could set off a chain-reaction that could have devastating effects for society. The most likely attack would focus on disruption of one or two key systems. Even small scale disruption of key systems, without adequate recovery plans and established information hierarchies in the event of attack, could severely affect government, commerce or society. Aside from physical attack, the easiest form of attack would be a denial of service attack. This does not require penetration of information systems (which requires password, systems, or source code cracking), but rather overloads key nodes from the outside. It is a form of data overload that overwhelms the systems' capabilities to respond, thereby affecting its internal operations as well.

The Tools of Info-terrorism

- Denial of service attack
- Hardware/software chipping (where special inserts are made into microchips at the time of manufacture to allow unauthorised access)
- Systems intrusion (via password cracking or exploiting operating system weakness and source code)
- Computer virus attack (logic bombs, Trojan Horses, worms)
- Physical attack (including Electromagnetic Pulse—EMP—bombs)
- Jamming and other electronic warfare techniques
- Information interception (Van Eck radiation intercept).

The most sophisticated (and consequently most difficult) form of attack is a systems penetration attack. Gaining access to systems can be a difficult and time consuming process and most high-security systems, such as those used by the military and the banks, are either 'air-gapped'[9] from external systems or are protected by technological security solutions such as firewalls. Unless one is an insider, has chipped the soft or hardware being used, or can crack or get around the firewall (and all of these have been done), it is difficult, but not impossible, to access these systems from the outside. By de-linking systems however, one loses all the advantages of advanced networked computing, such as speedy multi-user connectivity. For some that cost is too high. Consequently, in a surprising number of cases, critically important infrastructure systems are interlinked with

other systems that can be penetrated from the outside. Indeed, some are specifically designed to be remotely accessed, such as the SCADA system (Supervisory Control and Data Acquisition) which is typically used in energy distribution networks, such as oil and gas pipelines.

Terrorism

These questions are further complicated in the case of info-terrorism, the second source of threat to Australia's NII after the Y2K problem. The interests of terrorists are well served by information technologies. Low entry costs, difficulties in identifying an attack and its origins (anonymity and ambiguity) and the potential for extreme chaos throughout governments, corporations and society in general, all offer rich opportunities to terrorists. Terrorists will also be attracted to the fact that conventional notions of deterrence will be increasingly irrelevant in the context of Information Operations (Info Ops) as counter-targeting becomes difficult when an attacker launches an assault via a number of different national or international jurisdictions, using an anonymous or spoofed ID, and from a mobile laptop—possibly from within the country the terrorist is targeting.

Sydney 2000 Olympics

A key opening for a terrorist act in the near future is the Sydney Olympics in 2000. A number of past Olympiads have experienced terrorism, including Munich and Atlanta. While law enforcement organizations are concentrating on physical security they do not appear to have canvassed cyber security issues. An attack could be mounted against Australia or more likely against another country participating in the globally televised sports extravaganza. A wide range of targets and opportunities present themselves in the Olympic context. With the world looking on and with the year 2000 computer 'bug' providing 'cover', one single large-scale act could ruin the games and profoundly damage Australia's reputation.

An anonymous Australian government official recently wrote an article in the *Australian Financial Review* warning that the Federal Government had seriously failed its obligation to develop and implement a strategic security plan for the Games. With the terrorist group Harkat ul Mujahideen threatening Australia with retaliation for the latter's support of US cruise missile strikes in Afghanistan and The Sudan, Mr 'X' has warned that Canberra is unprepared for Olympic terrorism and that significant acts of violence are quite likely to occur (Mr X, 1998, p.19).

An interesting example of a highly educated, motivated, dedicated and ruthless terrorist who could have used new information technologies to great effect is the 'Unabomber'[10]. With adequate resources to fund acquisition of a computer and modem and a profound grudge against society—a Unabomber-type terrorist could wreak all kinds of damage. Certainly they would have a motive, could seek an opportunity, easily obtain a capability, whilst already possessing the will to act. If they go undiscovered as the original Unabomber was able to do for so long, the potential implications for the society the terrorist loves to hate could be major.

