

Chapter 5

Protecting Information Infrastructures

Gary Waters

Introduction

As discussed in chapter 2, the concept of Network Centric Warfare (NCW) anticipates ready access to information. This demands an ability to protect information such that its security can be as assured as its ready access. From a military perspective, therefore, the Australian Defence Force (ADF) must balance the quest for information superiority against the potential for creating an operational vulnerability. And it must do this within the broader context of balancing security and privacy as it increasingly shares information. From a national perspective, the Australian Government will wish to balance these same issues as it shares information across national security agencies and possibly with Non-Governmental Organisations (NGOs).

Reliance on information and information systems and addressing the consequent vulnerabilities raises the question of protecting along a spectrum—from simple failure to attacks from terrorists or state-based adversaries. Cyber-security demands far more attention, and while protecting critical information infrastructure addresses much of the problem, more needs to be done. Government and Defence need to develop a trusted information infrastructure and put in place the mechanism for Australia to protect its critical information infrastructure.

In addressing these issues, this chapter provides frameworks for dealing with operational vulnerabilities, cyber-terrorism, privacy, and security risk, which can be managed at the Defence enterprise level for the ADF and at the whole-of-government level for national issues.

Balancing information superiority and operational vulnerability

The pressure to ensure both a superior information position as well as security of that information within an environment of increased sharing of information has been building with the rise of NCW, increases in coalitions to deal with security threats and challenges, and the focus on domestic security since the 11 September 2001 terrorist attacks on the United States. Information superiority for the ADF will come from:¹

- seamless machine-to-machine integration of all manned and unmanned systems, including those in space, across the joint force;
- real-time pictures of the battlefield;
- predictive battlespace awareness—driven by commanders who will be required to predict and pre-empt adversary actions when and where they choose;
- assured use of information through effective Information Assurance (IA) and defensive Information Operations (IOs); and
- denial of effective use of information to adversaries through offensive IOs.

Achieving a balance between access to information and protection of that information is something of a contradiction in this age of information and globalisation. Ensuring access to information involves a number of key concepts and assumptions as follows:

- The concepts of ‘Information Superiority’ and NCW imply that all ADF commanders will have full access to relevant information.
- Commanders at all levels will continue to deal with uncertainty or the ‘fog of war’ due to a lack of complete and accurate information.
- ‘Reach back’ will allow support functions to be provided from outside the area of operations, thereby reducing the ‘footprint’ of the deployed force in the area of operations.
- There will be increasing use of civilian communications for strategic systems into the area of operations and for tactical systems within that area, through out-sourcing and commercialisation. These systems will have to be integrated with any Defence-owned and operated systems and with the systems of other Government agencies.
- The concept of ‘national information economy and infrastructure’ promotes the efficiencies of computer-based business automation and Internet-based services, which will apply equally to the national security arena.

Improved information accuracy and responsiveness are seen as key attributes that help reduce the probability of failure in modern military operations. The side which is not confounded by the ‘fog of war’ and which can get inside the decision cycle of the adversary can expect to have a higher probability of success. Information superiority requires connectivity and interoperability across all relevant force elements so that synchronised operations can be carried out at an appropriate operational tempo. The political sensitivities of operations also demand that adequate information and reporting is available at higher levels outside the area of operations.

Vulnerabilities

In terms of vulnerabilities that the ADF could introduce through increased information sharing and access, the following points are relevant:²

- Dependence on real-time information and intelligence introduces one form of vulnerability, while the sharing of that information and intelligence introduces another.
- Similarly, dependence on the security and information management policies of coalition partners and other agencies introduces one form of vulnerability, while the new interfaces with those policies of external partners introduces another.
- Key information relating to operations is distributed widely at the strategic, operational and tactical levels and is shared with coalition partners and other agencies.
- Commanders at all levels are exposed to information overload, which can saturate their ability to cope.
- Time-sensitive decisions can be slowed while commanders seek greater clarification of the situation, in the belief that the last piece of information can be found.
- Australian Government networks are dependent on commercial or allied communication systems.
- The adversary, whether State-based or simply an individual, has equal access to modern global communications and the Internet.
- Perceptions generated in political and public minds become reality and, therefore, have to be factored into any strategic and operational planning.
- More information is available at lower levels of command where there is a higher probability of capture by an adversary.

The advantages of access to information through Defence's restricted and secret systems in the normal execution of duties are expected by all personnel. Access to external email and the Internet for daily business is also expected. This dependency introduces potential vulnerabilities associated with the management of a large organisation such as Defence as follows:

- The dependence on email and Intranet for the conduct of business, both inside and outside the Department, means that any disruption of the networks and applications would have an immediate effect on the functioning of Defence.
- External connectivity provides an easy avenue for the manipulation of, and attack on, Defence's information.
- Deliberate or inadvertent misuse of the restricted system for the transmission of classified information outside Defence provides an easy avenue for the media (through whistle blowers, leakers, or paid informants) or adversaries (through sympathisers, agents or supporters).
- Disruption of personnel and pay processes would have an immediate impact on the morale and well-being of military and civilian personnel, more so when they are deployed on operations.

- Some Defence functions are contracted out and depend on e-business arrangements.

Balancing security and privacy in information sharing

Evolving national security policy in both Australia and the United States is seeking higher levels of cooperation, information sharing and system-to-system interaction across Government agencies and between the public and private sectors. Any implementation of trusted information sharing systems will demand that a number of components be addressed:³

- collaboratively developed public and private sector policies;
- the use of available frameworks, architectures, standards and technologies; and
- the deployment of systems that integrate effective risk management controls.

All three components are needed in developing trusted systems, which meet three key requirements for privacy and security—government and business requirements as well as citizen expectations.

Where possible, existing bodies of knowledge, current technologies and standards-based products should be used to build and manage the infrastructure for information sharing. In terms of information security, threat management, identity management, access management, and security command and control, capabilities exist today and can be applied effectively once appropriate policies and business processes have been established.⁴

As business privacy and personal privacy continue to become major issues for critical infrastructure protection across both the public and private sectors, an architecture will be needed to address privacy protection and to develop requirements for appropriate information privacy controls. Technologies, such as business intelligence, data management, enterprise management, and storage management systems are currently available to meet requirements.⁵ However, more needs to be done to build on the work in the private sector to foster business and personal privacy system architectures and to establish standards-based interoperability.

In the United States, the *National Strategy for Homeland Security* (July 2002) and the *National Strategy to Secure Cyberspace* (February 2003) demanded unprecedented levels of cooperation and system-to-system interaction among private sector companies and all levels of government to ensure protection of national critical infrastructure.⁶ This applies equally to Australia and the way in which the National Counter-Terrorism Committee addresses national critical infrastructure issues that reach across the Commonwealth, States and Territories. As John Sabo argues, for the United States:

This will involve new and trusted working relationships among organisations which have had little formal interaction on infrastructure protection issues, as well as on issues such as new systems, expanded network interfaces and significant increases in data collections, data flows, and data integration, analysis and dissemination.⁷

This applies equally in Australia, where common information security and infrastructure protection aspects across Government agencies need to be seen more as a national capability issue rather than simply as an operational support issue.

Managing security risk

There are four key areas in managing security risk—threat management, identity management, access management, and security command and control. These are discussed below.⁸

Threat Management controls are needed to protect networks and systems against external and internal threats. They must also be able to assess vulnerabilities, and identify and mitigate physical and systems-based risks and attacks. Essentially, it is these controls that protect the critical infrastructure.

Identity Management controls are needed to provide a foundation for ‘registering’ users and for establishing role-based access, as well as enabling role-based and portal views of information and applications. However, uniform policy development will be necessary to address the diverse perspectives of the different organisations involved.

Access Management controls are needed to protect classified, regulated and business-sensitive resources; control how resources are accessed and used; and ensure authorised availability across networks, systems and platforms.

Tiered controls for access management will probably be needed to reflect roles, information classification requirements, and particular organisational rules for information and for participants across the breadth of participating organisations and users. This will become increasingly important if new classification categories for sensitive critical infrastructure information are instigated that fall outside the scope of current security classification levels (such as Secret and Top Secret for Defence and Protected and Highly Protected for non-Defence agencies).

Security Command and Control capability is needed to effectively manage the security of the networked infrastructures. This includes such things as resource management, impact correlation, secure collaboration, intelligent visualisation and predictive analysis tools.

Managing privacy risk

Privacy is defined as ‘the proper handling of personally identifiable or business confidential information in accordance with policies having the consent of the data subject or as required by law or regulation’.⁹

Open standards-based architectures, protocols, languages or schemas do not yet exist for ensuring that privacy rules and policies can be embodied in Information Technology (IT) systems or for allowing them to be interoperable across networks that manage the collection and processing of information. Both personal privacy and business privacy requirements must be engineered into the new cyber-security architecture if Australia and the ADF are to develop and field trusted systems.

The vast quantities of data and information that may ultimately flow across network and jurisdictional boundaries will eventually demand automated management of relevant policy rules. These standardised policies and protocols will be needed for scalability, efficiency and trust reasons. Any rules will have to be enforced within an overall governance framework, the start point for which will be a privacy architecture.

There are several already defined services and capabilities that will assist in addressing privacy controls for information sharing. These include:¹⁰

- control and data usage functionality, to ensure that policies drive business rules processing;
- certification of system credentials;
- validation of data;
- interaction of data subjects, systems and processes;
- individual and business access to data as well as audit capability;
- use of agents, both technology-based and/or human;
- negotiation where appropriate; and
- enforcement of policy violations.

