

Chapter 3

Information Warfare—Attack and Defence

Gary Waters

Introduction

Information is used to create value and achieve a desired end-state or effect. Preventing this value from being realised, on the one hand, and protecting those systems that allow that value to be realised, on the other, are caught up in the notion of Information Warfare (IW). This chapter addresses these two aspects—the value of information and IW. It discusses the methods an adversary might use to attack Australia’s networks and other capabilities and what we should do to prevent that. Cyber-crime is the other side of the same coin—posing a threat to our networks. We need to determine just what constitutes our Critical Information Infrastructure (CII) in Australia and ensure we have adequate protection measures in place. These aspects are also canvassed.

The value of information

The objective for using information in business is to create capital value; across government, it is to deliver value to the public; and the objective in the military is to achieve a desired end-state or effect. Thus, information is used to create value and achieve a desired end-state or effect.

In a business sense, the value of Information Technology (IT) can be exploited by gaining leverage through process innovation, by applying data and information in one process to other processes, and by sharing networks or selling excess capacity.¹ This also applies to the fixed information infrastructure that supports the Australian Defence Organisation (ADO). Ed Waltz extends this thinking to the military operations dimension by arguing that leverage can be gained through the use of data-links to deliver real-time targeting information to weapons; intelligence could be applied to support the competitiveness of the economy; and coalition networks with appropriate security mechanisms can burden share.²

The real utility of information can be seen as a function of its accessibility and flexibility, as well as its reliability, together with the way in which it contributes to achieving a desired end-state or effect.

In traditional military thinking, information has tended to be viewed as battlefield intelligence and tactical attacks on enemy radar and telephone networks. That thinking should now be broadened to view information as a powerful lever that can alter an adversary's high-level decisions. Indeed, it becomes a strategic asset, in which opposing sides will try to shape the other's actions by manipulating the flow of intelligence and information.³

It was out of this thinking that *Command and Control Warfare* emerged in the early 1990s. David Ronfeldt and John Arquilla of RAND Corporation in Santa Monica took this further into the realms of cyber-war—turning the balance of information and knowledge in one's favour.⁴

In a strategic sense, the value of information boils down to the ability to 'acquire, process, distribute and protect information, while selectively denying or distributing it to adversaries and/or allies'.⁵ In other words, the real value comes from providing the right information to the right people at the right time in the right place and in the right form.

While information or knowledge superiority might win wars, it is also highly fragile—as Alvin and Heidi Toffler say, 'a small bit of the right information can provide an immense strategic or tactical advantage. The denial of a small bit of information can have catastrophic effects'.⁶ This leads to the notion of *information superiority*, which is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.⁷

Should an information attack be launched against the Australian Defence Force (ADF), it should be able to take defensive or offensive measures. A defensive response would generate alerts, increase the level of access restrictions, terminate vulnerable processes, or initiate other activities to mitigate potential damage on the ADF. An offensive response would support targeting and specific attack options that the ADF might wish to carry out.⁸

With many weapons increasingly coming to rely on information—such as smart munitions that use Global Positioning System (GPS) guidance—the ADF can expect information to become more directly relevant in warfare of the future. Similarly, a digitised force should be able to operate at a higher tempo than a non-digitised one through its improved ability to coordinate actions.⁹

Open source information

Outside the traditional military realm, the explosive growth of personal computers (PCs) and their linking via the Internet offers vast quantities of public information that is freely available. While the intelligence community is probably the most affected, all branches of government are impacted. Indeed, the ongoing extremist threat, other non-State threats, and the increasing need for whole-of-government

consideration of security issues should be sharpening the government's focus on the potential and indeed the strategic and tactical importance of open source information on the Internet.

