Chapter 5

Threats to national critical infrastructure

What is national critical infrastructure?

5.1 The term 'infrastructure' is a linguistic creation of the 20th century. Infrastructure is not confined to the public sector ownership of utilities but incorporates the services which organise and drive large corporations. It includes public utilities such as water, electricity and gas supplies, air-traffic control systems, banking and finance, telecommunications and transport systems.

5.2 A definition from the Australian Bankers' Association submission states:

> The Commonwealth has defined 'critical infrastructure' as that infrastructure which, if destroyed, degraded or rendered unavailable for an extended period, will significantly impact on the social or economic wellbeing or affect national security or defence. Clearly the banking sector is a vital component of the critical infrastructure. … but it must be appreciated that the banking sector is dependent upon at least two other components of the critical infrastructure, namely the electricity sector and the telecommunications sector.[1]

5.3 The Attorney General's Department submission observes that all of these structures are increasingly – if not exclusively – controlled by computers. Any system failure would seriously affect the Australian economy, and could threaten the safety and security of Australians.[2]

5.4 The Committee notes that some witnesses differentiated between the national information infrastructure and the national critical infrastructure.[3] However, their interdependency was highlighted in two examples given in the submission provided by the Australian Bankers' Association.[4]

5.5 The first example concerned damage to the main fibre optic cable between the US and China off the coast of Shanghai. It took four to five days to fix the problem, and the Chinese economy was rumoured to have lost many millions of dollars in lost transactions.

[1] Submission no.19, p. 27

[2] Submission no.21, p. 3

[3] *Committee Hansard*, 17 July 2003, p. 3

[4] Submission no 19, p.27

5.6 The second example concerned the Auckland power blackout in 1998. Due to failure of all the main cables supplying power to the inner city, hundreds of businesses were forced to shut down.

5.7 The Committee's view is that any threat to these interdependent areas has potentially grave consequences. There is clearly a relationship between threats to critical infrastructure and terrorism, which are briefly discussed below.

What are the threats and risks?

5.8 The ACC's submission gave an example of what is thought to be the world's first environmental vandalism case. The submission notes that this case is used world wide as an example of a critical infrastructure (hacking) attack:

> Between December 1999 and April 2000, the sewerage treatment facilities of Maroochydore Shire Council, Queensland, came under sustained electronic attack. That attack resulted in an environmental disaster which saw millions of litres of raw sewage spill into rivers, parks and the grounds of a Hyatt Regency hotel. The matter was forwarded to the Queensland Police for investigation.
>
> As a result an ex-employee, Vitek Boden, was intercepted by police in a vehicle which contained a laptop computer, with wireless access to the sewerage control system. He was later charged found guilty on 30 charges involving computer hacking, theft and causing significant environmental damage, in what was described as the world's first environmental vandalism case.[5]

5.9 A more recent example was related in evidence by the Victoria Police:

> Earlier this year the Victoria Police Tactical Response Squad sought the assistance of the Computer Crime Squad in the investigation of a Melbourne man who had forwarded threatening emails against Melbourne Water to the National Terrorist Hotline. This man made a series of threats that he would remotely detonate drums of cyanide submerged in water reservoirs. The offender was apprehended and has been charged with a number of serious offences.[6]

5.10 In the latter example, there was an effective response to the threat, and it is clear that the heightened awareness of the possibility of such threats played a large part in the effective apprehension of the perpetrator.

5.11 However, the Committee notes that the earlier example appears to have taken the victims by surprise. It is clear that there is a need to stay ahead of as many potential vulnerabilities as possible, which the Committee acknowledges in this most technically complex area is not simple. This is so particularly because criminals often

[5] Submission no. 23, p.34

[6] *Committee Hansard*, 17 July 2003, p.38

have access to large financial resources to assist with developing their technical expertise.

5.12 The ACC submission gave examples of potential areas of threat.[7] These include:

- Attacks or failures within information systems which may expose a vulnerability potentially affecting others in the sector.
- Hacking into a computer network by an individual.
- Distribution of malicious software (such as viruses) which enter computer systems in order to damage them.
- Denial of service attacks, where the internet ports or email of the target computer system is bombarded with data to prevent it from communicating.
- Redirection, or spoofing, of website traffic away from its intended destination.