Many of these framework services can be supported by currently available technologies in business intelligence, data management, enterprise management and storage management, particularly when applied to enterprise implementations of data-sharing systems.¹¹

Dangers in getting privacy wrong

In March 2004, the Australian Federal Privacy Commissioner, Malcolm Crompton, argued that the case for stronger identity management was being made as a key element for preventing terrorism, preventing identity fraud, and even eliminating spam. Indeed, the case was strengthened as proponents argued how important identity management was for e-business and e-health.¹²

Malcolm Crompton highlighted some of the dangers for the community, business and government of getting privacy wrong when developing identity management solutions.¹³

- Subversion—the natural response of unwilling or suspicious participants, from reduced participation and deliberately misleading information all the way through to more active resistance.
- Pent up reaction that can produce very strong public policy responses, such as the legislative responses in the United States creating the ‘Do Not Call’ list to keep out direct marketers or the worldwide movement against spam.
- Financial loss when developed projects must be shelved.
- Self-defeating solutions that create new threats to privacy, security and identity integrity.
- Creating the foundation for a total surveillance society, the full implications of which may only be recognised after it is too late.

Technological solutions can be a key part of getting privacy right in this area. Some technologies, such as biometrics, have the potential to enhance privacy depending on how carefully they are designed and implemented. But some of our thinking needs to change, such as the assumption that full identification is needed in all circumstances. Solutions to the issues that Crompton highlights include finding the right answers through technology, law and accountability processes. A critical issue will be the need to fully engage all stakeholders in vigorous public debate along the way.¹⁴

Search engines, such as Google, have become increasingly more powerful, just as the World Wide Web has become a richer source of information as more individuals, businesses and government agencies rely on it more and more to transmit and share information. The information is stored on servers that are linked to the Internet.

Any errors can lead to this information, which is not meant for public viewing, being made available to the public. Errors can come through improperly-configured servers, inadequacies in computer security systems, or simply human error. It is virtually impossible to pull back the information once a search engine has found it.

An article in the *Sydney Morning Herald* on 18 February 2004¹⁵ highlighted that Google’s search engine ‘crawled’ over every web page on the Internet on a bi-weekly basis. It ‘grabbed’ not only every page on every public server, but also every link attached to every page, and then catalogued the information.

The article¹⁶ also highlights vulnerabilities which can bring up spreadsheets, credit card numbers and social security numbers linked to a list of customers, as well as total dollar figures in financial spreadsheets. It would be virtually impossible to monitor the tens of millions of searches that occur every day,

according to a search engine expert, Tom Wilde.¹⁷ The concern goes even further in terms of the potential for identity theft and identity fraud, as well as other cyber-crime aspects discussed in chapter 3.

Research by AusCERT¹⁸ found that 42 per cent of 200 organisations surveyed had information compromised through attacks on their IT networks. That same research highlighted that in 2001 Optus was breached and 425 000 user names and passwords were compromised.¹⁹

Cyber-security

Thomas Homer-Dixon postulates a future scenario:²⁰ In different parts of a US state, half a dozen small groups of men and women gather. Each travels in a rented mini-van to its prearranged destination—for some, a location outside one of the hundreds of electrical substations throughout the state: for others, a point upwind from key, high-voltage transmission lines. The groups unload their equipment from the vans. Those outside the substations put together simple mortars made from materials bought at local hardware stores, while those near the transmission lines use helium to inflate weather balloons with long silvery tails. At a precisely coordinated moment, the homemade mortars are fired, sending showers of aluminium chaff over the substations. The balloons are released and drift into the transmission lines.

Simultaneously, other groups are doing the same thing along the eastern seaboard and in the south and southwest of the United States. A national electrical system already under heavy strain is short-circuited, causing a cascade of power failures across the country. Traffic lights shut off. Water and sewerage systems are disabled. Communications systems break down. The financial system and national economy come to a halt. And if that is not of sufficient concern, Brad Ashley²¹ of the US Air Force notes that:

Today's battlefields transcend national borders. Cyberspace adds an entirely new dimension to military operations, and the ubiquitous dependence on information technology in both the government and commercial sectors increases exponentially the opportunities for adversaries as well as the potential ramification of attacks.²²

Indeed, Ashley goes well beyond Homer-Dixon's scenario and depicts a number of scenarios all rolled into one devastating attack.²³ Ashley postulates that military systems are under relentless electronic attack and the global media is reporting these attacks with great zeal, thereby adding to the problem. An unknown adversary has seized control of military logistics, transportation and administration systems associated with deployment of forces.

Commercial websites are inundated with requests for connection, which paralyses parts of the Internet. Worldwide computer virus attacks occur, affecting

over 60 million computers, including military systems. An orchestrated campaign of individuals flooding Defence and security websites is carried out, a cyber Jihad is started, and national infrastructure computers are infiltrated, leading to raw sewage being released into rivers and coastal waters.

Worse still, Defence networks are penetrated, power grids are infiltrated and shut down, computer problems close the stock market in several capitals. The competitive media helps spread the ensuing panic throughout the world.

If these incidents sound plausible, it is because they have occurred, in varying forms and to varying levels of success over a lengthy period of time. However, were they to be orchestrated over a very short time span as Ashley postulates, their results could be devastating.

To some, the scenarios postulated of Homer-Dixon and Ashley may have sounded far-fetched in 2000; however, the 11 September 2001 terrorist attacks on the United States changed all that. Many nations have since realised that their societies are susceptible to terrorist attacks. There are two trends that explain this: the growing technological capacity of small groups or even individuals to wreak havoc; and the increasing vulnerability of economic and technological systems to quite deliberate and specific attacks.

Adding to the vulnerabilities are the changing communications technologies that now encompass satellite phones and the Internet which permit the coordination of resources and activities across the world. Criminal and terrorist organisations can use the Internet to share information on weapons and tactics, transfer funds, and plan criminal activities or attacks. The links between crime and terrorist organisations mean that any criminal cyber-attack could be financing a terrorist organisation. Identity theft is also cause for concern for banks and financial institutions, as once again a criminal cyber-attack could be linked to a terrorist organisation.

There are several reasons why hackers will seek to gain illegal access to IT systems. These include: to gain financially, to commit sabotage, to steal identities, to commit fraud, to carry out espionage, or to cover up other physical theft. The level of sophistication needed to hack into sites has decreased while the availability of hacking tools has increased substantially. As Ashley notes, adversaries in cyber-space require minimal technology, little training or funding, no infrastructure support, and can launch attacks from anywhere at anytime.²⁴ A report in 2004 by Trend Micro indicated that viruses affecting personal computers (PCs) cost businesses worldwide some US\$13 billion in damages in 2001, US\$20 billion in 2002, and US\$55 billion in 2003.²⁵ Add to this, the estimated annual loss due to computer crime of US\$67.2 billion, for US organisations alone.²⁶

Information-processing technologies have also boosted the power of terrorists by allowing them to hide or encrypt their messages, with the power of a modern lap-top computer today exceeding anything that could have been imagined three to four decades ago. Not only can terrorists and criminals run readily available sophisticated encryption software, they can also use less advanced computer technologies to achieve similar effect. Steganography (hidden writing) that allows people to embed messages into digital photographs or music clips which can then be posted on the World Wide Web for subsequent downloading was reportedly used by terrorists who planned an attack on the US embassy in Paris in 2004.²⁷

The World Wide Web also provides ample access to information about critical infrastructure. For example, the floor plans and design of the World Trade Center in New York were readily available, as was information on how to collapse large buildings. Instructions for making bombs and other destructive materials are also readily available. Indeed, practically anything needed on kidnapping, bomb-making, and assassination is now available on-line.²⁸

Australia's economic and technological systems make the nation, the Government and the ADF all the more vulnerable because of the interconnectedness across modern society and the increasing geographic concentration of wealth, people, knowledge, and communication links such as highways, rail lines, electrical grids, and fibre-optic cables. As societies modernise, their networks become more interconnected, which means that the number of nodes increases, the links among the nodes increases, and the speed at which things move across these links increases. All of this adds to the rich array of potential targets.

Not only does vulnerability increase through greater numbers, but also the features of interconnected networks can make their behaviour unstable and unpredictable. One obvious example is that of a stock market crash, in which selling drives down prices, which, in turn, leads to more selling. The tight coupling of networks also makes it more likely that problems with one node can spread to others. The United States has experienced a number of cascading effects when electrical, telephone, and air traffic systems have suffered partial failure, which has spread across the country. In addition, the nature of these networks also sees a small shock producing a disproportionately large disruption.²⁹

A special commission set up by President Bill Clinton in 1997 reported that 'growing complexity and interdependence, especially in the energy and communications infrastructures, create an increased possibility that a rather minor and routine disturbance can cascade into a regional outage'. The commission continued: 'We are convinced that our vulnerabilities are increasing steadily, that the means to exploit those weaknesses are readily available and that the costs [of launching an attack] continue to drop'.³⁰

So much for physical networks: what about psychological networks? Australian citizens are nodes in this network, linked through the Internet, satellites, fibre-optic cables, radio, and television news. Immediately after a crisis, the media and others report the story across this network. Televisions stay on, telephone lines and e-mail messages are used constantly, to the extent that services, especially the Internet, become noticeably slower immediately after the event.