Joseph Nye, a former head of the US National Intelligence Council in the 1990s stated:

Open source intelligence is the outer pieces of the jigsaw puzzle, without which one can neither begin nor complete the puzzle ... open source intelligence is the critical foundation for the all-source intelligence product, but it cannot ever replace the totality of the all-source effort.¹⁰

Within this context, the Australian Government needs to consider the value of open source information; the importance of the ever-increasing amount of information on the Internet; the utility of new analytic tools that can collect, sift, analyse, and disseminate this publicly available information; and, training issues relating to open source technology and techniques.¹¹

Open source information may be defined as that information which is publicly available and that anyone can lawfully obtain by request, purchase, or observation. However, the acquisition of such information must conform to any existing legal copyright requirements. Open source information can include:

- media such as newspapers, magazines, radio, television, and computer-based information;
- public data such as government reports, and official data such as budgets and demographics, hearings, legislative debates, press conferences, and speeches;
- information derived from professional and academic sources such as conferences, symposia, professional associations, academic papers, dissertations and theses, and experts;¹²
- commercial data such as commercial imagery; and
- grey literature such as trip reports, working papers, discussion papers, unofficial government documents, proceedings, preprints, research reports, studies, and market surveys.¹³

It can also include company proprietary, financially sensitive, legally protected, or personally damaging information that is unclassified.¹⁴ Increasingly, it also encompasses information derived from Internet blogs.

In 2004, the US Congress called for an open source centre that could collect, analyse, produce, and disseminate open-source intelligence. Congress argued that open source intelligence was a valuable source of information that had to be integrated into the intelligence cycle to ensure that US policy-makers were fully informed. Accordingly, the National Open Source Center (NOSC) was established on 1 November 2005, and placed under the management of the

Central Intelligence Agency (CIA). The NOSC's functions included 'collection, analysis and research, training, and IT management to facilitate government-wide access and use'. The intent now is to provide a centre of expertise for exploiting open-source information across whole-of-government. Indeed, the NOSC can be tasked by other agencies for specific research.¹⁵

For Australia, it will be important to ensure that open-source experts are available across all government agencies so as to also avoid unnecessary duplicative efforts. Thus, some form of Centre with the requisite expertise and capability to train open source experts in government agencies is needed now. Such a Centre could improve information sharing across agencies by using state-of-the-art IT, seeking to maximise connectivity throughout the Australian Government and eliminate incompatible formats and any duplicative effort. Individual agencies should still be able to maintain independent open-source databases, but they would have to be maintained in formats accessible to other agencies.

Commercial satellites offer a good supplement to imagery from government satellites. Indeed, today, anyone with access to the Internet can obtain high-quality overhead imagery. It would be important for an Australian Centre, therefore, to have links to the Defence Imagery and Geospatial Organisation (DIGO).

In short, there would seem to be real merit in establishing an Australian Open Source Agency outside the Intelligence Community, with the intent to provide open-source information to all elements of the Australian Government, including parliamentary committees. Increasingly, open-source information will become essential for all functions of government and will demand more concerted efforts to acquire and analyse the vast quantities of available information. This could be one of the functions of a Cyber-warfare Centre as described in the final chapter by Des Ball.

Information Warfare

In the end, information is an important enabler, which may at times be of great strategic value, but in essence this is usually because of other actions, effects, and end-states to which it contributes.

Some of the pro-information literature tends to argue that information dominance avoids the need to use force and that it leads to an ability to disrupt the adversary rather than destroy his forces. While there may be an element of truth in that, the use of force is not incompatible with achieving a superior information position, and disruption and destruction are not mutually exclusive.¹⁶

War will continue to be a dangerous and violent clash, while improved information will tend to facilitate a more economical use of force.¹⁷ Information

is not an end in itself.¹⁸ Rather, it is a means to an end, and increasingly nations will view that end as the achievement of an effect, whether it be diplomatic, military, economic, informational, societal, technological, or a combination of these instruments of national power.

Ed Waltz offers a basic model of warfare in terms of options for attack. He argues that one can launch a physical attack, engage in deception, carry out a psychological attack, or engage in an information attack.¹⁹ In each of these, information has a key role. The aim of these options is to destroy, to deceive or surprise, to disorient, and to severely dislocate (by affecting confidence in information through destruction, deception or disorientation).

The logical extension of all of this for the country that can master the information domain is to close the loop on Sun Tzu's observation that the acme of skill is to 'subdue the enemy without fighting'.²⁰ The US thought leader Dick Szafranski updated Sun Tzu's observation by arguing that the knowledge systems of an adversary should be the primary strategic target.²¹ This is not meant to imply that information is the only option for attack, but rather that its importance as a partner to the more traditional physical forms of attack has increased.

