CIIP Country Surveys

Australia

Australia

Concept of CIIP and Description of System

In Australia, critical information infrastructure protection (CIIP) is perceived as vital to the maintenance of community and business confidence. 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"[1].

The Australian national information infrastructure (NII)[2] is seen as the backbone of the information society, and therefore as the crucial element of CIIP. Some of the elements of the NII are critical to Australia's defense and the country's economic and social well-being. In many cases, attacks on the NII would impact those elements depending on the NII. Serious disruptions to the functioning of society or an inability to govern effectively could result.[3]

The following are the CI sectors in Australia:[4]

- Banking and finance,
- (Tele-) Communications,
- Energy and utilities,
- Information services,
- Transport and distribution,
- Other critical government services (including defense and emergency services).

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

2 The 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.

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

4 NII Report 1998, 7.

CIIP Initiatives and Policy

CIIP Initiatives

Since the end of the 1990s, several important steps have been taken to better manage CIIP in Australia. In the 2002/2003 budget, the Commonwealth government allocated AUS$ 24.9 million over four years to continue its efforts to protect the national information infrastructure (NII), which is largely in private hands. The budget allocation will enhance the capability of agencies within the Attorney-General's office, as well as the Defence and Communications, Information Technology, and Arts portfolios to protect critical infrastructure. In addition, the government will form a partnership with industry to minimize potential harm to these crucial systems.[5]

"Australia's National Information Infrastructure: Threats and Vulnerabilities"

The report "Australia's National Information Infrastructure: Threats and Vulnerabilities" was published in February 1997 by the Defence Signals Directorate (DSD). The report contains detailed studies about the strengths and vulnerabilities of key CII sectors. The main conclusions of the report were:[6]

- The potential vulnerability of society to significant NII disruptions is increasing,
- There is a lack of formal structure for the coordination and implementation of a national policy for protecting and assuring the continued operation of critical elements of the NII in peacetime and during hostilities,
- More can be done within affordable limits to minimize existing threats.

The most important recommendation in the DSD report was the establishment of a formal structure involving the government and the private sector to coordinate and implement national policy for the protection of the NII. Further recommendations focused on the collection and assessment

5 For more information see the media release at: http://www.ag.gov.au/publications/Budget2003/mediareleases/nii.htm.

6 NII Report 1998, 11 and 56.

of information, awareness-raising and protection, and on the establishment of a national CERT and a vulnerability analysis team.[7]

Interdepartmental Committee on the Protection of the National Information Infrastructure (IDC)

In August 1997, the Secretaries' Committee on National Security (SCNS) accepted the recommendations of the DSD report and tasked the Attorney-General's Department with the establishment of an Interdepartmental Committee on the Protection of the National Information Infrastructure (IDC). The IDC report of 1998 proposed the establishment of a framework to protect against and minimize the impact of attacks, and to detect and respond to attacks on the NII.

Consultative Industry Forum (CIF)

Since much of the NII lies within the private sector, the IDC report proposed the establishment of an industry forum. It was argued that such a forum would provide a link between the government and the industry and would also provide industry input to policy development and facilitate the development of industry responses to government policy in this area. To this end, the Consultative Industry Forum (CIF) was established.[8] Initially, the CIF provided a valuable mechanism for dealing with the industry. However, concerns have been raised by industry and government representatives over the group's size, composition, and lack of strategic direction.[9]

As a result of the discussions with the industry, the Australian government decided to pursue a collaborative relationship with the industry based on the following lines:

- To hold a Business-Government Task Force meeting with the owners of NII elements,
- To encourage the development of small trust-based information-sharing groups with links to the Commonwealth in key sectors,
- To conduct an awareness-raising program,
- To hold ongoing consultations with industry interests on specific policy initiatives as they arise.

7 NII Report 1998, 1.
8 NII Report 1998, 1.
9 Interview with a representative of the National Office for the Information Economy (NOIE), April 2002.

In the aftermath of 11 September 2001, the Australian authorities have introduced stronger measures to protect CI. Those measures include airport and airline security, heightened intelligence service, additional training for staff in areas such as postal services, and increased protection for major public buildings and diplomatic posts.[10]

CIIP Policy

The Commonwealth has the authority to protect its owns interests, including national security interests. It may provide advice to the state, territory, and local governments, and to the private sector on measures to prevent or respond to attacks that have the potential to impact on the economic and social well-being of Australia. The issue is one for law enforcement unless the government decides, in the case of a specific incident, that it is a defense matter.[11]

NII Report of 1998

The Australian NII report of 1998 states that while the concept of information warfare has been largely focused on malicious attacks, information assurance can be used to protect against, or respond to, natural or accidental as well as malicious disruptions. The report argues that "unlike the physical world, where government-supplied services such as police or defense forces may be the main line of defense, information assurance is a tool that is equally relevant to both the public and the private sectors and needs to be applied accordingly".[12] The protection of the NII is seen as a joint public and private-sector responsibility.

