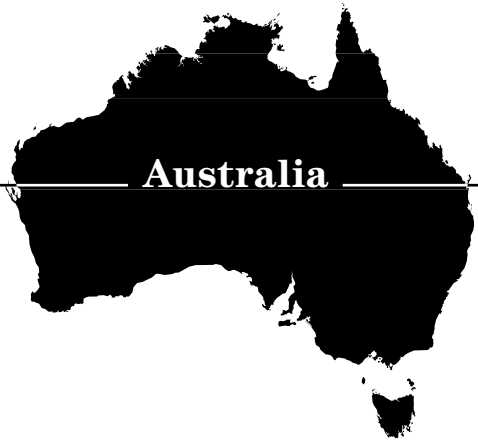
CIIP Country Surveys



Australia

This Country Survey of Australia 2004 was mainly written by Adam Cobb, Director Stratwise Strategic Intelligence, Australia.

Australia

Critical Sectors

The Australian government defines critical infrastructure as "infrastructure which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on social or economic well-being or affect national security or defence."[32] Australia's national information infrastructure (NII) is defined to include the national network within and through which information is stored, processed, and transported; the people who manage and service the network; and the information itself.[33] The prime minister has defined the aim of CIIP as "to assure Australians that both the physical safety of key assets as well as the information technology systems on which so many of them depend are protected".[34]

The scope of Australian critical infrastructure includes the following items:[35]

- Communications (Telecommunications (Phone, Fax, Internet, Cable, Satellites) and Electronic Mass Communications),
- Energy (Gas, Petroleum Fuels, Refineries, Pipelines, Electricity generation and Transmission, Nuclear Research Reactor),
- Finance (Banking, Insurance, and Trading Exchanges),
- Food Supply (Bulk Production, Storage, and Distribution),
- Government Services (Defense and Intelligence Facilities, Houses of Parliament, Key Government Departments, Foreign Missions and Key Residences, Emergency Services (Police, Fire, Ambulance)),
- Health (Hospitals, Public Health, and Research and Development Laboratories),
- Manufacturing (Defense Industry, Heavy Industry, and Chemicals),
- National Icons (Buildings (e.g., Sydney Opera House), Cultural, Sport, and Tourism),

32 Attorney General's Department National Security Website (http://www.ag.gov.au/). http://www.nationalsecurity.gov.au/www/nationalsecurityHome.nsf/Web+Pages/5C51DE424EB541C2CA256C95000A8DDA?OpenDocument.

33 Attorney-General's Department. *Protecting Australia's National Information Infrastructure. Report of the Interdepartmental Committee on Protection of the National Information Infrastructure.* (Canberra, December 1998), pp. 7–8.

34 Media release from Australian Prime Minister Howard's office, see http://www.pm.gov.au/news/media_releases/2001/media_release1367.htm.

- Transport (Air Traffic Control, Road, Sea, Rail and Inter-modal (Cargo Distribution Centers)),
- Utilities (Water, Waste Water, and Waste Management).

Technology is relied upon to operate, monitor, and maintain these vast, exposed networks and the fragile information grids that underpin them.

In a big country such as Australia with a dispersed resource base, redundancy in distribution networks, and in the information systems upon which they depend, has been kept to a strict minimum due to cost pressures. For example, Australia's biggest city, Sydney, is dependent on three sources of power, not all of which are distributed through redundant networks with backup systems. Another vulnerability may be created when all power lines supplying a metropolis are channeled through a single relay station, making it into a potential choke point.[36]

The air traffic control network has recently been upgraded to a fully computerized and *automated* system called TAAATS (*The Australian Advanced Air Traffic System*). Clearly, business continuity plans are vitally important in the TAAATS concept, and much attention has been paid to ensuring redundancy within and between the two control centers (Brisbane and Melbourne). However the TAAATS website does note that it relies on just three major nodes in its packet switching network.[37]