The Australian Government should expect terrorists of the future to target the critical networks that underpin society. This would include networks for producing and distributing energy, information, water, and food; the highways, railways, and airports that make up the nation's transportation grid; and the health care system.³¹ While an attack on the food system would be of greatest concern to people, vulnerability of the energy and information networks attract a lot of attention because they so clearly underpin the vitality of modern economies.³²

The use of Supervisory Control and Data Acquisition (SCADA) systems that monitor and direct equipment at unmanned facilities from a central point pose a worrying potential vulnerability. In 1998, a 12-year old hacker gained control of the SCADA systems that run the Roosevelt Dam in Arizona and, in 2001, a disgruntled worker, Vitek Boden,³³ released waste water in Maroochy Shire, Queensland. More than three million SCADA devices exist throughout the world.³⁴

The real concern is that these SCADA networks sit 'squarely at the intersection of the digital and physical worlds. They're vulnerable, they're unpatchable, and they're connected to the Internet'.³⁵

SCADA systems are used to digitise and automate tasks such as opening and closing valves in pipes and circuit breakers, monitoring temperatures and pressures, and managing machinery on the assembly line. As these systems connect to corporate networks and as those corporate networks connect to the Internet or adopt wireless technology, the vulnerabilities become more pronounced. The power grid could be taken down, emergency telephone systems could be rendered useless, floodgates to a dam could be disabled, and so on.

These control systems have been designed and developed with efficiency and reliability in mind, not security. Many of the legacy control systems cannot accommodate the newer security technologies such as encryption. Compounding these technical difficulties is a range of cultural and management issues, firmly rooted in the physical world, that pays scant attention to cyber-security concerns.

Initially, SCADA systems were developed with proprietary technology, with no connectivity to corporate networks. However, the impact of globalisation and the Information Age demanded greater efficiency, greater transparency and

greater connectivity, which resulted in linking the control networks to corporate networks. This means that hackers who seek to insert worms and viruses in corporate networks can get an additional dividend in that any connectivity to control systems that are not turned off can be affected by the worm or virus.

It was in this way that the Sasser virus disabled several oil platforms in the Gulf of Mexico for two days in 2004, while the SoBig virus affected the rail signalling and dispatching systems of CSX Transportation in August 2003, stopping train services for up to six hours.³⁶

While Distributed Control Systems were the predominant form of control systems decades ago, whereby they existed within a small geographic area (say a single manufacturing plant), had all components (hardware, software, master controllers, workstations, etc) provided by the same vendor, and operated over a dedicated Local Area Network, that is no longer the case. The proliferation of SCADA systems across a wide geographic area to distribute oil and electricity in the main sees a lot of master systems communicating with remote devices over the Internet, wireless radio, the public telephone system, or private microwave and fibre-optic networks. The remote units are not only controlled by their master, they also send real-time data back.

The SCADA networks themselves are also vulnerable because of their dependency on the telecommunications that support them. Transmissions could be intercepted and altered, redirected or even destroyed, so the transport medium introduces another area of vulnerability. The use of dial-up modems, where little or no authentication is required, introduces yet another form of vulnerability. Not many companies would operate today without firewalls and Intrusion Detection Systems (IDS) on their IT networks, yet very few have such security mechanisms on their control networks. Even if firewall filters were fitted to the control networks, most firewalls have been designed to filter Internet Protocols (IPs) but not control system protocols.

It is not just about improving SCADA systems, however. More can be done to improve the information security on the corporate networks. Improved router configuration, antivirus software, IDS, and more diligent software patching would all help reduce the vulnerability. There are also non-technology actions that can be taken, such as improved configuration management, better documentation of network architectures, and better contingency planning.³⁷

Returning to the broader issue of cyber-terrorism, it is worth noting the US House Armed Services Committee's Sub-committee on Terrorism, Unconventional Threats and Capabilities consideration of 'Cyber Terrorism: The New Asymmetric Threat'³⁸ on 24 July 2003. The Committee chairman, Jim Saxton, argued that the rapid flow of information was becoming increasingly important on the battlefield. He said that in the nineteenth century three words per minute could be transferred whilst 38 830 soldiers were needed to provide information over

10 square kilometres. In the 1990–91 Gulf War, the transmission rate was increased to 192 000 words per minute whilst only 24 soldiers were needed to cover 10 square kilometres. It is expected that by 2010 the data transfer rate will be further increased to one trillion words per minute whilst only three soldiers will be needed to cover 10 square kilometres.³⁹

At the same hearing, Dr Eugene Spafford⁴⁰ said that threats from malicious software (malware) had grown steadily for 15 years and threatened military, government, industry, academic and general public information systems. The interconnections across these segments of the community meant that a threat to one could readily spread to the others. His concern is exacerbated by the malware's use of victim computers to carry out the attack, which presents an asymmetric threat to computer systems.

Spafford went on to say that the malware threat to US systems, and the military in particular, is significant because software is at the heart of most advanced systems, spanning weapons, command and control, communications, mission planning, and platform guidance. Furthermore, intelligence, surveillance, and logistics all depend on massive computational resources.⁴¹

There is also the threat from simple failure that must be factored in. Systems are becoming more complex and much of the software is commercial off-the-shelf (COTS) and not developed to contend with active attacks and degraded environments. Moreover, software vendors have tended to concentrate more on time-to-market as the most important criterion for success, rather than well-designed and well-tested code.⁴² Increased connectivity, whereby systems are configured so that every machine has network access, which is needed to provide for remote backups, access to patches, and user access to World Wide Web browsing and e-mail, adds to the threat.⁴³ Spafford went on to offer a number of recommendations:⁴⁴

- Explicitly seek to create heterogeneous environments so that common avenues of attack are not present.
- Develop different architectures.
- Rethink the use of COTS software in mission-critical circumstances.
- Rethink the need to have all systems connected to the network.
- Require greater efforts to educate personnel on the dangers of using unauthorised code, or of changing the settings on the computers they use.
- Revisit laws that criminalise technology instead of behaviour.
- Provide increased support to law enforcement for tools to track malware, and to support the investigation and prosecution of those who write malware and attack systems.
- Do not be fooled by the 'open source is more secure' advocates. The reliability of software does not depend on whether the source is open or proprietary.
- Initiate research into the development of metrics for security and risk.

- Establish research into methods of better, more affordable software engineering, and how to build reliable systems from components that are not trusted.
- Emphasise the need for a systems-level view of information security. Assuring individual components does little to assure overall implementation and use.
- Establish better incentives for security.
- Increase the priority and funding for basic scientific research into issues of security and protection of software. Too much money is being spent on upgrading patches and not enough is being spent on fundamental research by qualified personnel.
- Most importantly, re-examine the issue of the insider threat to mission critical systems.

There are clearly deficiencies in US and Australian cyber-defences. Malicious and incorrect software pose particular threats because of their asymmetric potential—small operators can initiate large and devastating attacks. The situation cannot be remedied simply by continuing to spend more on newer models of the same systems that are currently deficient. It will require vision and willingness to make hard choices to equip the military and other national security agencies with the defensible IT systems they deserve.⁴⁵

Mr Robert Lentz, Director, Information Assurance, Department of Defense also gave testimony at the hearing,⁴⁶ where he argued that a new era of warfare had emerged, through the greater power, agility, and speed afforded by connectivity. Thus, a smaller force can mass combat effects virtually anywhere, anytime through these multiple connections. However, this increasing dependence on information networks creates new vulnerabilities, as adversaries develop new ways of attacking and disrupting friendly forces.

Lentz also described the goals that then Defense Secretary Rumsfeld established for networks, namely to⁴⁷

- develop a ubiquitous network environment;
- richly populate the network environment with information of value, as determined by the consumer; and
- ensure the network is highly available, secure and reliable.

Through these goals, Secretary Rumsfeld was seeking to establish the Department's IA Program—the strategy, policy and resources required to create a trusted, reliable network. While the challenges for IA are substantial because of the size and diversity of the Defence and national security IA community and because IA is both pervasive and interdependent upon many other policies and processes, there are clear opportunities. In the first instance, the policy formulation process could be more open, more visible, more collaborative, and, as a consequence, faster.⁴⁸

Lentz also made the telling comment that the US Administration did not expect to achieve guaranteed protection of its information, systems and networks. However, it had put in place 'a robust Computer Network Defence capability within the Department, a capability that continues to evolve and transform itself in pace with the evolving and transforming threat'.⁴⁹

Finally, Lentz offered a telling reason for factoring legacy systems into strategic planning, by saying that all systems are legacy systems as soon as they go on-line. The demand for greater bandwidth, functionality, connectivity and other features is constantly expanding. Lentz argued that the demand would be met, but that the greater task was to ensure it was met securely. To that end, development of protective technologies for space-based laser, advanced fibre-optic, and wireless transport networks were being pursued, as was the development of end-to-end IA architectures and technologies.⁵⁰

The rate of adoption of Internet-based technology, including dependence on the Internet for voice communications and data distribution, means that nations today have the ability to conduct cyber-warfare.⁵¹ Thus, organisations need to have a strategy for keeping their businesses running, if information systems and facilities that depend on those information systems are unable to operate.

The increasing use of IP networking technology to connect critical infrastructure and the movement to packet-switched voice communications (away from a circuit-based architecture) has increased the vulnerability. Additionally, Voice over Internet Protocol (VOIP) equipment is susceptible to traditional Internet threats like worms, viruses and break-ins from hackers. Denial of Service (DS) attacks, which have been experienced in recent times and taken down websites, could be used to disrupt the flow of voice-carrying packets on an IP network, thereby causing a major breakdown in communications. At the infrastructure level, interfaces that allow maintenance and control of equipment have traditionally been accessed through dial-up modems, and are increasingly being converted to IP network connections.