In a warfighting sense, sensor technologies have extended the engagement envelope; computers and communications technologies have led to an increase in the tempo of operations; and the integration of sensors into weapons has made them more precise and lethal. The real transformation, therefore, has not been in sensor, weapons or IT *per se*, but in shifting the focus from the physical dimension to the information dimension.

Waltz calls this the transition toward the dominant use of information and the targeting of information itself. He makes a neat distinction between IW, which emphasises the use of information as a weapon or target, and Information-based Warfare, which he describes as the use and exploitation of information for advantage—often in support of physical weapons and targets.²²

Martin Libicki contends that there are seven different types of IW that can be categorised by the nature of the operations they contain. These are:²³

- *Command and Control Warfare*, which is aimed at separating command from the forces by attacking command and control (C2) systems.
- *Intelligence-based Warfare*, which aims to support other forms of attack by collecting, exploiting and protecting information.
- *Electronic Warfare*, which attacks communications by concentrating on transfer (radio-electronics) and formats (cryptographic).
- *Psychological Warfare*, which attacks the human mind.
- *Hacker Warfare*, which ranges over the Global Information Infrastructure (GII).

- *Economic Information Warfare*, which aims to control an economy by controlling certain information.
- *Cyber Warfare*, which brings together abstract forms of terrorism, simulation and reality control.

Waltz differentiates *Command and Control Warfare* as attacks against the Defence Information Infrastructure (DII) and *Information Warfare* as attacks against the National Information Infrastructure (NII).²⁴

The key aspects that emerge from Waltz's analysis of this work are that three security-related attributes are needed from an information infrastructure—availability, integrity and confidentiality.²⁵ Availability encompasses information services (processes) as well as information itself (context). An adversary's objective in IW would be to disrupt (availability), corrupt (integrity) or exploit (confidentiality or privacy).

The ADF is developing new ways of accomplishing its missions by leveraging the power of information and applying network-centric concepts, made possible by rapidly advancing IT. Indeed, military leaders have always recognised the key contribution that information makes to victory in warfare. To that end, they have always sought to gain a decisive information advantage over their adversaries.

As David Alberts argues, in the Information Age militaries now need to understand

the complex relationships among information quality, knowledge, awareness, the degree to which information is shared, shared awareness, the nature of collaboration, and its effect on synchronisation, and turning this understanding into deployed military capability.²⁶

Technological advances in recent years have vastly increased the military's capability to collect, record, store, process, disseminate, and utilise information. However, the advances in the ability to process information simply have not kept pace with the ability to collect that information.

Technology is also bridging distances and providing the capability for individuals to be able to interact with each other in increasingly sophisticated ways, making it easier for individuals and organisations to share information, to collaborate on tasks, and to synchronise actions.

Thus, our increasing reliance on satellite technology and IT to mount joint and combined operations presents any adversary with an opportunity for an asymmetric advantage if our networks can be corrupted, damaged, or destroyed. Furthermore, our national reliance on IT networks and the increasing interconnectedness of all forms of national power mean that a strategic campaign

could be waged against both our military forces deployed in distant theatres and our domestic IT infrastructure.

How would an adversary attack us?

As a Center for Security Policy paper observed recently: ‘The increasing digitization of military operations, economic and financial infrastructure, as well as all modern communication networks carries with it a great risk’.²⁷ The combination of global connectivity, mobility of employees, and rapid technological change exposes Australia’s civilian information infrastructure to certain risks such as fraud, theft, industrial espionage and disruption to business continuity. Thus, the civilian IT systems of our nation and the ADF’s Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems are at great risk if they are not adequately defended.

What would a state-based adversary seek to do though? Such an adversary would seek to disrupt our decision-making process by interfering with our ability to obtain, process, transmit, and use information.²⁸ Furthermore, depending on the circumstances, that adversary may wish to impede our decision-making with the aim of delaying or even deterring conflict so that it is no longer on our terms. Once the use of military force becomes likely, the adversary would use IW to shape the battlespace in such a way that their likelihood of victory would be improved.