E-Security National Agenda

In 2000, an increased rate of referrals of computer network attacks to the Australian Federal Police and a four-fold increase in reports of computer incidents to the Australian Computer Emergency and Response Team (AusCERT) could be observed. This was the government's main reason for taking a new approach. The "E-Security National Agenda" will involve the National Office for the Information Economy (NOIE) as the key player

10 Media release from the Australian prime minister's office, see http://pm.gov.au/news/media_releases/2001/media_release1367.htm.
11 NII Report 1998, 15.
12 NII Report 1998, 8.

in coordinating e-security activities across the Commonwealth and with a number of other government bodies.[13]

The 2002 Australian Computer Crime and Security Survey reported that computer security incidents or attacks had approximately doubled in the last 12 months compared to 1999 figures.[14] Case studies on e-crime are being developed in Australia as an education tool. It is expected that these case studies will educate businesses, SMEs, and consumers about the need for better protective security practices.

Law and Legislative Action

Crimes Act 1901 Part VIA

This act deals with attacks against Commonwealth computers, and with all computer attacks using the Australian telecommunications system.

Telecommunications (Interception) Act 1979

This act prohibits the interception of telecommunications (including data transmissions) within Australia except under warrant.

Crimes Act 1901 Parts II and VII

This act deals with national security offences such as treason and espionage.

Radiocommunications Act 1992

This act covers offences relating to radio emission, including interference likely to prejudice the safe operation of aircraft or vessels, interference with certain radio communications, and interference likely to cause danger, loss, or damage.

Electronic Transactions Act 1999

This act provides a liberal regulatory regime for the use of electronic communications for legal and government transactions.

There are also provisions in the Telecommunications Act of 1997 requiring a carrier or carriage service provider to enter into an agree-

13 Dependability Development Support Initiative (DDSI). *European Dependability Policy Environments*, *Country Report Australia*. (version April 2002).

14 http://www.auscert.org.au/Information/Auscert_info/2002cs.pdf.

ment with the Commonwealth about planning for network survivability or operational requirements in time of crisis, and providing that rules and licenses for carriers or service providers may require compliance with a disaster plan.

The government has introduced new computer crime legislation, the Cybercrime Bill 2001, to implement the rulings on computer offences proposed in the recently released Model Criminal Code Report. This is an important step toward achieving national consistency in this area and remedying the deficiencies in existing laws. Mirror legislation has already been implemented in New South Wales, and other states are also expected to follow suit. The proposed legislation on computer offences is designed to protect the security, integrity, and reliability of computer data and electronic communications. The penalties will provide a strong deterrent to those who engage in cyber-crime such as hacking, computer virus propagation, and denial of service attacks. Serious offences such as stalking and fraud are also covered.[15]

Organizational Analysis[16]

Public Agencies

So far, there is no single Australian authority responsible for CIIP. Rather, there are several organizations including both public and private actors that own and operate the CII. Until now security imperatives have not been as relevant as economic and commercial motivations in arriving at arrangements for infrastructure governance.[17]

Two central coordination bodies have been established in Australia to oversee the government's CIIP efforts: the E-Security Coordination Group (ESCG) and the Critical Infrastructure Protection Group (CIPG).[18]

15 Interview with a representative of the National Office for the Information Economy (NOIE), July 2002.

16 This section relies strongly on the findings of the Dependability Development Support Initiative (DDSI). *European Dependability Policy Environments*, *Country Report Australia*. (version April 2002).

17 Cobb, Adam. *Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks.* Foreign Affairs, Defence and Trade Group, Research Paper 18. (29 June, 1998).

18 http://www.asio.gov.au/Media/Contents/protecting%20NII.htm.

E-Security Coordination Group (ESCG)

The ESCG is the government's core policy development and coordination body on e-security matters for the public and private sectors. Its main tasks are the development of a secure and trusted electronic operating environment, awareness-raising on e-security, reporting of incidents, and information-sharing. The ESCG is chaired by the National Office for the Information Economy (NOIE) (see below). The E-Security Policy Section of the ESCG provides administrative support to the E-Security Coordination Group. The Section also manages the consultative industry arrangements on behalf of, and in conjunction with, other Commonwealth agencies.[19]

Critical Infrastructure Protection Group (CIPG)

The CIPG is a sub-committee of the ESCG. While the ESCG is interested in e-security issues affecting the broader economy and community, the CIPG concentrates on issues relating to the impact of critical incidents on the NII. The CIPG's main task is to conduct threat and vulnerability assessments of key participants in the telecommunications, finance, and electricity sectors, and of air traffic control.[20] Recently, the CIPG started a study on the degree of threat to Australia's NII from critical incidents. This is to become the centerpiece of the government's policy. The CIPG is chaired by the Attorney-General's Department.

Attorney-General's Department

The main task of the Attorney-General's Department[21] is to coordinate governmental efforts to identify and protect the NII and to coordinate the development of the CII policy. The Attorney-General's Department gives the CIPG executive, policy, and secretariat support. It ensures that critical NII elements are protected in accordance with the government's priorities.