The Gartner Report⁵² identified potential targets as the network interfaces found in equipment used by dams, railroads, electrical grids and power generation facilities, and the interface points between the public switched telephone network and IP networks. Connecting computer systems in banking and finance, law enforcement, rail transportation, and in industries such as chemical, oil and gas, and electrical to IP networking adds to the increasing vulnerability of critical infrastructure.

Most security technology, when used in conjunction with 'best practices', is appropriate to the proportional risk presented by the threat of cyberwarfare. ... The proportional-risk assumption does not mean that

a cyberwarfare attack would be unsuccessful if undertaken by a determined foe, but that risk is low.⁵³

The phrase 'digital Pearl Harbor' has been around since 1995, according to Jim Lewis in 2003, then with the Center for Strategic and International Studies and a former Clinton Administration technology policy official.⁵⁴ Lewis considered the threat from cyber-terrorists to have been over-stated. Indeed, work carried out by Gartner in 2003 highlighted that disgruntled insiders, not foreign terrorists, posed the greatest cyber-security threat to companies.⁵⁵

Even the most comprehensive IT security technology cannot stop the careless, uninformed, or disgruntled person with access to the network from wreaking havoc. 'The fact is that some of the most devastating threats to computer security have come from individuals who were deemed trusted insiders'.⁵⁶

Costs associated with security policies and software are significant enough, without having their effect decreased by insiders who may not fully appreciate their role in maintaining a secure enterprise. The main reasons behind internal security breaches are noted as ignorance, carelessness, disregard for security policies, and maliciousness.⁵⁷ Hence, the best way to address the potential for such breaches is through an awareness and education program, aimed at reducing the effect of 'social engineering'.

Social engineering plays upon the inherent trust that people have in one another and their basic desire to help others. Social engineering tactics will not work if people are informed and aware. Thus, employees should not open unsolicited email attachments and they should scan attached documents for a virus before opening them. They should be aware that attackers will seek to take advantage of a natural trust in sharing files. Employees who use Internet Relay Chat and Instant Messaging services should know about ploys that might be used to lure them into downloading and executing malware that would allow an intruder to use the systems as attack platforms for launching distributed DS attacks. Employees should treat with extreme caution any requests for passwords or any other sensitive information.⁵⁸

Richard Hunter of Gartner has cautioned companies to alert their employees against social engineering. Hunter's view is that the most successful ways for foreigners to steal US secrets is to use such practices or to buy US companies in possession of secrets. After all, computer hacking constitutes only 6 per cent of theft attempts.⁵⁹

At a conference in 2004, concern was expressed over US federal agencies not securing their computer networks and failing to factor technology security into long-term planning. House Government Reform Committee Chairman, Tom Davis, called for increased investment in IT security infrastructure, but acknowledged that the appropriations process 'is always about the here and

now'.⁶⁰ The problem is, of course, that information network defence requires long-term investment and top-level attention, which is not a natural by-product of the annual budgetary cycle.

The Internet continues to hold so much promise, but, according to the *Economist*, it has to become more trustworthy if it is to realise its full potential.⁶¹ Detracting from trust in the Internet is the continuing worm and virus attacks such as the Blaster worm and SoBig virus that attacked in 2003, causing estimated losses of US\$35 billion.⁶² As the uptake of broadband increases and as more PCs and other devices are connected, the potential fall-out from further virus, or the more insidious worm, attacks can only increase.

The speed with which these attacks can be launched is also increasing (i.e. attacks are happening faster). The time from initial disclosure of a flaw to the attack by the Slammer worm in January 2003 was six months, which halved the time taken in the previous year. For the Blaster worm in August 2003, the time had fallen drastically to three weeks.⁶³ Over 500 000 computers were infected and CSX Corporation had to stop its train services as its rail signalling system was brought down, and check-in services of a number of major airlines were disrupted.⁶⁴

Worse still, the intensity of attacks has increased, with the Slammer worm infecting 90 per cent of vulnerable computers within 10 minutes.⁶⁵ The network-security monitoring firm, Qualys, has argued that most organisations take on average one month to patch their known vulnerabilities, whereas future attacks could inflict their intended damage within a couple of minutes.⁶⁶

On 27 January 2004, the world experienced the MyDoom virus (also known as Norvarg or Shimgapi). It was immediately rated as a high-level security threat, geared as it was around mounting DS attacks on SCO's website (a US software company). Attacks, such as this, which aim to bring down a company's systems by flooding them with traffic, could very well be precursors to cyber-attacks by nations or terrorist organisations.

Indeed, John Donovan's (Managing Director of Symantec—an Internet security company) research indicated that politically motivated attacks were likely to increase.⁶⁷ The attack on SCO was even more insidious as MyDoom left a communications port open on the infected computer, which could have been remotely accessed by a hacker.

Furthermore, as Robert Lemos (a staff writer for CNET News.com) argued, such a virus allowed hackers to hide their real locations, thus making it very difficult to trace any on-line attack. The Code Red virus infected many computers in July 2001, with tens of thousands still infected in 2004 (according to Lemos).⁶⁸

The Sobig.F virus of August 2003 accounted for one out of every 17 email messages and infected over 570 000 computers, while MyDoom accounted for

one in 12. Message Labs (a company that filters email for corporate customers) had detected and quarantined more than 1.5 million infected emails within 27 hours.⁶⁹ The Sobig virus could have launched an Internet-wide attack had its programming been so designed.⁷⁰

The dramatic increase in cyber-incidents can be seen from the following statistics—between 1995 and 2005, the reports to Carnegie Mellon's Computer Emergency Response Team increased from 171 incidents to 5990.⁷¹

Trust in the Internet is also undermined through fraud and spam. Indeed, the statistics quoted by the *Economist* are alarming—citing that some 10 per cent of all emails were scams of one sort or another.⁷² The degree of cunning in much of this fraud is worrying; for example, brand spoofs that claim to come from trusted companies, fake web pages, fake press releases, and 'phishing'—tricking recipients into giving out sensitive information, such as credit-card numbers, pin numbers and passwords.

Most companies, government agencies and indeed a number of private individuals are now using firewalls to keep malicious code out of their internal networks, and IDS that analyse what gets past the firewalls. Anti-virus software has become commonplace, although there remains a concern over how up-to-date that software is.⁷³

While many argue that greater government intervention is needed, that is likely to simply drive up the cost of being connected. Others argue that software vendors should be liable for its security—in other words, vendors should be writing simpler, safer software. So, perhaps, the solution is a combination of both, whereby government legislates that vendors are liable. This would then compel software companies to carry product-liability insurance. Insurance companies would respond by pricing the risk, whereby software companies that write safer code would have an economic advantage.⁷⁴

Another option might be to eliminate Internet anonymity, such that every user could be traced.⁷⁵ One way of doing this might be to authenticate each email before it can be sent, by referring to a driving licence, passport, tax file number, social-security number, or some other trusted form of identification.⁷⁶

As Ed Waltz observes, by using a basic risk management approach we can aim to prevent access to 80 per cent of possible attacks.⁷⁷ We can detect the presence of the remaining 20 per cent, noting that we would seek to contain 19 per cent of those attacks, and aim to have in place the recovery mechanisms for the 1 per cent that are not prevented, detected or contained.⁷⁸ Even with this methodology in place, we must acknowledge that there may be attacks from which we cannot recover and, therefore, we also need to cater for that residual of less than 1 per cent.⁷⁹

Functions that are needed to support protection include monitoring the information infrastructure; generating alerts if an attack is detected or anticipated; controlling the response to modify protection levels or restore service if an attack has been carried out; conducting forensic analysis (including attack patterns, attacker behaviour, damage, and so forth); and reporting to higher authority.⁸⁰

The potential for individuals, organisations or nation-states to mount an information attack with the intent of exploiting, disrupting, or manipulating Australian Government or ADF operations is increasing, to the extent that some analysts have coined the term ‘weapons of mass effect’, because they can threaten national interests.⁸¹ Hence, it would be prudent for the Australian Government and the ADF to develop the capabilities for discerning, deterring and defending against such threats.

The Australian Government recognises the country’s increased vulnerability to acts of cyber-terrorism and other e-security threats because of the nation’s growing dependence on the information economy. Accordingly, the Government has designed an e-security policy framework to⁸²

- enhance e-security awareness and practices amongst home users and the business community;
- promote the security of Australia’s national information infrastructure through information sharing and collaboration with the private sector;
- ensure the government’s electronic systems are appropriately secure; and
- promote the security of the global information economy through international engagement.

The Australian Government has also enacted the *Cybercrime Act 2001* to ‘prosecute groups who use the Internet to plan and launch cyber-attacks that could seriously interfere with the functioning of the government, financial sector and industry’.⁸³ The Government’s definition of cyber-attacks includes activities such as hacking, computer virus propagation and DS attacks.

Computer Emergency Response Teams (CERTs) have been set up internationally to improve computer systems’ security. Australia has set up a team, AusCERT. This is a not-for-profit body operated by the University of Queensland. The Attorney-General’s Department also has the Australian Government Computer Emergency Readiness Team (GovCERT.au) that

develops and coordinates government policy for computer emergency preparation, preparedness, response, readiness and recovery for major national information infrastructure incidents. It also acts as a point of contact within the Australian Government for foreign governments on CERT issues, and coordinates any foreign government requests.⁸⁴

Australia is also leading an Asia-Pacific Economic Cooperation (APEC) initiative to build CERT capacities in developing economies.