The adversary would support the training and operations of their military with civilian computer expertise and equipment, sourced from training and education establishments and IT industries in their country. The intention would be to integrate these civilians into regular military operations. Then these integrated IW capabilities would be directed primarily at the ADF.

One avenue of attack could be through computer viruses designed to attack our computer systems and networks. A virus such as Myfip could be used as it can be disguised and, once activated on poorly protected network systems, can compromise the entire network information system and steal any of the following file types:²⁹

- .pdf—Adobe Portable Document Format
- .doc—Microsoft Word Document
- .dwg—AutoCAD drawing
- .sch—CirCAD schematic
- .pcb—CirCAD circuit board layout
- .dwt—AutoCAD template
- .dwf—AutoCAD drawing
- .max—ORCAD layout
- .mdb—Microsoft database.

The network could lose its documents, plans, communications and databases, or it might simply have all of its proprietary information stolen and remain totally unaware.

The adversary would test our cyber-defences with low-level assaults and incursions, essentially conducting 'cyber-reconnaissance' by probing the computer networks of Australian Government agencies and private companies, seeking to identify weak points in the networks, understand how Australian leaders think, discover the communications patterns of Australian Government and private companies, and obtain valuable information stored throughout the networks.³⁰

An attack could be launched against ADF or other Government Department email systems through a Distributed Denial of Service (DDoS), where systems would be overwhelmed by 'botnets' that make a request for service from a single information resource. These botnets (that could number more than 100 000)³¹ would be extensive networks of computers used by the adversary to overload the response capability of our information systems.

The adversary will have been planning for several years to conduct a limited war by attacking our C4ISR systems, as well as our national economic system, possibly using a terrorist organisation to detonate an electro-magnetic pulse weapon above Australia, at the appropriate time. The adversary would also have developed its IW doctrine along the following lines:

Information Warfare involves combat operations in a high-tech battlefield environment in which both sides use information-technology means, equipment, or systems in a rivalry over the power to obtain, control and use information. Information Warfare is combat aimed at seizing the battlefield initiative; with digitized units as its essential combat force; the seizure, control, and use of information as its main substance; and all sorts of information weaponry [smart weapons] and systems as its major means.³²

The adversary would carry out its attacks with non-attributable asymmetric techniques that focus upon information suppression, destruction and alteration, which would be consistent with its doctrine of exploiting the inherent vulnerabilities of information systems. Furthermore, its doctrine would anticipate using highly-trained civilian computer experts as its 'soldiers' in an information war rather than committing large numbers of troops to overrun the ADF. In this, it would seek to deter and even blackmail Australia through the dominance it achieves in possessing information.

As part of the adversary's attempt to corrupt our networks, they would also employ special equipment (both airborne and covertly-emplaced local systems) to intercept the *pro forma* data codes used in our computer-to-computer data

exchanges. The *pro forma* include the dial tones of protocols and link-ups that determine the signaling method (such as data transfer multiplexers and private branch exchanges) and the paths and speeds of data transmission.

Buoyed with success against our IT networks, the adversary would also attack our air defences by jamming our radar stations, deceiving the processing, and reconfiguring the displays so that certain azimuths and aircraft types cannot be ‘seen’. Adversary aircraft, both manned and unmanned, effectively would have unrestricted access over Australian airspace.

To prevent our air response capability being mobilised, the adversary would inject wireless application protocols (WAPs) and firewall-penetrating software into the avionics of our aircraft as they become airborne, allowing them to be effectively ‘hijacked’ by that adversary’s cyber-specialists with foreknowledge of the details of the hardware and software used in our avionics systems. High-power lasers and radio frequency (RF) weapons would be used to burn out the avionics in any of our aircraft that were not susceptible to ‘hijacking’.³³

Similarly, our maritime response capability would be immobilised by electronic warfare (EW) attacks against the radar systems on our ships and the confounding of ships’ communications systems. The radars and other electronic systems aboard every vessel in the fleet would have been carefully studied beforehand—the antenna designs and the signal frequencies, strengths and pulse characteristics—and electronic countermeasures (ECM) equipment and application tactics calibrated to effectively jam or deceive each system. Satellite communications (SATCOM) links with the Australian fleet would be in the adversary’s hands, following the ‘hijacking’ of all of the transponders on our communications satellites.³⁴