5.13 The Committee learned that these activities can include nuisance worms, mass-mailing email systems, blended threats (which are threats which contain malicious code which attack vulnerabilities within a system) and the viruses such as Nimda, Code Red and the SQL Slammer worm, which Symantec told the Inquiry had the potential to bring down significant portions of the Internet backbone.[8]

5.14 In a report published in 2002,[9] the Office of Strategic Crime Assessment (OSCA– now part of the Australian Crime Commission (ACC)) noted that there were risks not only from electronic attack, but also from exploitation of software or procedural vulnerabilities. This included 'social engineering,'[10] a term which was used by several witnesses. In evidence PricewaterhouseCoopers explained:

> Social engineering is getting a person's confidence so that they may tell you information that you should not rightfully have.[11]

5.15 From the evidence given, it appeared to the Committee that this particular vulnerability would be difficult to overcome through purely technical means. The solution relies on protocols, and on human beings being aware of 'social engineering' attempts to obtain information, and resisting them. While organisations need to have clear guidelines regarding the preservation of crucial information, as well as defining the consequences of breaching the guidelines, there will always be the possibility of an unpredictable breach arising from 'the human factor'.

[7] Submission no 23, p. 34

[8] *Committee Hansard*, 18 July 2003, p.70

[9] *Long-Term Criminal Risks to the National Information Infrastructure (NII),OSCA* 2002

[8] Submission no. 12a; *Committee Hansard*, 17 July 2003, p.7

[11] *Committee Hansard* 21 July 2003, p.64

Preventing infrastructure damage

5.16 Clearly, given the potential for damage to industry and the economy, the protection of critical national infrastructure is a matter of some concern. Symantec Australia gave a list of the matters considered important in determining a protection strategy:

> You have to identify what your key assets are, you have to identify where your threats, vulnerabilities and risks are, and then you have to take appropriate action and build systems around the bits and pieces of your system to make sure they all work together in harmony. … you have to prepare just in case everything goes wrong and look at business continuity management… it is not just one thing; it is a whole series of things.[12]

5.17 The Committee was concerned about just how realistic it is to expect global compliance with these standards, once established. Standards Australia's response was that a decision about where to exert security requirements comes down to having a cost-benefit basis for making that decision, because security is all about considering what you are trying to secure:

> There are trade-offs. The functionality is limited if you go for a higher rather than a lower level of security, and it is going to cost you more at the end of the day. … standards are a key issue [they] provide a language that allows you to communicate how you manage security.[13]

A view on best practice information security

5.18 In its submission, Symantec noted:

> With more than 85% of the world's critical infrastructure owned and operated by private entities, public/private cooperation is critical to securing our critical data from the rising incidence and impact of malicious activity.[14]

5.19 Symantec sets out its best practice strategies for 'government and enterprises'.[15] It summarises much of what was put to the Committee in submissions as well as in evidence. The strategies include:

- Security policies.
- Risk assessments.
- Standards, procedures, and metrics.
- Security roadmap.

[12] *Committee Hansard*, 18 July 2003, pp. 49-50

[13] *Committee Hansard*, 18 July 2003, pp. 50-51

[14] Submission no 13, p.7

[15] Submission no 13, p.8

- Selection and implementation of solutions.
- Training of security professionals and employees.
- Security management.
- Incident response and recovery.

Regional initiatives

5.20 Within the region, strategies for the protection of both the national critical infrastructure and the national information infrastructure are being studied within APEC. In evidence Mr Orlowski[16] noted that the critical infrastructure is the responsibility of APEC's counter-terrorism group.

5.21 The Committee heard that APEC's most important work in this area is ensuring that each economy or country has the capability for computer emergency response teams (CERT) to meet any emergency, and for developing a compendium of security standards. Both these tasks address strategies identified by Symantec.

5.22 While governments set their own standards, Mr Orlowski told the Inquiry:

> the extent of standards use within the private sector is very patchy between different organisations. A lot of our critical infrastructure is in fact operated by the private sector, so there is a need to ensure that they have guidance on the way they should be protecting this infrastructure on which we rely.[17]

National initiatives

5.23 The Attorney General's Department submission points out that NOIE (the National Office of the Information Economy) and the Attorney General's Department are the key agencies with policy responsibility for implementing the government's E-Security National Agenda. The operational agencies include the AFP, the Australian High Tech Crime Centre (AHTCC), the Australian Intelligence and Security Organisation (ASIO) and the Defence Signals Directorate (DSD). The Department also notes that additional agencies – including APRA, ASIC and the ACC – have been included in the establishment of AusCERT (the Australian Computer Emergency Response Team).