Such a terrorist would be capable of researching critical nodes (freely available in open sources as this paper has demonstrated) and mis-representing themselves to gain access to codes and passwords, thereby gaining access to vital systems used to run the society

against which they hold a grudge. In the age of 'down-sizing', job insecurity, government cuts to welfare as well as a range of other services (including the Universities—remembering that the Unabomber was a Harvard mathematics whiz), the potential may well exist for Unabomber-type terrorism, especially in open societies like Australia and the US when more than ever before individuals have access to and knowledge of vital NII systems and the means to attack them. It would be all the worse if the proposed Unabomber-type terrorist also happens to be the systems manager of a critically important system.

Crime

The third significant area of information operations activity is in the realm of crime. Criminals and organised crime groups have been quick to seize the opportunity afforded by new communications technologies and their rapid spread throughout society. Indeed one expert claimed in *The Australian* recently that 'big crime cartels are at least two years ahead of the business world in their take-up of sophisticated technology' (McIntosh, 1997, p.33). Of the four areas of potential threat identified above, crime is currently the most common area in which to find the active utilisation of Info Ops techniques and strategies. In information operations the techniques for attacking an air traffic control system are essentially the same as those used to attack a bank. Consequently, statistics on cyber crime are valuable indicators, as hard evidence does not exist for terrorist or military information warfare.

In 1998 the Office of Strategic Crime Assessments (OSCA), within the Australian Attorney-General's Department, conducted a *Computer Crime and Security Survey* (OSCA, 1997). The study canvassed a number of Australia's top 500 companies, government departments and other large organizations, and investigated the type, frequency and kind of information attacks these organizations have experienced in the past and fear in the future. The results make for interesting reading and suggest what might be expected in the future from terrorists and the military's competitors.

The survey notes that Australian law enforcement agencies have reported significant increases in both the sophistication and number of external attacks on Australian companies in the past 18 months, a trend that is supported by AUSCERT statistics. 'Financial systems and confidential corporate data were the two most frequently attacked information types....a number of respondents...expressed concern as to the vulnerability of their financial systems to attack' (OSCA, 1997: para. 4.09). The survey shows the following motivations for the attacks: extortion and terrorism (10 per cent), espionage (26 per cent), financial gain (10 per cent), malicious damage (4 per cent), and curiosity (49 per cent). While the majority of attacks came from within (employees, contractors and consultants), 'the threat from outsiders is growing at an alarming rate'. This Australian finding is consistent with international studies. External attackers accessed information systems via the Internet (25 per cent), remote dial-in (16 per cent) and 'other' routes (19 per cent) (OSCA, 1997: para. 4.04). A compliance and fraud officer of a major bank estimated the cost of information attack to their organization alone to be 'in excess of $500 000' (OSCA, 1997: para. 4.14).

Military Information Operations

Currently Australia faces no threat from other states in the region (MoD, 1997). This premise has been the basis of strategic guidance and defence planning for quite some time and there is no immediate reason to challenge this strategic convention. However, the long-term trends in the Asia-Pacific region are of some concern. Already many Asian countries have been rocked by financial and economic problems unthought of a few years ago.

Information operations (Info Ops) offer advantages to developing states. Less dependent on information systems in their day-to-day existence, their vulnerability to an attack is reduced. With freely available information on the techniques of Info Ops and with low entry costs, Info Ops could no doubt be an attractive option. This is compounded when one considers the spiralling costs of conventional weapons and the requisite logistic, training and support expenses of keeping those forces in battle readiness. Because they offer anonymity, Info Ops are also compatible with the requirements of covert operations, the effects of which are deniable in an Info Ops context. With increasing regional tensions even the smallest, least developed countries could develop the motive, opportunity, capability and the willpower to launch an Info Ops attack. Info Ops could be seen to offer developing states a silver bullet to overcome the asymmetries of power between them and advanced states. Unlikely as it may now appear, who knows how things might look in 2010?

Info Ops would be a less attractive option for peer competitor states however. The consequences of attacking the financial system of a neighbour are just as likely to rebound on the attacker as they are likely to disable the defender when significant interdependencies exist between them. In addition, the systemic unintended consequences could be great and affect all manner of systems upon which the attacker depends, as well as causing friction within alliances.

Much of the writing on Info Ops suggests that it will be used in isolation from other forms of military action. This line of argument is suggestive of some interesting parallels between early air power theory and early information warfare texts (MacIsaac, 1986). Yet what would be the point of a large-scale coordinated attack on Australia's NII if it was not as a precursor to an invasion? If a major conflict was in prospect, then Info Ops would be an excellent tool for the aggressor. Used as the first shot in a major conflict, Info Ops would be a key element of surprise and could seriously disable core systems of the defender. This raises a number of interesting questions regarding proportionate response and escalation control in the event of an information attack. Would an assault on a country's financial system be an act of war, presuming the attack and the attacker could be identified? How might a country respond?