The Australian Federal Police (AFP) hosts the Australian High Tech Crime Centre, which investigates e-security incidents in public and private sector organisations. The Centre 'performs a national coordination role for the law enforcement effort in combating serious, multi-jurisdictional crime involving complex technology'.⁸⁵

While the Australian Government and the Australian business sector have established solid risk management guidelines and adhere to sound international risk management standards, Heinrich de Nysschen argues that:

in future a concerted effort will have to be maintained, building on current efforts, involving all stakeholders, to develop proactive and reactive IT risk management strategies. Only then could we ensure that Australian IT systems, infrastructure and assets are secure, and able to effectively mitigate the impact of potential future security incidents.⁸⁶

Heinrich de Nysschen's view tends to be echoed by comments in 2006 from the US Cyber Security Industry Alliance, which argued for a short list of high priorities on communications and cyber-security to be addressed very quickly.⁸⁷ First, a more aggressive research and development program to build secure information systems is needed to mitigate the risk. Of the US\$1 billion science and technology budget for the US Department of Homeland Security (DHS) in 2007, only US\$20 million is earmarked for cyber-security.⁸⁸ The second priority is an early-warning system, while the third is the ability to assure communications bandwidth in an emergency. The fourth priority is a plan to recover the Internet after a disaster and to cope with the interim.

Critical Infrastructure Protection in Australia

Critical infrastructure covers

those systems we all rely on in our day-to-day lives—communications networks, banking, energy, water and food supplies, health services, social security and community services, emergency services and transport. These are the physical facilities, supply chains, information technologies and communication networks, which, if destroyed or degraded, would adversely impact on Australia's social or economic wellbeing, or affect our ability to ensure national security.⁸⁹

It also includes key government services and national icons.⁹⁰

The continuity of supply of all critical infrastructure is dependent, to some extent, on availability of other infrastructure. Indeed, some sectors are mutually dependent on one another. The degree and complexity of interdependencies is

increasing as Australia becomes more dependent on shared information systems and convergent communication technologies, such as the Internet.

The Australian Government is seeking 'to ensure that there are adequate levels of protective security for national critical infrastructure, minimal single points of failure and rapid, tested recovery arrangements'.⁹¹ Furthermore, the government sees its role as providing strategic leadership on national critical infrastructure protection through the Attorney-General's Department. This department is responsible for

providing national coordination in areas of joint Commonwealth, state and territory responsibility, producing and communicating relevant information to key government and non-government stakeholders, promoting critical infrastructure protection as a national research priority and leading Australia's international engagement on critical infrastructure protection issues.⁹²

Compounding the challenge for government is that in some instances, around 90 per cent of critical infrastructure is privately owned. Individual companies are unlikely to have the information or resources to address the risks from a whole-of-sector perspective. Clearly, critical infrastructure protection can only be carried out by a mix of government at all levels and private companies and their industry affiliations. This is as much an awareness activity as it is a risk assessment and mitigation activity. Indeed, this statistic has led the Government to argue:

The primary responsibility for the protection of Australia's critical infrastructure rests with infrastructure owners and operators. ... Protecting Australia's critical infrastructure therefore requires high levels of cooperation between business and government at all levels.⁹³

The former Australian Prime Minister, John Howard, told a business forum on 23 June 2004 that 'we now live in a world where taking measures to improve security and fight terrorism is a cost of doing business'.⁹⁴ The *Australian Financial Review* noted 'concerns in the government' that both the Critical Infrastructure Advisory Council and the Trusted Information Sharing Network (TISN) would be more effective through greater engagement of Chief Executive Officers in counter-terrorism consultations.⁹⁵

The TISN strategy provides an overarching statement of principles for critical infrastructure protection in Australia, outlines the major tasks and assigns the necessary responsibilities across government, the owners and operators of infrastructure, their representative bodies, professional associations, regulators and standards setting institutions.⁹⁶ The TISN allows owners and operators of critical infrastructure to share information on issues related to the protection of critical infrastructure within and between their respective industry sectors.

These issues include business continuity, consequence management, information system vulnerabilities and attacks, e-crime and the protection of key sites.

The Australian Government has established the Computer Network Vulnerability Assessment Program, which

provides co-funding on a dollar-for-dollar basis to help owners and operators of critical infrastructure identify major vulnerabilities within computer systems and dependencies between computer networks, and to test the ability of systems to resist exploitation.⁹⁷

To counter this increase in vulnerability, both the public and private sectors are putting in place stronger authentication and identity management for IT systems. Two-factor authentication is coming into vogue, whereby a password or Personal Identification Number (PIN) is used together with an authenticator such as a secure ID token, smart card, or digital certificate.

The government has also created the Business Government Advisory Group on National Security, which 'provides senior business leaders with an opportunity to discuss the strategic direction of our national security policy and provide advice and feedback on national security issues relating to critical infrastructure protection'.⁹⁸ This group is chaired by the Attorney-General.

The 2004–2005 Australian Federal Budget allocated further funding to support the Government's Critical Infrastructure Protection strategy, including the TISN. The 2004 budget funding was designed to assist the telecommunications (including Internet Service Providers (ISPs), broadcasting and postal industries in improving the protection of Australia's communications infrastructure through improved information sharing and cooperation.

Funding in this budget also supported a number of groups⁹⁹ such as the Communications Sector Infrastructure Assurance Advisory Group (CSIAAG),¹⁰⁰ the Critical Infrastructure Advisory Council (CIAC) and the National Counter-Terrorism Committee and related groups such as the Information Technology Security Experts Advisory Group.¹⁰¹ The Australian Broadcasting Authority also received funding to assist in developing and maintaining effective communications mechanisms with broadcast operators for critical infrastructure protection coordination.

There were a number of significant new security-related initiatives in the Australian Government's Budget speech of 9 May 2006. The AFP received ongoing research and development capacity to counter the use of new and emerging technologies by terrorists and it established a single facility to manage the collection, monitoring, recording and evidence preparation of terrorism-related electronic surveillance material. Part of the significant allocation to the Australian Security Intelligence Organisation (ASIO) was designed to improve its IT networks to cope with the new demands and expanded operations.

Preventing identity theft also received attention in the 2006 budget. Both a national Document Verification Service and Identity Security Strike Teams were set up. The new service allows government agencies to check Australian passports, the Health Services access cards, Australian citizenship certificates, birth certificates and drivers' licences issued in Australia.

Funding was also provided for key law enforcement and security agencies to ensure a continued capability to intercept telecommunications; further funding was allocated to improve communications within government and with the public during a national crisis; and funding was provided to establish a National Emergency Call Centre capability that can be operational with one hour's notice of an emergency of national significance being declared by the government.

In 2007, the Australian Government revised its *E-Security National Agenda*,¹⁰² releasing the new version in July that year, and allocating a budget of A\$73.6 million over four years. IT security in critical infrastructure, individuals at home and companies are now considered to be highly interrelated. The government has recognised that poor PC security can lead to home computers being used in Distributed Denial of Service (DDoS) attacks on critical infrastructure and government agencies. The increase in the sophistication of e-security attacks has made it more difficult for anti-malware software companies to identify attacks and protect clients.

The Agenda created a single whole-of-government committee—the E-Security Policy and Coordination (ESPaC) Committee—to replace two former committees run by the Department of Communications, Information Technology and the Arts (DCITA) and the Attorney-General's Department. The Agenda has three priorities:

- reducing the e-security risk to Australia's national critical infrastructure;
- reducing the e-security risk to Australian Government information and communication systems; and
- enhancing the protection of home users and Small-to-Medium Enterprises (SMEs) from electronic attacks and fraud.

In respect of the first priority, the operations of GovCERT.au will be expanded significantly through the addition of 10 more staff members. It will also have responsibility for the Computer Network Vulnerability Assessment Program, which supports critical infrastructure owners and operators in checking network security.

Government will consider establishing a dedicated Centre to share security information between government and critical infrastructure organisations so as to minimise the impact of electronic attacks.

The AFP will expand its activities in combating on-line criminal activity, including enhancing its ability to detect, deter and investigate criminal threats

against critical infrastructure and for technology enabled crime such as on-line fraud.

In respect of the second priority, the Defence Signals Directorate (DSD) will receive increased funding to improve its technical advice on IT security issues for government agencies, managing e-security breaches for agencies, and analysis of malware to rapidly develop countermeasures. The Australian Government Information Management Office (AGIMO) has been commissioned to establish a single framework for the continued delivery of government services in the event of a disruption and/or failure of government-operated information, communication and technology systems.

In respect of the third priority, the Australian Communications and Media Authority (ACMA) will expand its work with Australian ISPs to help them identify compromised computers of their clients. The DCITA will continue to develop and expand its information to home and SME users, delivering information via www.staysmartonline.gov.au.

Notwithstanding these significant initiatives, more effort needs to be put into developing a reliable national indicators and warning architecture, and to improve national planning, programming and operations to build the capabilities needed to discern, deter and defend against the spectrum of cyber-threats that loom on the national security horizon. Changes in the nature of computers and networking could improve processing power, information storage, and bandwidth to the extent that artificial intelligence could be applied to cyber-warfare.¹⁰³

The specific requirements for developing a national indicators and warning architecture for infrastructure protection would be in terms of facilitating the following:¹⁰⁴

- an understanding of baseline infrastructure operations;
- the identification of indicators and precursors to an attack; and
- a surge capacity for detecting and analysing patterns of potential attacks.