5.24 AusCERT was founded in 1992 and covers the private sector. The Attorney General's Department submission notes:

> AusCERT acts as a coordination centre, in an advisory capacity, as a centre of expertise and as a portal to its contacts throughout the world, for issues of computer security. AusCERT is part of the University of Queensland, and is

[16] *Committee Hansard*, 17 July 2003, p. 3

[17] *Committee Hansard*, 17 July 2003, p. 4

> a member of the Forum of Incident Reponses and Security Teams, a global organisation.[18]

5.25 AusCERT is partly funded by the Commonwealth government and raises other funds to cover its operating costs through member subscriptions and the provision of computer security training and education and consultancy services.[19] The Australian Crime Commission has recently provided funding support (along with other Commonwealth agencies) for a national incident reporting scheme and public alerts service, which will be provided free of charge to the Australian community.

5.26 The Committee was also told of a project jointly sponsored by AusAID (the Australian Aid Authority) and AusCERT. The project involves building computer emergency response team capacity in developing countries. Its purpose is to provide infrastructure to countries which might not have the level of expertise available to protect their own information infrastructure.[20]

5.27 The ABA told the Inquiry of the development of a banking and finance infrastructure advisory group which will report to the Critical Infrastructure Advisory Council (CIAC), an initiative established by the Attorney General and the Minister for Communications, Information Technology and the Arts. The Council's role is to oversee the sector advisory groups and provide advice to the Attorney-General on the national approach to protecting critical infrastructure.

5.28 The submission from the Attorney General's department explained that CIAC is a part of an initiative announced by the Prime Minister in November 2002. Alongside CIAC is the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN).

> 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.[21]

5.29 The Committee understands from the submission that TISN will use existing industry advisory groups from different sectors where possible. The Network is designed to promote a culture of trust 'based around shared threats and vulnerabilities'.[22] The Attorney General's Department anticipates that the advisory group will develop strong links to the equivalent US forums the Information Sharing and Analysis Centers (ISACs).

[18] Submission no 21, p. 22

[19] AusCert website: http://www.auscert.org.au

[20] *Committee Hansard*, 17 July 2003, p.2

[21] Submission no. 21, p.24

[22] Submission no. 21, p.24

5.30 The Committee also noted from the submission provided by the Australian Bankers' Association that there is a proposal for TISN to include a number of Infrastructure Assurance Advisory Groups (IAAGS). These groups will be representative of particular sectors: for example, the ABA will be part of an IAAG for the finance sector.[23]

5.31 While the Committee welcomes a co-operative approach to infrastructure protection, it is aware that there is a need for a consistent approach to that protection.

Training

5.32 One of the keys to a consistent approach to protection and an identified element of the best practice strategies is training. During the inquiry the Committee was advised of some of the work being progressed in this area.

5.33 Mr Orlowski indicated in evidence that APEC is providing some training to the less developed economies in the region.[24] PricewaterhouseCoopers noted that technical training must be integrated with training in presenting technical findings to a court.[25]

5.34 This need was also acknowledged in the ACC's evidence which referred to the need for training and the necessity to have access to highly specialised knowledge. However the ACC also noted the need for:

> a coordinated and perhaps far more centralised or nationally driven level of expertise, while at the state level you have the skills that might be required for your own jurisdiction.[26]

5.35 The Committee notes that effectiveness in this area demands, (as with so many aspects of the responses to cybercrime) central co-ordination of both training and expertise. The Committee considers that establishment of a such a body preferably within an existing agency should be given a high priority.

5.36 The Committee also notes that this is a matter in which the public and private sectors must work together. Almost all witnesses noted the need for, and the initiatives being taken in, public/private sector co-operation and liaison.