Critical elements of our command, control and communications system would be destroyed or incapacitated by RF weapons, carried by Unmanned Aerial Vehicles (UAVs) and cruise missiles on one-shot, one-way missions. Ultra-wide band (UWB) weapons, which generate RF radiation over a wide frequency spectrum (nominally from about 100 MHz to more than 1 GHz), but with little directivity, would be used to incapacitate electronic components across broad categories of telecommunications and computerised infrastructure. High-power microwave (HPM) weapons, which generate an RF beam at a very narrow frequency band (in the 100 MHz to 100 GHz range) would be used against our hardened C2 centres, using both ‘front door’ and ‘back door’ entry points. In the former case, the RF weapons designers would have used foreknowledge of the antenna systems at the command centres to produce an in-band waveform, with the right frequency and the right modulation to couple with the antennas, allowing the intense energy to burn out components connected to the antennas.³⁵

Residual command, control, communications and intelligence (C3I) systems, such as delegated command authorities, fibre-optic cables, rejuvenated sensor

systems and makeshift broadcast stations would be dealt with by Special Forces—landed by submarines, and guided by UAVs.³⁶

China's cyber-attack capability

As one example of the cyber-attack capability of nation-states, a brief discussion on China is offered here. On 9 December 2007, the *New York Times* reported that in a series of sophisticated attempts against the US nuclear weapons laboratory at Oak Ridge, Tennessee, Chinese hackers had removed data.³⁷ In March 2007, US Strategic Command Chief General James E. Cartwright told Congress that the United States was under widespread attack in cyber-space.³⁸ During 2007 and 2008, 12 986 direct assaults on federal agencies and more than 80 000 attempted attacks on Department of Defense computer network systems were reported. Some of these attacks reduced the US military's operational capabilities.³⁹

An American cyber-security company that focuses on centralised activity emanating from China reported that attacks from China had almost tripled in the three months before December 2007.⁴⁰ In December 2007, Jonathan Evans, the chief of the United Kingdom's domestic counter-intelligence agency MI5, warned a number of accountants, legal firms, and chief executives and security chiefs at banks that they were being spied on electronically by Chinese state organisations. Evans noted that a number of British companies, with Rolls Royce being one example, had discovered that viruses of Chinese Government origin were uploading vast quantities of industrial secrets to Internet servers in China.⁴¹

Earlier, in October, one of Germany's top internal security officers, Hans Elmar Remberg, told a Berlin conference on industrial espionage that his country was involved in a cyber-war with the Chinese, arguing that he believed Chinese interests were behind the recent digital attacks. One month earlier, in September, the French Secretary General for National Defence, François Delon, argued that he had proof that there was involvement from China in cyber-attacks on France, but could not conclusively say it was the Chinese Government.⁴²

The German Government too has been subjected to cyber-attacks, with German Chancellor, Angela Merkel, being informed in August 2007 that three computer networks in her own office had been penetrated by Chinese intelligence services. A few days later, she confronted the visiting Chinese premier directly about the attacks. Premier Wen Jiabao was shocked and promised that his government would get to the bottom of the matter. Interestingly, he then asked for detailed information from Germany's counter-intelligence agencies to help China's security police find the culprit.⁴³

Notwithstanding the wide-ranging nature of such attacks, by far the target attacked most intensely by the Chinese is the US military, closely followed by the State Department, the Commerce Department, and the US Department of

Homeland Security. Computer networks in sensitive US sectors relating to commerce, academia, industry, finance, and energy are also being targeted. Indeed, one US cyber-security expert told a group of federal managers that ‘the Chinese are in half of your agencies’ systems’.⁴⁴