Greater analytical expertise is needed within Defence and other government agencies to address the challenges related to information-based attacks. Rapid attribution of cyber-events is critical to mitigating attacks and deterring future ones. This means mature forensic capabilities are needed to support the attribution and the necessary legal regime to allow for rapid apprehension and prosecution. International deficiencies such as uniform laws that criminalise cyber-attacks and protocols for enforcing laws also need to be addressed.¹⁰⁵

Furthermore, all federal departments and agencies should be tasked with developing and submitting plans for protecting the physical and cyber-critical infrastructure and key resources that they own or operate. The plans should

address identification, prioritisation, protection, and contingency planning, including the recovery and reconstitution of essential capabilities.¹⁰⁶

Securing the Defence enterprise

From the discussion thus far, it is obvious that as Defence, like other enterprises, reaches out with its networks and is accessed by ever-growing numbers of friends, partners and adversaries, the risk of misuse, theft or sabotage increases. A suitable framework for addressing the vulnerabilities outlined in this chapter, and for securing the Defence enterprise, might be in terms of four integrated layers of activity—policy, operations, systems, and technical measures.¹⁰⁷

In policy terms, the ADF would need to address such issues as the design, planning and implementation of communications and information systems, which is a collaborative activity between users and providers to achieve a negotiated service. Force protection consequences should be more important than information access, which means that information might have to be restricted or even withheld from a user who has a high probability of capture or compromise. Active information governance measures such as responsibility, authority, procedures, contingency arrangements, reporting and standards should apply across the network.

In operations terms, the ADF would need to address connectivity and interoperability associated with joint force operations as well as combined force operations. In the former, all force elements would need to be connected at the lowest practicable organisational levels (e.g. infantry patrol to close air support aircraft). In the latter, connectivity might be between components and selected force elements (e.g. ADF land component commander to US amphibious task group). Finally, connectivity to Defence finance, logistics and personnel systems and to the systems of other agencies is required by deployed forces.

Systems integration and interoperability will minimise duplication and single points of failure. Cryptographic security, security against computer network attack, and personnel and infrastructure security arrangements should all be provided to the lowest level of connectivity. Robust system redundancy should be provided with appropriate levels of survivability and recovery, and preventive security measures should be offered through enhanced deterrence, detection, containment and response services.

In technical terms, a number of possible initiatives present themselves. First, IT systems (including communications and cryptographic) standards, configuration and protocols should be made compatible with national and combined requirements. Second, dynamic system security can be achieved through appropriate cryptographic, firewall, and virus protection, while dynamic system survivability can be achieved through appropriate routing, standby and duplicate equipment and services. Third, coalition IT and communications

standards should be compatible with commercial requirements. Fourth, classification, storage, release and distribution arrangements should be made that also include training, processes, procedures and responsibilities.

Other technical matters such as security architectures, secure identities and access, secure workforce, secure content management and secure web services also need to be addressed. These are covered in more detail below.¹⁰⁸

Integrated security architectures need to cover directory services, Public Key Infrastructure (PKI), and privilege management infrastructure, as well as digital signatures, authentication, access control, network security, workstation and Personal Digital Assistant (PDA) security, application security, and monitoring, IDS and incident response systems.

Identity and access management needs to cover all aspects of authentication, authorisation and entitlement. Access should be granted only for authorised users, and those users should access only that information they need to access.

Increasingly, workers will be more mobile and their access will need to be secured. Similarly, portals and email systems add to overall vulnerability, which in turn demands greater security vigilance. While web services provide real-time integration of business services from multiple sources, they also add even further to network vulnerability.

As part of this framework, Defence also needs a strong risk assessment methodology (covering attack and penetration testing, and emergency response measures), solid infrastructure security (by designing secure networks, perimeter security controls, multi-layered anti-virus architectures, secure wireless networks and remote access points, and system hardening), business continuity and the ability to recover from shocks and disruptions. Just as importantly, any enterprise with which Defence interacts electronically needs to have in place these security features.

Trusted information infrastructure

One way of addressing trusted information infrastructure is to develop a data access and management system that incorporates enterprise security, identity management, IA and information dissemination management. At the technical level, this would mean data standardisation, encryption and PKI tagging, and a protected data fusion engine that could manage the secure authentication process.

As Philip Dean and Bruce Talbot¹⁰⁹ suggest, such a system would provide a secure place to post classified information that would be accessible from networks of various classifications, all within a securely managed workflow that would ensure that trust could be managed, assured and controlled.

COTS software would be sufficient for providing Multi-Level Identity Management and Secure Service Provisioning. These two concepts would need

to be developed in tandem to ensure that security could be delivered through a layered approach that also manages identification, security clearance and access rights of both providers and users of the information. Location, information access and physical protection would be afforded by:

- providing a posting area for information that could be fully managed and secured and that could only be accessed by authorised users;
- offering compartmented storage within that posting area as necessary; and
- tagging devices such as PCs to ensure that they meet device constraints related to the specified information.

A data standardisation regime would be needed to ensure data that had been posted could be received by all authorised devices. Additionally, a management standardisation regime would be needed so that all interactions could be managed, such as the posting of documents, the identities of information providers and users, and the flow of information (based on policies, rules and identity).

Just as intelligence, command and control, and corporate information systems cry out for multiple layers of security to improve information sharing and collaboration and to reduce costs, so too do the interoperability requirements within the battlespace. Specifically, mission control systems such as fire-control systems on naval surface combatants and the multi-function displays in combat aircraft will need to be linked to ground forces in future in order to deliver integrated joint fires.¹¹⁰

While the foregoing is aimed squarely at Defence, the same issues pertain to a whole-of-nation perspective to securing Government agencies and ensuring a networked trusted information infrastructure.

Addressing the national requirement

Australia is confronted with a dynamic strategic environment that is continuously evolving. In meeting the exigencies of that environment, Australia will rely increasingly on the power it derives from networked government agencies and the processes for whole-of-government approaches to threats and problems. These exigencies will arise with little notice, impacting on national interests at home and overseas, and may originate from home soil as much as from another country.

As Australia finds itself engaged in persistent operations, where traditional distinctions blur between peace and war, combatants and non-combatants, and foreign and domestic activities, it will need to be perpetually reassessing any strategic gaps both in its preparedness to act and its actual performance on the day.¹¹¹ Accordingly, Australia needs the ability to focus, shape, and guide national effort across its networks. That national effort can no longer be permitted to be fragmented in its organisation and disjointed in its application.¹¹² Any

national effort must incorporate an offensive dimension as well as a defensive one, as well as preventive and responsive policies.¹¹³

From a military perspective, we are clearly moving into the fourth generation of warfare, a generation we might term 'net-war'. The first generation involved massed manpower, the second massed firepower, and the third manoeuvre. Net-war will be characterised by antagonists who will fight in the

political, economic, social and military arenas and communicate their messages through a combination of networks and mass media. This generation is likely to be based more on ideas rather than military technology; this is a crucial point. Warfare will not be the relatively clear-cut, high technology 'stately dance' of conventional war but rather extremely complex, mainly low-intensity conflicts. In these conflicts it will be hard to differentiate between war and peace, military operations and crimes, front and rear areas, combatants and non-combatants. Fighting will involve an amalgam of military tactics from all four generations and the concepts of 'victory' and 'defeat' will probably cease to exist.¹¹⁴

When these pressures are combined with where the ADF is moving with respect to NCW, there are compelling reasons to oversee developments from a single organisational perspective. A Net-war or Cyber-warfare Centre would provide just this—ensuring a joined-up national effort that incorporated offensive, defensive, preventive and responsive strategies, policies and actions while supporting the development and protection of robust networks that underpin the ADF's NCW capability. Such a Centre would be responsible for all aspects of operational planning, support and training, as well as research and capability development not only for the ADF but across national security agencies as a whole. Moreover, the Centre would have a key role in supporting Australia as network complexity and national, allied and coalition Internet-working increase in the years ahead.

Conclusion

Information is the lifeblood of the ADF's future networked force and, as such, it must be protected. The quest for information superiority to underpin network-centric operations in future will introduce operational vulnerabilities. The challenge is to identify these vulnerabilities and develop a framework to address them (in policy, operations, systems, and technical terms). Information sharing is crucial for networked, dispersed forces, but as these forces reach back into their enterprise systems and across into others, the issue of privacy looms large and must be managed through sensible architectures.

The security of information and the underpinning technology is compounded by the threat of cyber-attack, which demands a sophisticated protection system

for monitoring the information infrastructure, issuing alerts, and controlling responses as necessary. It would seem timely for national planning, programming and operations to build the capabilities needed to discern, deter and defend against the spectrum of cyber-threats that loom on the national security horizon.

Reliance on information does not just introduce vulnerabilities in the ADF and in its enterprise systems; it also introduces vulnerabilities in all critical information infrastructure on which Australia relies. Defence must have in place robust information security mechanisms across its networks, and it must also ensure that similar security mechanisms exist in other enterprises with which it seeks connectivity.

A trusted information infrastructure is key to supporting Information Superiority and Support (IS&S), which in turn, is key to a networked ADF. That Trusted Information Infrastructure involves much more than just the ADF's networks, and must address enterprise security, identity management, IA, and the management of dissemination of the information. And it applies as much to all Australian Government agencies as it does to Defence.

As network complexity and national and coalition Internet-working increase in the years ahead, there will be pressure on the Australian Government to ensure a joined-up national effort that incorporates both offensive and defensive policies and actions through some form of a Cyber-warfare Centre. Defence could take the initiative now and set up such a Centre to support the development and protection of its robust networks needed to underpin its NCW capability.