5.37 The Committee is concerned that although there is a proliferation of potential solutions, and many groups which are addressing the issues, there lacks (as with the other areas which are the subject of this Inquiry) a central body which has the function of keeping track of potential threats and solutions; such an organisation could act as a clearing house for this information, ensuring that it was disseminated widely and

[23] Submission no.19, p.28

[24] *Committee Hansard*, 17 July 2003, p. 2

[25] *Committee Hansard*, 21 July 2003, p.71

[26] *Committee Hansard*, 18 July 2003, p.12

appropriately. Although the Committee sees the ACC and the AHTCC contributing to this task, it does not believe that a law enforcement agency is best suited to the task.

Role of the ACC

5.38 The ACC's contribution to prevention is in sharing its experience and its intelligence, as far as it is appropriate, with other agencies who develop these strategies.

5.39 The ACC submission notes[27] that historically, the NCA/ACC has only investigated attacks on critical infrastructure concerning organised crime. However the ACC now incorporates the Office of Strategic Crime Assessment (OSCA) which has the task, among others, of assessing all kinds of criminal threats, including those in cyberspace.

5.40 The commencement of a Cybercrime Program in 2001 under the ACC's predecessor, the NCA, highlighted the possibility of threats posed by organised criminal activity to both the Australian information and the physical infrastructures. The ACC sees its new functions – notably its role in advising the ACC Board on national criminal intelligence priorities – as well as maintenance of liaison and intelligence work as important parts of its role in combating organised crime.

5.41 The Committee notes that the ACC sees its multi-jurisdictional focus on the 'high end of criminality' as a 'unique tool to Australia's response to this high risk and emerging form of criminality'.[28] The ACC also perceives its coercive powers and national intelligence framework as invaluable in the investigation of critical infrastructure attacks especially against government institutions.

5.42 The Committee supports the ACC's view of its role within an area of criminality that is merging with terrorist threats to national security. However, the Committee notes the views of the Victorian Bar in evidence in discussing the proposal that monitoring warrants – similar to those available under the *Australian Security Intelligence Act 1979* (the ASIO Act) – be available to the ACC for cybercrime investigations. The Committee was advised that this power exists already under the ASIO Act in cases in which there is a threat to national infrastructure:

> Provided the suspected behaviour fits the definition of 'security' in section 4 of that [the ASIO] Act then the fact that the behaviour is being carried out by use of cybercrime techniques will not mean that government will not be able to deal with it provided it has the necessary impact on national security.[29]

[27] Submission no 23. p. 34

[28] Submission no 23, p. 34

[29] *Committee Hansard*, 17 July 2003, p 23

5.43 The main focus of the work of the ACC is not on security but on the collection and processing of criminal information and intelligence, as set out in section 7A of the ACC Act (see Appendix 1). There is an ASIO representative on the ACC Board, which ensures an ongoing exchange of information and views at the highest level.

5.44 The ACC expressed some concern about its own vulnerabilities to attack and sees a solution in the formation of partnerships with other organisations. They include:

- AGEC (the Action Group into the law enforcement implications of Electronic Commerce) chaired by AUSTRAC, which has a focus on banking, money laundering and electronic payment systems.
- Information Infrastructure Protection Group (IIPG) chaired by AGD, with a focus on threats to the national critical infrastructure information.
- Electronic Security Coordination Group (ESCG), chaired by NOIE.
- AusCERT (Australian Computer Emergency Response Team) who have recently been contracted to provide Alerts and Warnings, and an Incident Reporting Scheme.[30]

5.45 The Committee notes the importance of the ACC's partnership approach, which as an intelligence sharing initiative will assist in keeping information about potential threats as up to date as possible. While part of the ACC is operationally directed towards major criminal activity, and apprehending the perpetrators, the former ABCI and OSCA, who have a research and intelligence focus have much to offer a partnership with other agencies.

5.46 The Committee also notes that the Commission acknowledges the need for the development of its own internal strategies which would minimise the effect of any attempt at exploitation of weaknesses in its information systems. The Committee encourages the Commission to give priority to this. However, while the Committee agrees that partnerships are necessary to combat cybercrime it would remind the ACC, and particularly the Board, of the need to continue to set its priorities within the context of its work programs.

Conclusion.

5.47 The evidence and the submissions presented to the Inquiry demonstrate a number of initiatives across both the private and the public sector aimed at minimising threats to critical infrastructure and at dealing with those which may occur. However, as with other areas within this Inquiry, there remains a need to ensure that all such initiatives are undertaken in an environment in which each interest group remains informed of the activities of the others.

[30] Submission no. 23, p. 36