Both TAAATS control centers also have alternative power supplies. That is not true for a wide range of federal government installations, including key military sites that are totally dependant on civil infrastructure.[38] A study of the power and communication distribution networks in the capital, Canberra, and their limited connections to the rest of the country, suggest that a terrorist attack against just 3 key sites could degrade (possibly severely) the functioning of federal government, including key agencies responsible for national security.[39]

35 Attorney General's Department National Security website, with additions.

36 Cobb, A.C., *Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks*. Foreign Affairs, Defence and Trade Group, Research Paper 18 (29 June, 1998); http://www.aph.gov.au/library/pubs/rp/1997-98/98rp18.htm. See also Cobb, A.C., *Critical Infrastructure Attack: An Investigation of the Vulnerability of an OECD Country*. In: Information Operations. Bosch, J.M.J., H.A.M. Luijf, and A.R. Mollema (eds.), Netherlands Annual Review of Military Studies (NL ARMS) 1999. ISSN: 0166-9982 (Tilburg, 1999). http://www.tno.nl/instit/fel/refs/pub99/nlarms.html.

37 http://www.airservicesaustralia.com/mediainfo/informationfeatures/abouttaaats/hardwaredetails.htm.

38 Cobb, A.C., *Thinking about the Unthinkable*, op. cit.

39 Ibid.

Many of Australia's assets rely on the country's vulnerable NII. For example, Australia recently signed landmark oil and gas contracts with the People's Republic of China, estimated to be worth more than $50bn over twenty years.[40] The resources for this historic deal will be extracted in one of Australia's most remote, exposed, and infrastructure-poor regions, the North West Shelf. The deal with China is of national significance, but rests on a very fragile basis. The maritime oils fields are spread over a vast stretch of sea; they lie thousands of kilometers north of Perth and far from major defense bases. The regional communications network has very little redundancy, and its fuel distribution system almost none. The North West Shelf is Australia's most critical infrastructure in terms of both vulnerability and value.

Any comprehensive risk assessment requires an evaluation of threats against the vulnerabilities identified. The first such study in Australia, undertaken in 1997 by the *Strategic and Defence Studies Centre*[41], part of the *Australian National University*, assessed terrorism as the most likely form of threat against Australia's critical infrastructure and estimated that while the vulnerabilities were great, the threat at that time was low.[42] That assessment considered all forms of attack, including, but not limited to, cyberattacks. Interestingly, that assessment discussed the possibility of hijacked airliners being used on suicide missions, a proposition considered so outrageous and alarmist at the time that it was edited out of subsequent editions of the paper.[43]

The low threat environment has dramatically shifted to a high threat environment since that first assessment was made. Australia's closest ally and strategic partner is the United States. Australia has been at the heart of all coalition operations in the war on terrorism and in Iraq. Following the Afghanistan campaign, Osama bin Laden has singled out Australia for special mention in most of his public statements.

Cyberattacks have already occurred. Australia's biggest Internet Service Provider (ISP), Telstra, was disabled for over three weeks due to a series of attacks in October 2003. Businesses were forced to go without Internet and

40 http://news.ninemsn.com.au/Business/story_52627.asp; http://abcasiapacific.com/news/stories/asiapacific_stories_974625.htm.

41 http://rspas.anu.edu.au/sdsc/index.html.

42 Cobb, A.C., *Australia's Vulnerability to Information Attack: Towards a National Information Policy*. Strategic and Defence Studies Centre, ANU, Working Paper, No.306, 1997.

43 Cobb, A.C., *Thinking about the Unthinkable*, op. cit, was the next edition of the ANU Working Paper where the airliner scenario was edited out.

e-mail services, causing damage untold, but estimated to be comfortably in the millions of Australian dollars.[44] The crisis demonstrated just how much Australian business has become dependant on a functional Internet system, and hinted at the scale of costs that could be expected to reoccur in future.

Australia has significant vulnerabilities across its critical infrastructure. While the general terrorist threat against Australia has increased dramatically, it remains to be seen to what extent groups like al-Qaida and Gema'ah Islamiyah will turn to cyberattack as a modus operandi.