ENDNOTES

¹ I thank my colleague Brigadier Steve Ayling for his assistance in clarifying some of this thinking in 2004 and 2005.

² My thanks to Steve Ayling for his informed discussions on helping me identify these vulnerabilities.

³ John T. Sabo, *Addressing a Critical Aspect of Homeland Security: Managing Security and Privacy in Information Sharing Systems*, Computer Associates White Paper, January 2004, available at <http://www.ehcca.com/presentations/privacyfutures1/4_01_2.pdf>, accessed 4 April 2008, p. 2.

⁴ Sabo, *Addressing a Critical Aspect of Homeland Security: Managing Security and Privacy in Information Sharing Systems*, p. 2.

⁵ Sabo, *Addressing a Critical Aspect of Homeland Security: Managing Security and Privacy in Information Sharing Systems*, p. 2.

⁶ Sabo, *Addressing a Critical Aspect of Homeland Security: Managing Security and Privacy in Information Sharing Systems*, p. 2.

⁷ Sabo, *Addressing a Critical Aspect of Homeland Security: Managing Security and Privacy in Information Sharing Systems*, p. 3.

⁸ Sabo, *Addressing a Critical Aspect of Homeland Security: Managing Security and Privacy in Information Sharing Systems*, pp. 4–5.

⁹ Sabo, *Addressing a Critical Aspect of Homeland Security: Managing Security and Privacy in Information Sharing Systems*, p. 5.

¹⁰ Sabo, *Addressing a Critical Aspect of Homeland Security: Managing Security and Privacy in Information Sharing Systems*, p. 6.

¹¹ Sabo, *Addressing a Critical Aspect of Homeland Security: Managing Security and Privacy in Information Sharing Systems*, p. 6.

- ¹² The Federal Privacy Commissioner Malcolm Crompton completed his five-year term at the Commission on 19 April 2004. Just prior to his departure, he delivered a keynote farewell address entitled 'Proof of ID Required? Getting Identity Management Right' in Sydney to the Australian IT Security Forum on 30 March 2004, available at <http://www.privacy.gov.au/news/speeches/sp1_04p.pdf>, accessed 3 March 2008.
- ¹³ Crompton, 'Proof of ID Required? Getting Identity Management Right'.
- ¹⁴ Crompton, 'Proof of ID Required? Getting Identity Management Right'.
- ¹⁵ See 'Privacy exposed', *Sydney Morning Herald*, 19 February 2004, available at <<http://smh.com.au/articles/2004/02/18/1077072702295.html>>, accessed 3 March 2008.
- ¹⁶ 'Privacy exposed', *Sydney Morning Herald*, 19 February 2004.
- ¹⁷ 'Privacy exposed', *Sydney Morning Herald*, 19 February 2004.
- ¹⁸ AusCERT is based at Queensland University and is a non-profit computer security organisation.
- ¹⁹ 'Privacy exposed', *Sydney Morning Herald*, 19 February 2004.
- ²⁰ Thomas Homer-Dixon, 'The Rise of Complex Terrorism', *Foreign Policy*, Issue No. 128, January//February 2002, pp. 52–62.
- ²¹ Colonel Ashley was the Chief of Plans, Policy and Resources Division in the Communications and Information Directorate of Headquarters Pacific Air Forces, Hickham Air Force Base, Hawaii.
- ²² Colonel Bradley K. Ashley, US Air Force, 'The United States is Vulnerable to Cyberterrorism', *SIGNAL*, March 2004, p. 61.
- ²³ Ashley, 'The United States is Vulnerable to Cyberterrorism', *SIGNAL*, p. 61.
- ²⁴ Ashley, 'The United States is Vulnerable to Cyberterrorism', *SIGNAL*, pp. 62–63.
- ²⁵ Heinrich de Nysschen, 'Homeland Security', *Image & Data Manager*, May/June 2005, p. 36.
- ²⁶ US Government Accountability Office (GAO), *CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO-07-705, Report to Congressional Requesters, Washington, DC, June 2007, available at <<http://www.gao.gov/new.items/d07705.pdf>>, accessed 4 March 2008.
- ²⁷ Homer-Dixon, 'The Rise of Complex Terrorism', p. 2.
- ²⁸ Homer-Dixon, 'The Rise of Complex Terrorism', p. 3.
- ²⁹ Homer-Dixon, 'The Rise of Complex Terrorism', pp. 3–4.
- ³⁰ Homer-Dixon, 'The Rise of Complex Terrorism', p. 4.
- ³¹ Homer-Dixon, 'The Rise of Complex Terrorism', pp. 5–6.
- ³² Homer-Dixon, 'The Rise of Complex Terrorism', p. 6.
- ³³ 'Fighting the worms of mass destruction', *Economist*, 27 November 2003, available at <http://www.economist.com/science/displayStory.cfm?story_id=2246018> and on the Computer Crime Center website at <http://www.crime-research.org/library/Analytic_nov1.html>, 28 November 2003, accessed 3 March 2008.
- ³⁴ Ashley, 'The United States is Vulnerable to Cyberterrorism', *SIGNAL*, p. 64.
- ³⁵ Todd Datz, 'Out of Control', *CSO*, vol. 2, no. 1, 2005, p. 28.
- ³⁶ Datz, 'Out of Control', *CSO*, p. 30.
- ³⁷ Datz, 'Out of Control', *CSO*, p. 32.
- ³⁸ Jim Saxton, opening statement before the House Armed Services Committee on Terrorism, Unconventional Threats and Capabilities; hearing on 'Cyber Terrorism: The New Asymmetric Threat', 24 July 2003, available at <<http://www.iwar.org.uk/cip/resources/status-of-dod-ia/03-07-24saxton.htm>>, accessed 3 March 2008.
- ³⁹ Saxton, opening statement at hearing on 'Cyber Terrorism: The New Asymmetric Threat'.
- ⁴⁰ Eugene. H. Spafford, testimony before the House Armed Services Committee on Terrorism, Unconventional Threats and Capabilities; hearing on 'Cyber Terrorism: The New Asymmetric Threat', 24 July 2003, available at <<http://www.iwar.org.uk/cip/resources/status-of-dod-ia/03-07-24spafford.pdf>>, accessed 3 March 2008.
- ⁴¹ Spafford, testimony at hearing on 'Cyber Terrorism: The New Asymmetric Threat'.
- ⁴² This is referred to as competing 'in Internet time'.
- ⁴³ Spafford, testimony at hearing on 'Cyber Terrorism: The New Asymmetric Threat'.
- ⁴⁴ Spafford, testimony at hearing on 'Cyber Terrorism: The New Asymmetric Threat'.
- ⁴⁵ Spafford, testimony at hearing on 'Cyber Terrorism: The New Asymmetric Threat'.

- ⁴⁶ Robert F. Lentz, testimony before the House Armed Services Committee on Terrorism, Unconventional Threats and Capabilities; hearing on 'Cyber Terrorism: The New Asymmetric Threat', 24 July 2003, available at <<http://www.iwar.org.uk/cip/resources/status-of-dod-ia/03-07-24lentz.htm>>, accessed 3 March 2008.
- ⁴⁷ Lentz, testimony at hearing on 'Cyber Terrorism: The New Asymmetric Threat'.
- ⁴⁸ Lentz, testimony at hearing on 'Cyber Terrorism: The New Asymmetric Threat'.
- ⁴⁹ Lentz, testimony at hearing on 'Cyber Terrorism: The New Asymmetric Threat'.
- ⁵⁰ Lentz, testimony at hearing on 'Cyber Terrorism: The New Asymmetric Threat'.
- ⁵¹ See Antone Gonsalves, 'Gartner: Dependence On Internet Boosts Risks of Cyberwar', *InformationWeek*, 15 January 2004, wherein he cites a report from David Fraley of Gartner which noted that nations would be able to carry out cyber-warfare by 2005, available at <<http://www.informationweek.com/story/showArticle.jhtml?articleID=17301666>>, accessed 3 March 2008.
- ⁵² Antone Gonsalves, 'Gartner: Dependence On Internet Boosts Risks of Cyberwar', *InformationWeek*.
- ⁵³ Antone Gonsalves, 'Gartner: Dependence On Internet Boosts Risks of Cyberwar', *InformationWeek*.
- ⁵⁴ Drew Clark, 'Computer security officials discount chances of "digital Pearl Harbor"', *National Journal's Technology Daily*, 3 June 2003, available at <<http://www.govexec.com/dailyfed/0603/060303td2.htm>>, accessed 3 March 2008.
- ⁵⁵ Clark, 'Computer security officials discount chances of "digital Pearl Harbor"'.
⁵⁶ 'Behind the Firewall—The Insider Threat', 15 April 2003, ARTICLE ID: 2122. See <<http://enterprisecurity.symantec.com/article.cfm?articleid=2122&PID=14615847&EID=389>>.
- ⁵⁷ 'Behind the Firewall—The Insider Threat'.
- ⁵⁸ 'Behind the Firewall—The Insider Threat'.
- ⁵⁹ Clark, 'Computer security officials discount chances of "digital Pearl Harbor"'. I must also thank Richard Hunter for including me in the Gartner Research work of 2003.
- ⁶⁰ David McGlinchey, 'Agencies, Congress urged to upgrade computer security planning', GovExec.com, Washington DC, 17 March 2004, available at <<http://www.govexec.com/dailyfed/0304/031704d1.htm>>, accessed 3 March 2008.
- ⁶¹ 'Fighting the worms of mass destruction'.
- ⁶² 'Fighting the worms of mass destruction'.
- ⁶³ 'Fighting the worms of mass destruction'.
- ⁶⁴ International Institute for Strategic Studies, *International Institute for Strategic Studies (IISS) Strategic Survey 2003/4*, Oxford University Press, Oxford, May 2004, p. 51.
- ⁶⁵ 'Fighting the worms of mass destruction'.
- ⁶⁶ 'Fighting the worms of mass destruction'. Gerhard Eschelbeck of Qualys is cited in the article.
- ⁶⁷ See Chris Jenkins, 'Internet Terrorism Fears as Virus Hits', *Australian*, 28 January 2004, p. 3.
- ⁶⁸ Jenkins, 'Internet Terrorism Fears as Virus Hits', *Australian*, 28 January 2004, p. 3.
- ⁶⁹ Jenkins, 'Internet Terrorism Fears as Virus Hits', *Australian*, 28 January 2004, p. 3.
- ⁷⁰ International Institute for Strategic Studies, *IISS Strategic Survey 2003/4*, p. 62.
- ⁷¹ 'Cert/CC Statistics 1998-2005', Carnegie Mellon Software Engineering Institute, undated.
- ⁷² 'Fighting the worms of mass destruction', citing Brightmail, the world's market leader in filtering e-mails.
- ⁷³ 'Fighting the worms of mass destruction', citing Brightmail.
- ⁷⁴ 'Fighting the worms of mass destruction', citing Brightmail.
- ⁷⁵ 'Fighting the worms of mass destruction'. Alan Nugent, the chief technologist at the software company Novell, is cited in the article.
- ⁷⁶ 'Fighting the worms of mass destruction', citing Alan Nugent.
- ⁷⁷ Edward Waltz, *Information Warfare: Principles and Operations*, Artech House Publications, Boston and London, 1998, p. 157.
- ⁷⁸ Waltz, *Information Warfare: Principles and Operations*, p. 157.
- ⁷⁹ Waltz, *Information Warfare: Principles and Operations*, p. 157.
- ⁸⁰ Waltz, *Information Warfare: Principles and Operations*, p. 160.