While the United States and other governments appear reticent to reveal the extent of the vulnerabilities of their databases to Chinese penetration, the information available does tend to indicate how widespread Chinese cyber-attacks have become. Cyber-warfare units in the Chinese People’s Liberation Army (PLA) have already penetrated the Pentagon’s Non-classified Internet Protocol Router Network (NIPRNet) and have designed software to disable it in time of conflict or confrontation. Major General William Lord, Director of Information, Services, and Integration in the US Air Force’s Office of Warfighting Integration, admits that China has downloaded data from the NIPRNet already, and that China now poses a nation-state threat.⁴⁵

Richard Lawless, Deputy Undersecretary of Defense for Asia-Pacific Affairs, told a Congressional panel on 13 June 2007 that the Chinese are ‘leveraging information technology expertise available in China’s booming economy to make significant strides in cyber-warfare’. He noted the Chinese military’s determination to dominate, to a certain degree, the capabilities of the Internet, and that this capacity provides them with a growing and very impressive ability to wage cyber-warfare.⁴⁶

Lawless argued that the Chinese have developed a very sophisticated, broadly-based capability to attack and degrade US computer and Internet systems. He noted that the Chinese well-appreciated how to access computers and disrupt networks, particularly by penetrating the networks to glean protected information and by carrying out computer network attacks, which would allow them to shut down critical systems in times of emergency. Lawless argues that the capability is already there; it is being broadened; and it represents a major component of Chinese asymmetric warfare capability.⁴⁷ It is also believed that PLA cyber-warfare units have access to source codes for America’s ubiquitous office software, giving them a skeleton key to every networked government, military, business, and private computer in the United States.

As China’s cyber-attack capability becomes clearer, the US Government will need to acknowledge the vulnerability of America’s national security information infrastructure as well as its commercial, financial and energy information networks and make the requisite changes. And, via their computer network operations, China’s clandestine intelligence collection would seem to be the foremost intelligence threat to America’s science and technology secrets.⁴⁸ Clearly, this applies equally to Australia.

What should we do?

As our computer networks proliferate and dependencies on them increase, their protection against cyber-attacks needs far more attention than previously. The knowledge and abilities of hackers have become much more sophisticated and are outstripping methods that detect, identify and alert users to network attacks. These current cyber-defence methods tend to rely on data mining approaches that are useful for simple attacks but not for the more complex or coordinated attacks of recent times. Cyber-space security urgently requires next-generation network management and Intrusion Detection Systems (IDS).

One method of dealing with the emergent challenges is to address network security from a system control and decision perspective that would combine short-term sensor information and long-term knowledge databases to provide improved decision-support systems as part of improved C2. In this respect, information fusion is needed to provide the foundation for a decision and control framework that can detect and predict multi-stage stealthy cyber-attacks.⁴⁹

The problem with our networks

Large networks today contain a multitude of hardware and software packages and are connected in multiple ways. Inevitably, the complexity of these networks introduces security problems that evade detection by network administrators, who tend to focus on isolated and discrete vulnerabilities.

Cyber-attacks traditionally have been one-dimensional—Denial of Service (DS) attacks, insertion of computer viruses or worms, and unauthorised intrusions (referred to as ‘hacking’). These attacks were mainly launched against websites, mail servers or client machines. For the future, cyber-threats will be more diversified and take the form of multi-stage and multi-dimensional attacks that utilise and target a variety of attack tools and technologies. For example, the latest generation of worms uses a variety of different exploits, propagation methods, and payloads to inflict damage. Networks and computers that become infected are used to launch attacks against other networks and computers and may access or delete data held within them.

Framework for network defence

In improving cyber-defence, the awareness of potential attacks and an assessment of the impacts of those attacks must be made. This is typical risk assessment/risk management. Recent advances in applying data fusion techniques offer part of the solution.

The fusion of data allows basic awareness and assessments to be refined in order to identify new cyber-attacks. Recognition of the features of such attacks must be both dynamic and adaptive in order to generate initial estimates of the situation and to respond as new or unknown forms of attack emerge.