National Office for the Information Economy (NOIE)

The National Office for the Information Economy (NOIE) is the lead Commonwealth agency for information economy issues. Established in 1997, it was tasked with the establishment of a globally leading online econo-

19 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.

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

21 See http://www.ag.gov.au/aghome/aghome.htm.

my and society.[22] On 11 October 2000, the Minister for Communications, Information Technology and the Arts announced that the government will expand the functions of the NOIE and establish it as an executive agency within the Communications, Information Technology and Arts portfolio. The NOIE has direct responsibility for the development and coordination of advice to the government on issues related to the information economy. The NOIE's strategy consists of:

- The development of cooperative arrangements between the public and private sectors,
- The integration of electronic and physical protective security and response arrangements,
- Encouraging further development of a response capability in the private and public sectors,
- The build-up of a database on threats and vulnerabilities,
- The development of review arrangements.

Office of Government Information Technology (OGIT)

The OGIT was established in 1995 with the task of developing efficient and effective IT strategies and systems within the government. Its principal role is "getting the government on-line". The OGIT was eventually renamed the Office for Government On-line (OGO).[23] In late 2000, the functions of the OGO were incorporated into the NOIE as part of the NOIE's expanded functions. This provided a coordinated approach to technical, regulatory, and social issues affecting government, business, and consumers in the take-up of online services and the development of an information economy.[24]

Australian Security Intelligence Organisation (ASIO)

The Australian Security Intelligence Organisation (ASIO) is Australia's security service.[25] 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

22 http://www.noie.gov.au.
23 NII Report 1998, 7.
24 http://www.noie.gov.au/about/index.htm.
25 Its functions are set out in the Australian Security Intelligence Organisation Act 1979.

ASIO functions include the provision of security assessments and protective security advice.

Cooperation between Public and Private Sectors

Cooperative arrangements between the public and the private sectors have been a fundamental part of Australia's CIIP framework since the late 1990s. A recent government initiative to develop links with industry was the inaugural meeting of the Prime Minister's Task Force on Critical Infrastructure. Held in Sydney in March 2002, the meeting was very successful in providing business input for the assessment of current arrangements to protect the CI/CII sectors.

Business-Government Task Force on Critical Infrastructure[26]

In Australia, the most important public-private partnership is currently the Business-Government Task Force on Critical Infrastructure. The overall aim is to raise awareness among the key players from the public and private sectors. The Task Force also seeks to ensure business input into the development of policies to protect Australia's CII. The Business-Government Task Force on Critical Infrastructure is co-chaired by the Attorney-General's Department, which is responsible for national security, and the NOIE, which is responsible for the promotion of the information society. However, so far, the organizational and legal framework for the Business-Government Task Force on Critical Infrastructure remains undecided. The members of the Task Force include Commonwealth government agencies, state and territory governments,[27] major companies from the private sector, and major trade associations (e.g., the water, petroleum, electrical, and internet sectors). A deliberate effort was made to ensure that participants were Australian companies rather than branch offices of US companies.[28]

26 Mainly based on an interview with a representative of the National Office for the Information Economy (NOIE), April 2002.

27 Primarily Attorney-General/Justice Departments.

28 Rathmell, Andrew: *Trip Note, Australian Business-Government Task Force on Critical Infrastructure*, 26–27 March 2002 (thanks to the author for the provision of this note).

Early Warning

AusCERT

The Australian Computer Emergency Response Team (AusCERT) is a non-profit organization located at the University of Queensland. As a single, trusted point of contact in Australia for the Internet community, 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.[29]

ISIDRAS

ISIDRAS is an IT incident-reporting scheme for Commonwealth government agencies specifically concerned with high-level incidents that could cause damage to the government's IT infrastructures. ISIDRAS is run by the Defence Signals Directorate (DSD).[30]

Warning Alert and Incident Reporting Scheme

Discussions are underway for the development of an early warning alert and incident reporting scheme. This would be targeted at SMEs and some members of the NII. The arrangements for the alert scheme are likely to commence in mid-2002. Some corporate organizations and critical infrastructure sectors that are not members of AusCERT and who do not receive global CERT and open-source information will also be included as part of the target audience.[31]

Research and Development

In Australia, CIIP research and development (R&D) is undertaken by Commonwealth government agencies, the academic community, and commercial e-security businesses. The Commonwealth has a number of industry development polices and programs that positively impact

29 http://www.auscert.org.au, and NII Report 1998, 2.

30 http://www.dsd.gov.au.

31 Interview with a representative of the National Office for the Information Economy (NOIE), July 2002.

on e-security R&D in Australia. In order to position e-security R&D as a national priority, NOIE is presently investigating additional means of augmenting these policies and programs, including through facilitating linkages between researchers in the commercial, government, and academic sectors, and increasing awareness of funding opportunities. The Defence Signals Directorate (DSD) and the Defence Science and Technology Organisation (DSTO) are looking to establish regular, targeted funding of specific e-security R&D projects.[32]

32 Interview with a representative of the National Office for the Information Economy (NOIE), July 2002.