- ⁸¹ Frank J. Cilluffo and J. Paul Nicholas, 'Cyberstrategy 2.0', *Journal of International Security Affairs*, No. 10, Spring 2006, available at <http://www.securityaffairs.org/issues/2006/10/cilluffo_nicholas.php>, accessed 3 March 2008.
- ⁸² Department of the Prime Minister and Cabinet, *Protecting Australia Against Terrorism 2006: Australia's National Counter-Terrorism Policy and Arrangements*, Department of the Prime Minister and Cabinet, Canberra, 2006, p. 60, available at <http://cipp.gmu.edu/archive/Australia_ProtectAU_Terrorism_2006.pdf>, accessed 3 March 2008.
- ⁸³ Department of the Prime Minister and Cabinet, *Protecting Australia Against Terrorism 2006*, p. 61.
- ⁸⁴ Department of the Prime Minister and Cabinet, *Protecting Australia Against Terrorism 2006*, p. 61.
- ⁸⁵ Department of the Prime Minister and Cabinet, *Protecting Australia Against Terrorism 2006*, p. 62.
- ⁸⁶ Heinrich de Nysschen, 'Homeland Security', p. 37.
- ⁸⁷ Paul Kurtz, the executive director of the Cyber Security Industry Alliance, was quoted in Heather Greenfield, 'Industry Officials Sketch Priorities for DHS Cyber Czar', *National Journal's Technology Daily*, 2 October 2006, available at <<http://www.govexec.com/dailyfed/1006/100206tdpml1.htm>>, accessed 3 March 2008.
- ⁸⁸ Heather Greenfield, 'Industry Officials Sketch Priorities for DHS Cyber Czar'. The article cites Paul Kurtz as quoting this figure.
- ⁸⁹ Department of the Prime Minister and Cabinet, *Protecting Australia Against Terrorism 2006*, p. 45.
- ⁹⁰ Parliament House News Release by the Attorney-General, The Hon Philip Ruddock MP, *Protecting Australia's Critical Infrastructure*, 11 May 2004, available at <[http://ag.gov.au/www/agd/rwpattach.nsf/VAP/\(CFD7369FCAE9B8F32F341DBE097801FF\)~MR03CriticalInfrastructure07May04.doc/\\$file/MR03CriticalInfrastructure07May04.doc](http://ag.gov.au/www/agd/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~MR03CriticalInfrastructure07May04.doc/$file/MR03CriticalInfrastructure07May04.doc)>, accessed 3 March 2008.
- ⁹¹ Department of the Prime Minister and Cabinet, *Protecting Australia Against Terrorism 2006*, pp. 45–46.
- ⁹² Department of the Prime Minister and Cabinet, *Protecting Australia Against Terrorism 2006*, p. 46.
- ⁹³ Department of the Prime Minister and Cabinet, *Protecting Australia Against Terrorism 2006*, p. 45.
- ⁹⁴ See Mark Davis, 'Canberra, CEOs extend forum on Terrorism', *Australian Financial Review*, 24 June 2004, p. 3.
- ⁹⁵ Davis, 'Canberra, CEOs extend forum on Terrorism', *Australian Financial Review*, p. 3.
- ⁹⁶ The origin of TISN lies with the announcement by the Prime Minister in November 2001 of his desire to form a Business–Government Task Force on Critical Infrastructure. The Task Force, which met in March 2002, recommended the establishment of an information-sharing network which led to the Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection (CIP). In December 2002, the Council of Australian Governments (COAG) endorsed the development by the National Counter-Terrorism Committee (NCTC) of guidelines for critical infrastructure protection, including the establishment of criteria to identify critical infrastructure and the outlining of appropriate security measures. The TISN was launched at the National Summit on Critical Infrastructure Protection on 2 April 2003. For more details on TISN, see The Department of the Prime Minister and Cabinet, *Protecting Australia Against Terrorism 2006*, p. 47.
- ⁹⁷ Department of the Prime Minister and Cabinet, *Protecting Australia Against Terrorism 2006*, p. 61.
- ⁹⁸ Department of the Prime Minister and Cabinet, *Protecting Australia Against Terrorism 2006*, p. 46.
- ⁹⁹ Ruddock, *Protecting Australia's Critical Infrastructure*.
- ¹⁰⁰ CSIAAG brings together owners and operators of Australia's communications sector infrastructure in a trusted forum.
- ¹⁰¹ This group advises CIAC on cyber-aspects of critical infrastructure protection.
- ¹⁰² See Australian Homeland Security Research Centre, *National Security Briefing Notes—Advancing domestic and national security practice: 2007 E-Security National Agenda*, July 2007, available at http://www.homelandsecurity.org.au/files/2007_e-security_agenda.pdf>, accessed 3 March 2008.
- ¹⁰³ See The White House, *The National Strategy to Secure Cyberspace*, US White House, Office of the Press Secretary, February 2003, available at <http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf>, accessed 3 March 2008.
- ¹⁰⁴ These are listed as tasks for the Secretary of the US DHS in *Critical Infrastructure Identification, Prioritization, and Protection*, Homeland Security Presidential Directive No. 7, US White House, 17 December 2003, available at <<http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html>>, accessed 3 March 2008.

¹⁰⁵ Drawn from discussion in Cilluffo and Nicholas, 'Cyberstrategy 2.0', and the *US National Strategy to Secure Cyberspace*.

¹⁰⁶ Drawn from *Critical Infrastructure Identification, Prioritization, and Protection*, Homeland Security Presidential Directive No. 7.

¹⁰⁷ I acknowledge the contribution of my colleague Brigadier Steve Ayling for his thoughts on the framework.

¹⁰⁸ See also Accenture, *The Accenture Security Practice: Security and the High-Performance Business*, 2003, available at <<http://whitepapers.silicon.com/0,39024759,60086441p,00.htm>>, accessed 3 March 2008.

¹⁰⁹ I am indebted to my colleagues Philip Dean and Bruce Talbot for their assistance in clarifying my thinking of how a trusted information infrastructure could be developed.

¹¹⁰ For an insight into more effective joint fires for the future, see Alan Titheridge, Gary Waters, and Ross Babbage, *Firepower to Win: Australian Defence Force Joint Fires in 2020*, Kokoda Paper no. 5, The Kokoda Foundation, Canberra, October 2007.

¹¹¹ Donald Reed refers to this as the 'new strategic reality' in Donald J. Reed, 'Why Strategy Matters in the War on Terror', *Homeland Security Affairs*, vol. II, no. 3, October 2006, p. 5, available at <<http://www.hsaj.org/pages/volume2/issue3/pdfs/2.3.10.pdf>>, accessed 3 March 2008.

¹¹² Reed, 'Why Strategy Matters in the War on Terror', *Homeland Security Affairs*, p. 13. Reed sees this as the essence of strategy going forward.

¹¹³ National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, W.W. Norton & Company, Inc., New York, 2004, p. 363, available at <<http://www.9-11commission.gov/report/911Report.pdf>>, accessed 3 March 2008.

¹¹⁴ David Potts (ed.), *The Big Issue: Command and Combat in the Information Age*, Strategic and Combat Studies Institute Occasional Paper no. 45, CCRP Publication Series, February 2003, pp. 244–45, available at <http://www.dodccrp.org/files/Potts_Big_Issue.pdf>, accessed 3 March 2008.