The following types of *network-based attacks*, focused on web, email or network attack, were identified as the most likely by Shen et al.⁵⁰

- *Buffer overflow* (web attack)—This occurs when a program does not check to ensure the data it is putting into a buffer area will actually fit into that area. A vulnerability currently exists in Microsoft IIS 5.0 running on Windows 2000 that allows a remote intruder to run arbitrary codes on the targeted machine, whereby the intruder is able to gain complete administrative control of the machine. A remote attacker could send a request that might cause the web server to crash with unexpected results.
- *Semantic URL attack* (web attack)—In a semantic Uniform Resource Locator (URL)⁵¹ attack, a client manually adjusts the parameters of its request by maintaining the URL's syntax but altering its semantic meaning. This attack is primarily used against Common Gateway Interface (CGI)⁵² driven websites. A similar attack involving web browser cookies⁵³ is commonly referred to as cookie poisoning.
- *Email bombing* (email attack)—An email bomb involves sending large volumes of email across the Internet to an address, seeking to overflow the mailbox or overwhelm the server. One possible response to this form of attack is to identify the source of the email bomb or spam and configure the router (either internally or through the network service provider) to prevent incoming packets from that address.
- *Email spam* (email attack)—Spam involves the use of electronic messaging systems to send unsolicited, undesired bulk messages, without the permission of the recipients. The addresses of recipients are obtained from network postings, web pages, databases, or through guesswork, using common names and domains.
- *Malware attachment* (email attack)—Malicious software (or malware) is software designed to infiltrate or damage a computer system without the owner's informed consent. Common Malware attacks include worms, viruses, and 'Trojan horses'.
- *Denial of service* (network attack)—A DS attack is an attempt to make a computer resource unavailable to its intended users. Typically, the targets are high-profile web servers, with the aim of the attack being to make the hosted web pages unavailable on the Internet. A DDS attack occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually a web server. Systems can be compromised through a variety of methods and attacks may be multi-stage. For example, email spam and Malware may be used first to gain control of several temporal network nodes, which might be poorly-protected servers, followed by a DS attack that is triggered to a specific target.

From a network defence perspective, the following *defensive actions* were considered by Shen et al:⁵⁴

- *Deployment of Intrusion Detection Systems*—An optimal deployment strategy of IDS should be used to maximise the chance of detecting all possible cyber-network attacks and intrusions.
- *Firewall configuration*—A firewall is an IT security device which is configured to permit or deny data connections that may be set and configured by the organisation's security policy. Firewalls can be either hardware or software based or both.
- *Email-filter configuration*—Email filtering involves organising email according to specified criteria. While this usually refers to the automatic processing of incoming messages, it also applies to outgoing emails and can involve human intervention as well as automatic processing. Email filtering will usually do one of three things—pass the message through unchanged for delivery to the specified user's mailbox, redirect the message for delivery elsewhere, or discard the message. Some email filters are also able to edit messages during processing.
- *Shut down or reset servers*—This should eliminate the threat; however, it also denies access to authorised users for the period of the shut-down.

Policy-makers, government administrators, infrastructure owners and operators need to work together to protect Australia against IW, implementing eight key initiatives.⁵⁵ First, all external entities who interface with the Australian Government's information infrastructure should be required to be ISO 17799 certified⁵⁶ or a new standard yet to be developed.

The ISO standards cover the following 12 domains: risk assessment and treatment, security policy, organisation of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, information security incident management, and business continuity management and compliance. Security analysts responsible for protecting sensitive information can be relatively confident if an organisation is ISO 17799 compliant. A high degree of information assurance (security) is likely to be a characteristic of the data set being used. The reverse may be true if the organisation is not compliant with ISO 17799.⁵⁷

Second, the Australian Government needs to oversee an information security awareness training program across all sectors, highlighting the threats and vulnerabilities associated with the use of the information infrastructure (especially computer networks and the Internet).

Third, all sensitive national research and development programs should implement an information security plan that includes personnel screening

practices, security training, and monitoring practices. The methods and means used by unfriendly competitors or hostile nation-states and the nature of modern-day information processing technology dictate that we must be vigilant in protecting critical information assets and our national research infrastructure.

Fourth, access to the Internet by Australian Government employees should be restricted and isolated. Only a limited number of employees need to have direct access to the Internet. In such cases, the workstations should be completely isolated from the internal network.

Fifth, communications on all Australian Government information systems should be encrypted.