Initiatives and Policy

Reassessing Australia's National Security Policy

The attacks in the US on 11 September 2001 and on Bali on 12 October 2002 have prompted a thorough reassessment of Australia's national security policies, organizations, and laws. Some of these changes have had some impact on CIIP initiatives, but the core focus has been on counter-terrorism (CT) and CIP. Interestingly, by 2001 a number of important changes had already been made in the CIIP field, such as the establishment of the E-Security Coordination Group, which was charged with creating the E-Security National Agenda in September of the same year (see below).[45]

CIIP funding in the May 2001 Budget was AUS$2m. This jumped to AUS$6m the following year.[46] Compared to the AUS$2bn devoted to all counter-terrorism arrangements, these are trivial amounts. They reflect the government's continuing skepticism about the possibility of cyberattack, but also the fact that government has a limited "moral leadership" role to play insofar as Australia's critical infrastructure is operated almost entirely by private companies.

Early developments included legislative reform, such as the *Australian Security Intelligence Agency* (ASIO*) Amendment Act* (1999)[47] and the *Cybercrime Act* (2001)[48]. Developments in 2003 include the creation of

44 'Storm on BigPond, users attack Telstra', *The Sydney Morning Herald*, 21 October 2003, http://www.smh.com.au/articles/2003/10/20/1066631346473.html?from=storyrhs.

45 http://www.noie.gov.au/projects/confidence/Protecting/nat_agenda.htm.

46 The 02–03 Budget reported the increase as AUS$24.9 million over four years.

47 http://www.aph.gov.au/library/pubs/bd/1998-99/99bd172.htm#Passage.

48 http://www.aph.gov.au/library/pubs/bd/2001-02/02bd048.htm.

49 National Counter-Terrorism Plan, http://www.nationalsecurity.gov.au/www/nationalsecurityhome.nsf/AllDocs/RWPCD8501294925DA06CA256D42001C1A4C?OpenDocument.

the National Counter-Terrorism Plan,[49] the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN), and the Australian High Tech Crime Centre (AHTCC). The latter two developments are extensions of existing arrangements. TISN takes over from the Consultative Industry Forum, and the AHTCC is a new national policing initiative run by the Australian Federal Police.

National Counter-Terrorism Plan (NCTP)

The introduction of a *National Counter-Terrorism Plan* (NCTP)[50] in June 2003 added a new policy dimension to CIIP insofar as it outlined national responsibilities, albeit in a cursory way, with respect to CIP. Because almost all of Australia's vulnerable CI is operated by networked computers connected through communication nets that comprise a key part of CI, the absence of specific policy direction with respect to CIIP in the NCTP is highly ambiguous. Consequently, the government needs to clarify the interrelationship between the *E-Security National Agenda* (see below) and the NCTP. Indeed, neither document is very specific on a range of matters. It is not known if the classified versions are more specific and robust, and better conceived than those that can be accessed publicly.

In November 2003, Australian authorities said they had discovered a suspected al-Qaida terrorist cell in Sydney.[51] Its alleged bomb-maker, Willy Brigitte, a former French soldier, reportedly owned photographs of Australia's only nuclear reactor.[52] The Australian Radiation Protection and Safety Agency reported that a successful attack on the Lucas Heights medical research reactor, located in a Sydney suburb, could contaminate the entire population of Australia's largest city (4 million people).[53] The head of ASIO, Australia's peak security agency, told a parliamentary enquiry that, while there were "many unanswered questions", Brigitte could indeed have intended to harm

50 Ibid.

51 Australian authorities had been monitoring Gema'ah Islamiyah, which was responsible for the 2002 Bali, and 2003 Jakarta, bombings. JI had established "mantiki 4", a regional operation based in Australia, and there have been unconfirmed reports of efforts as far back as before the Sydney Olympics to attack Australia. http://quickstart.clari.net/qs_se/webnews/wed/ad/Qindonesia-hambali.Rpc1_DSB.html.