WHAT SHOULD BE DONE?

Until recently, it has been very hard to raise the profile of information security because it has been viewed as a technical issue, something computer managers should be aware of but not line managers, let alone those concerned about national security. But societal dependence on information systems demands that urgent attention be paid to information security. Because Australia possesses many advantages as an information economy, the

response must be multi-faceted, concentrating on how best to exploit the opportunities presented in the 'information age' as well as seeking the best possible protection from the vagaries of informational dependence. The stronger and more secure Australia becomes as an information base the more attractive it will be to investors seeking a safe and reliable space within which to conduct their business.

There are four main proposals that could be easily adopted with minimal expense that will be canvassed here. First, encryption. This is a very contentious issue for governments, essentially because they do not want that technology 'falling into the wrong hands'. It offers a level of information protection to all that use it and the fear is that as it becomes more difficult to crack bigger keys the government will lose its ability to read what people are saying. Without going into that debate, suffice it to say that encryption can offer systems protection.

Second, when one thinks of information security the immediate response is to think 'firewall'. However studies as well as expert opinion have shown that in many cases the most important safeguards start with simple security procedures in offices and homes, such as hiding passwords. What is really needed is a change in office culture that respects the gravity of information security demands. The best way to advance new thinking on corporate information security is through awareness programs and supplementation of training regimes that emphasise the implications of getting basic computer security wrong[11].

Third, in the immediate future corporate plans must be developed to cope with an information attack contingency. For example, if the telephone exchanges upon which the Department of Defence relies for terrestrial communications were attacked, does Defence have a plan to prioritise its communication needs with the remaining available systems? What if, in addition to communications, the energy supply from the Canberra grid were to collapse, putting further pressure on a wide range of defence systems? Is there a plan at ADHQ that is practised regularly that prioritises the operations of the organization so that it can still function when core energy and communications systems are degraded? The same question can be asked of the banks or any other vital part of the NII. Rather than having a solution to these problems imposed from above, information assurance plans are best designed at the organization level. However, that does not preclude cooperation or coordination with others, either locally or internationally, on best practice in the event of a failure of a part(s) of the NII.

Finally, a National Infrastructure Protection Agency should be established within the Department of Prime Minister and Cabinet(PM&C). It should comprise a Council, Warning Centre, and Secretariat. The Council's role should be to oversee the work of the agency and to make recommendations to Cabinet to ensure the security and proper functioning of the national infrastructure. Membership should be open to Government Ministers and senior representatives of the corporations that operate the infrastructures concerned. The Warning Centre, the core of the organization, should be a nation-wide government and non-government voluntary monitoring system that can detect and trace any irregularities in the operation of the infrastructure, once system-wide benchmarking has taken place. The Secretariat should have a very small staff, drawn from existing agencies with a contribution to make in infrastructure protection.

There is a trade-off between diversity and connectivity in information systems. Diversity in information systems equates with security. However, it also complicates monitoring

activity within a system and across the interconnections between systems. Because information attacks are potentially anonymous and ambiguous, a monitoring function is vitally necessary. This core organization would benchmark existing systems and monitor, on an anonymous basis, any suspicious activity. On discovering a flaw in a system or the evidence of a threat, the organization would notify users of the problem and develop solutions to overcome the attack. Anonymity in reporting events is vital if commercial and military confidence is to be maintained.
The need for such an organization is recognised by the officials responsible for assurance of the NII in the Attorney-General's Department who argue that, at a minimum, Australia needs:

> "some central repository of information on incidents that have taken place; otherwise… there would be no way of knowing whether security is adequate. Similarly, if the information remains distributed we need a mechanism for informing organizations of the latest threats and security techniques" (Ford, 1998).