52 Terrorists could radiate Sydney: report, *The Bulletin Magazine*, 12 November 2003, http://news.ninemsn.com.au/National/story_8377.asp; see also http://bulletin.ninemsn.com.au/bulletin/eddesk.nsf/0/F990BCFC4B94A14ECA256DD60008E5B7?open.

53 Ibid. See also, "Ruddock silent on 'plot to attack reactor' claim", *Sydney Morning Herald*, 10 November 2003 http://www.smh.com.au/articles/2003/11/10/1068329468981.html.

Australia.[54] With such potential physical threats against critical infrastructure, it is perhaps understandable that the focus of government has been applied to counter-terrorism and CIP initiatives at the expense of a more robust and, in particular, a more coordinated approach to CIIP.[55]

Organizational Overview

Public Agencies

While the *E-Security Coordination Group* (ESCG) is the overarching governmental agency with particular focus on *policy*, the *Critical Infrastructure Protection Group* (CIPG) is the *operational* arm of government with respect to CIIP.

E-Security Coordination Group (ESCG)

The *E-Security Coordination Group (ESCG)* is the government's core policy development and coordination body on all e-Security matters. Its main tasks are the development of a secure and trusted electronic operating environment, raising awareness of e-Security, reporting of incidents, and information-sharing. The ESCG is chaired by the *National Office for the Information Economy* (NOIE).[56]

The establishment of the ESCG in February 2001 clarified the diffuse structure of government organizations involved in CIIP. Prior to the formation of the ESCG, a range of organizations across government had played some part in CIIP issues, but the system lacked a clearly defined lead organization. With no leader, there was also no chain of command, no clear set of responsibilities, no coordination of disparate CIIP efforts across government and between government and the private sector, and no formal CIIP policy.

In September 2001, the ESCG produced the first national strategy for CIIP: the *E-Security National Agenda*.[57] This is a brief outline of responsibilities

54 "Brigitte 'in plot to blow up reactor'", *Australian Financial Review*, 12 November 2003, http://203.26.51.49/articles/2003/11/11/1068329561183.html.

55 'Australia leaves the hack door open to cyber sabotage', *The Sydney Morning Herald*, 8 April 2003, http://www.smh.com.au/articles/2003/04/07/1049567603965.html.

56 Dale, Tom. "Who's Who in eSecurity and eCrime". *eSecurity and eCrime Conference at Baker & McKenzie Cyberspace Law and Policy Centre*. (Sydney, 19–20 July 2001). http://www.austlii.edu.au/au/other/CyberLRes/2001/17.

57 http://www.noie.gov.au/projects/confidence/Protecting/nat_agenda.htm.

rather than a thoroughly structured and comprehensive policy document but it is a great leap forward from earlier efforts.[58]

National Office for the Information Economy (NOIE)

The *National Office for the Information Economy* (NOIE), which incorporated the *Office of Government Online* (OGO) in late 2000, is Australia's lead agency for information economy issues. Established in 1997, it was tasked with the establishment of a globally leading online economy and society through developing, overseeing, and coordinating government policy on electronic commerce, online services, and the Internet.[59] For example, it was deemed that all government services should be made available online. NOIE has direct responsibility for the development and coordination of advice to the government on issues related to the information economy.

NOIE is not a security agency, which makes it an unusual choice for the chair of the *E-Security Coordination Group* (ESCG) given the latter's specific role with respect to E-Security matters.

Critical Infrastructure Protection Group (CIPG)

The main task of the *Critical Infrastructure Protection Group* (CIPG) is to conduct threat and vulnerability assessments of key participants in the telecommunications, finance, and electricity sectors, and of air traffic control.[60] The CIPG is chaired by the Attorney-General's Department, and its members include the *Defence Signals Directorate* (DSD), the *Australian Security Intelligence Organisation* (ASIO), and the *Australian Federal Police* (AFP) – all operational military, security, and police intelligence services respectively.