Overseeing the work of the organization would be a committee comprising representatives of those participating businesses and government agencies whose role it would be to develop recommendations to Government on regulatory strategies to enhance the security of the NII. The Government conduit would preferably be a Cabinet-ranking Minister. It would not be preferable, or necessary, to create a new ministry for this purpose. Rather, the role should be delegated to an existing portfolio, such as PM&C, which would be a natural base due to its whole-of-government focus.
Superficially, one might suspect that various competitors would not be enthusiastic about participating in such a scheme. In exchanging information they could also be exposing their position. However, the initial trends suggest that most of the organizations at the heart of the NII realise that coordination will be vital to both their individual interests and those of the group. Indeed, never was security so mutually dependent as in the realm of information technology. As the OSCA survey demonstrates, when anonymity is assured, participants are eager to learn from each other's experiences. The OSCA research is particularly compelling as it draws on both corporate and government examples and demonstrates that the two groupings are willing to work together on this vital issue.

CONCLUSION

As an example of a typical OECD state, Australia is vulnerable to information attack. There are many exposed critical nodes in key elements of the National Information Infrastructure (NII) that could be exploited merely by the mischievous or, more seriously, by aggressors. Interdependence among systems, such as telecommunications, energy, and financial networks, as well as a general dependency in modern life on information systems, present new challenges to a wide range of government and corporate authorities. Criminals and organised crime syndicates already utilise weaknesses in the NII at a significant and growing cost to society. There are grounds to believe that potential threats to the NII exist which are likely to increase in time as terrorists and aggressive states seek to exploit new technologies that can cripple societies while permitting a degree of anonymity to the attacker. Nevertheless, there is a range of strategies that can be adopted to protect both specific units as well as the system that comprises NII. Some are quite simple solutions, others require more coordination but they do not have to be prohibitively expensive. A

comprehensive strategy for Australia which seeks to build on its strengths as an information economy, complemented by making its NII more robust, would be a good starting point to enable Australia to successfully engage in the economy and society of the new millennium.

There are important lessons in the Australian case for all advanced economies such as those in the European Union and North America. Dependence of critical infrastructures on networked computers presents a whole new world of challenges to strategic planners into the 21st century. Information warfare presents especially dispersed terrorists groups with excellent opportunities to attack and severely disrupt (and at the extreme disable) the foundations of modern society upon which daily life depend. It may well turn out that only a major crisis will force states to act to protect their citizens.

REFERENCE

Australian, *The*, 1998 (a), 'Doomwatch warns of millennium meltdown', *The Sunday Times*, re-printed in *The Australian,* 14 April 1998

Australian, The, 1998 (b), 'Millennium bug threatens to detonate or destroy nukes', *The Sunday Times*, re-printed in *The Australian,* 16 March 1998.

Australian, The, 1998 (c), 'Global leaders brace for casualties', *The Australian,* 7 April 1998.

Australian, The, 1998 (d), 'The world according to Richard Humphry', *The Australian,* 7 April 1998.

D. Ball, 1987, 'The Use of the Soviet Embassy in Canberra for Signals Intelligence (SIGINT) Collection', *SDSC Working Paper* No 134.

Bank for International Settlements 1994, *Payments Systems in Australia,* Bank for International Settlements, Basle.

K. Beazley, 1987, *The Defence of Australia 1987: A Policy Information Paper,* Australian Government Publishing Service, Canberra.

Business Review Weekly, 1998, 'Computer crash', cover story, (Australian) *Business Review Weekly*, 23 March 1998.

E.H. Carr, 1939, *The Twenty Years Crisis 1919-1939*, Macmillan, London.

E.H. Carr, 1942 *Conditions of Peace*. Macmillan, London.

E.H.Carr, 1945, *Nationalism and After.* London.

A.C. Cobb, 1996, *The Evolution of the Concept of Security Since WWII Among Western International Theorists*, Unpublished PhD thesis, Cambridge University. Held in Parliamentary Library, Folio No. 3768 c.1.

A.C. Cobb, 1997, ‘Australia’s Vulnerability to Information attack: Towards a National information Policy”, SDSC working paper #310.

F. Corr, and J. Hunter, 1992, 'Worldwide Communications and Information Systems', *IEEE Communications Magazine*, October; and 1994 'SWIFT Rolls Out Security Package', *Banking World,* March.
J. Fahey, 1998, Minister for Finance, Press Release, 24 April 1998.

P. Ford, 1998, 'Protecting the National Information Infrastructure', Australian Defence Headquarters Symposium, 12 May 1998, Information and Security Law Division, Attorney-General's Department.

M.B. Greenlee, 1996, 'Communications Security Standards', in J. W. Conard, ed, *Communications Systems Management,* Boston, Auerbach Publications.

W. Hope, 1992, 'Satellite Communications in Australia', in D. Ball, and H. Wilson, *Australia in Space,* Canberra papers No. 94.

A. Krepinevich, 1994, 'Cavalry to Computer: The Pattern of Military Revolutions', *The National Interest*, Fall.

Linklater, J., 1992, *Inside the Bank: The Role of the Reserve Bank of Australia in the Economic, Banking and Financial Systems,* Allen and Unwin, Sydney, p. 196.

D. MacIsaac, 1986, 'Voices from the Central Blue: The Air Power Theorists', in P. Paret, ed, *Makers of Modern Strategy: from Machiavelli to the Nuclear Age,* Princeton, PUP.

T. McIntosh, 'Forum to tackle hack attacks' *The Australian*, 30 September 1997.
(MoD) Minister of Defence, 1997, *Australia’s Strategic Policy*, Department of Defence.

OSCA (Office of Strategic Crime Assessments), 1997, *Computer Crime and Security Survey (1997)*, Canberra.

D. O'Neill, 1992, 'An Australian Defence Satellite Communications Capability', *Australia and Space,* Edited by D. Ball, and H. Wilson, Canberra Papers No. 94, SDSC, Canberra.

Optus, 1996, *Industry Development Report 1996*, an Optus Communication Publication.

Optus, 1996, *Satellite Information*, Optus publications, 1996.

W. Schwartau, 1994, *Information Warfare: Chaos on the Electronic Superhighway*. New York, Thundermouth Press.

SWIFT Annual Report, 1995, quoted in T. Manzi, 1996, *Financial Warfare: Assessing threats to the US Financial Infrastructure,* Unpublished thesis, Faculty of the US Joint Military Intelligence College.

Sunday Telegraph, *The*, 1998, 'Olympics threatened by Y2K', *The Sunday Telegraph*, 22 March 1998.

Telstra, 1996, *Broadband Bearer Network Australia Map*, 1996 produced by the National IDN Region Capacity Planning Centre in Melbourne.

TransGrid, 1996, *TransGrid Annual Report 1996*, Sydney.

A.Wrigley, 1990, The Defence Force and the Community: A Partnership in

Australia's Defence, Australian Government Publishing Service, Canberra.

X, Mr., 1998, "Canberra fails Olympic security test", *Australian Financial Review*, 2/9/98.

NOTES

1 The view expressed in this article are those of the author and may not be attributed to the Information and Research Services (IRS) or to the Department of the Parliamentary Library. Readers are reminded that this is not an official parliamentary or Australian government document.

2 RMA sceptics argue that the technologies associated with the RMA have existed for some time, for example, the first precision-guided munition was used in WWII.

3 One of the problems with this conceptualisation is that it is not well designed to overcome problems in asymmetric conflict—where an ill-equipped and poor adversary may not be susceptible to a computer attack because the most advanced forms of military technology they need are a machete and AK-47. The Vietnam and Afghanistan conflicts, as well as more recent events in Rwanda and Somalia, suggest the potential problems with over reliance on technology as a substitute for political solutions or sound security policymaking.

4 I am grateful to Dr Jerry Everard of the Australian Defence Intelligence Organization for this use of the term RMA. In fact, as some recent studies have shown, in past conflicts where roughly comparable technologies were available on each side, those that revolutionised their command structures and operational plans were those most likely to succeed. See (Krepinevich, 1994).

5 See for a US example the 15 July 1996 US Executive Order 'Establishment of President's Commission on Critical Infrastructure Protection Commission'.

6 Other bodies regulate the credit unions and securities, such as the Australian Financial Institutions Commission (credit unions), Australian Securities Commission (securities), and the Insurance and Superannuation Commission.

7 Example arose in discussion with ANZ officials, 16 August 1997.

8 Royal Australian Air Force 1998 Air Power Conference, 30–31 March 1998.

9 Air-gapped means simply that the systems are not connected to other systems (such as the Internet).

[10] The Unabomber (Theodore Kaczynski) was notorious in the United States for 17 years for sending parcel bombs that killed a number of people. He had a manifesto published that railed against society and presented his 'reasons' for seeking to destroy it. He was finally arrested in 1996 after a tip-off from his brother.

[11] At an information warfare conference at the Australian Defence Force Academy, a senior defence information security expert noted that if more people practised office procedure for hiding information then a significant amount of security violations would be reduced.