Defence Signals Directorate (DSD)

The *Defence Signals Directorate* (DSD) is Australia's national authority for signals intelligence and information security. DSD is responsible for advising state agencies on how to implement effective IT security. It does so by providing expert assistance to agencies in relation to cryptography and network security, and by developing guidelines and policies on implementing security. DSD's information security (INFOSEC) activities include information and incident collection, analysis, and warning services; setting

58 See the first edition of the CIIP Handbook: Wenger, Andreas, Jan Metzger, and Myriam Dunn (eds.), *The International CIIP Handbook: An Inventory of Protection Policies in Eight Countries* (Zurich: Center for Security Studies, 2002).

59 Ibid.

60 http://www.asio.gov.au/Media/Contents/electronic%20environment.htm.

awareness and certification standards; defensive measures, including protective security measures; response arrangements ranging from technical responses to single incidents to crisis management arrangements; and contingency planning.

Australian Security Intelligence Organisation (ASIO)

The *Australian Security Intelligence Organisation* (ASIO) is Australia's domestic spy agency.[61] Its primary mission is to provide advice to protect Australia from threats to national security. ASIO gathers information and produces intelligence enabling it to warn the government about situations that might endanger Australia's national security. It focuses on terrorists, political violence, and people who may clandestinely obtain sensitive government information or otherwise harm the country's interests. Further ASIO functions include the provision of security assessments and protective security advice. ASIO has a CIP section that is involved in producing assessments of vulnerabilities in, and threats to, critical infrastructure. The section is also concerned with INFOSEC threats, but relies on data generated by DSD for this purpose.

ASIO has the power to covertly enter and search the premises of those it suspects of espionage or terrorism. The *ASIO Act* (1979) was subsequently amended *(ASIO Amendment Act)*[62] in 1999, to give the organization the same covert access to the computers and computer systems of targets. Since the introduction of the *Cybercrime Act* (2001),[63] the ASIO's discretion in terms of targets has widened considerably, and now also pertains to CIIP investigations. Following the introduction of new counter-terrorism legislation in 2003, ASIO can detain and question suspects without charge for up to seven days. Previously, ASIO was unable to interrogate suspects, and relied on the Australian Federal Police to carry out police actions on its behalf or based on the intelligence ASIO had covertly generated.

61 Its functions are set out in the Australian Security Intelligence Organisation Act 1979. The Australian Secret Intelligence Service (ASIS) is Australia's overseas intelligence collection agency, it engages primarily in human intelligence (HUMINT) activities. ASIS's activities were only codified in law in 2001 – *Intelligence Services Act* (2001). The Australian system is based on British intelligence arrangements, and consequently the corresponding departments in the UK are: DSD: GCHQ, ASIO: MI5, ASIS: MI6.

62 http://www.aph.gov.au/library/pubs/bd/1998-99/99bd172.htm#Passage.

63 http://www.aph.gov.au/library/pubs/bd/2001-02/02bd048.htm.

The Australian Federal Police (AFP)

The introduction of the *Cybercrime Act* (2001) prompted the Australian Federal Police (AFP) to join forces with state and territory police, to create a national organization to address the threat of cybercrime. The line dividing cybercrime and cyber-terrorism is blurred because many of the tools and techniques are common to both activities. Consequently, the creation of the *Australian High Tech Crime Centre* (AHTCC) [64] is a major and important CIIP measure. AHTCC is the main Australian law enforcement unit involved in the investigation of electronic attack against the National Information Infrastructure.

Public Private Partnerships

The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN)

Building on the recommendations of the first *Consultative Industry Forum* (CIF),[65] in November 2001, the prime minister announced the formation of the *Business-Government Task Force on Critical Infrastructure*. The task force recommended replacing the CIF with a *Trusted Information-Sharing Network Infrastructure Protection (TISN)* [66] and associated advisory council. The TISN and council were established on 29 November 2002.[67]

TISN is intended to allow the owners and operators of critical infrastructure to share information on important issues such as business continuity, consequence management, information system attacks and vulnerabilities, e-Crime, protection of key sites from attack or sabotage, chemical, biological, and radiological threats to water and food supplies, and the identification and protection of offshore and maritime assets. It is, however, unclear from public documents how its approach differs from that of the earlier *Consultative Industry Forum* (CIF), which was plagued by the usual problems besting public private partnerships immersed in highly confidential commercial and national security environments.[68]

64 http://www.ahtcc.gov.au/.

65 This Forum resulted from the government's first report in the CIIP field, NII Report 1998, op. cit.

66 http://www.cript.gov.au/.

67 See http://www.cript.gov.au/.

68 The TISN is chaired by the Attorney-General's Department (AGD), which is a security-related agency. Prima facie, it would appear to have made more sense to locate the TISN in NOIE, and correspondingly the ESCG would have been a better fit in the AGD.

Early Warning Approaches

There are two key organizations that provide comprehensive cyberattack early warning services in Australia. The *Defence Signals Directorate* (DSD) provides early warning to federal government IT networks, and AusCERT provides the same services to private sector operators of CI. In addition, the Australian Government has recently launched the *OnSecure* website to strengthen the country's information security.

Information Security Incident Detection Reporting and Analysis Scheme (ISIDRAS)

The *Defence Signals Directorate* (DSD) maintains the rather cumbersomely entitled ISIDRAS scheme (*Information Security Incident Detection Reporting and Analysis Scheme*). ISIDRAS is an IT incident-reporting scheme for Australian government agencies specifically concerned with high-level incidents that could cause damage to the government's IT infrastructures. The type and extent of DSD resources applied to ISIDRAS is unknown. For example, it is not known whether DSD merely reacts to reports of suspect activity, or whether it has a proactive capability. DSD has released a breakdown of the types of incidents ISIDRAS experienced in FY 01–02,[69] but has decided not to release this information for subsequent years.

Australian Computer Emergency Response Team (AusCERT)

The *Australian Computer Emergency Response Team* (AusCERT) is a non-profit organization located at the University of Queensland. It provides an important information security service to the private sector and to some government agencies. AusCERT's aims are to reduce the probability of successful attacks, to reduce the direct costs of security to organizations, and to lower the risk of consequential damage.[70] In May 2003, the Australian government announced the launch of AusCERT's *National Information*

69 http://www.noie.gov.au/publications/presentations/esecurity/DSD1/dsd5.HTM.
70 http://www.auscert.org.au, and NII Report 1998, p. 2.

Technology Alert Service (NITAS)[71], which is sponsored by the federal government. NITAS provides a free service to subscriber owners and operators of the NII.

OnSecure Website

The *OnSecure* website was jointly developed by the *National Office for the Information Economy* (NOIE) and the *Defence Signals Directorate* (DSD) and allows government agencies to securely report information security incidents online rather than by mail or facsimile. Launched in December 2003, *OnSecure* will make it easier for Government agencies to report any attempted hacking, denial of service or other breaches of information security. It will also help the DSD to analyze incident reports more quickly and effectively, to identify any developing patterns and to assess the resulting threat level.

OnSecure also has a public site, www.onsecure.gov.au, which makes information security resource material available to the general public. The site will help Internet users to understand and respond to potential e-Security threats and will provide access to information and advice on issues such as spam, viruses, and fraud.[72]

Corporate Sector Initiatives

It is notable that in the past few years, a series of major listed telecommunications and IT companies have established private global data monitoring and incident response services of the kind provided by *Defence Signals Directorate* (DSD) and AusCERT, but for corporate clients. Their physical, electronic, biometric, and cyber-/network security measures are highly advanced.[73]

71 http://www.nationalsecurity.gov.au/www/attorneygeneralHome.nsf/0/64534A395BA69AF4CA256D24007BDCA2?OpenDocument.

72 http://www.onsecure.gov.au.

73 Information provided by Adam Cobb.

Center for Security Studies, ETH Zurich
Volume 2, Zürich 2004.

The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries

Myriam Dunn and Isabelle Wigert

edited by
Andreas Wenger and Jan Metzger