Sixth, any products, materials, integrated circuits, components, programs, processes or other goods that are deemed to be crucial to national security of Australia should be manufactured exclusively in this country or from highly trusted allies.

Seventh, private owners of information networks that interface with any of the nation's critical infrastructure (e.g. defence, law enforcement, finance, and energy) should be required to become ISO 17799 certified. Critical infrastructure is defined by Perry as 'services that are so vital that their incapacity or destruction would have a debilitating impact on the defence or economic security of Australia'.⁵⁸

Eighth, Australia should do all it can to produce more domestic engineers and scientists. We are not growing the intellectual resources that are needed.

Cyber-crime⁵⁹

As just mentioned, the accelerated use of the Internet has led to a dramatic rise in criminal activity that exploits this interconnectivity for illicit financial gain and other malicious purposes, such as Internet fraud, child exploitation, and identity theft. Efforts to address cyber-crime⁶⁰ include activities associated with protecting networks and information, detecting criminal activity, investigating crime, and prosecuting criminals.

The annual loss due to computer crime was estimated to be US\$67.2 billion for US organisations, according to a 2005 Federal Bureau of Investigation (FBI) survey. The estimated losses associated with particular crimes include \$49.3 billion in 2006 for identity theft⁶¹ and US\$1 billion annually⁶² due to phishing.⁶³ These projected losses are based on direct and indirect costs that may include actual money stolen, estimated cost of intellectual property stolen, and recovery cost of repairing or replacing damaged networks and equipment.

Cyber-forensic tools and techniques⁶⁴ are a key component of cyber-crime investigations as they allow the gathering and examination of electronic evidence that can be useful for prosecution.

Table 2—Techniques used to commit cyber-crimes⁶⁵

Type	Description
Spamming	Sending unsolicited commercial email advertising for products, services, and websites. Spam can also be used as a delivery mechanism for malware and other cyber-threats.
Phishing	A high-tech scam that frequently uses spam or pop-up messages to deceive people into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, or other sensitive information. Internet scammers use email bait to 'phish' for passwords and financial data from the sea of Internet users.
Spoofing	Creating a fraudulent website to mimic an actual, well-known website run by another party. Email spoofing occurs when the sender address and other parts of an email header are altered to appear as though the email originated from a different source. Spoofing hides the origin of an email message.
Pharming	A method used by phishers to deceive users into believing that they are communicating with a legitimate website. Pharming uses a variety of technical methods to redirect a user to a fraudulent or spoofed website when the user types in a legitimate web address. For example, one pharming technique is to redirect users—without their knowledge—to a different website from the one they intended to access. Also, software vulnerabilities may be exploited or malware employed to redirect the user to a fraudulent website when the user types in a legitimate address.
Denial of Service attack	An attack in which one user takes up so much of a shared resource that none of the resource is left for other users. DS attacks compromise the availability of the resource.
Distributed Denial of Service attack	A variant of the DS attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Viruses	A program that 'infects' computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. A virus requires human involvement (usually unwitting) to propagate.
Trojan horse	A computer program that conceals harmful code. It usually masquerades as a useful program that a user would wish to execute.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
Malware	Malicious software designed to carry out annoying or harmful actions. Malware often masquerades as useful programs or is embedded into useful programs so that users are induced into activating them. Malware can include viruses, worms, and spyware.
Spyware	Malware installed without the user's knowledge to surreptitiously track and/or transmit data to an unauthorised third party.
Botnet	A network of remotely controlled systems used to coordinate attacks and distribute malware, spam, and phishing scams. Bots (short for 'robots') are programs that are covertly installed on a targeted system allowing an unauthorised user to remotely control the compromised computer for a variety of malicious purposes.

(Source: GAO, *CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats*, pp. 7–8)

Cyber-crime laws vary across the international community. Australia enacted its *Cybercrime Act* of 2001⁶⁶ to address this type of crime in a manner similar to the *U.S. Computer Fraud and Abuse Act* of 1986,⁶⁷ which specifies as a crime the knowing unauthorised access to the computers used by a financial institution, by a federal government entity, or for interstate commerce. Such crimes include knowingly accessing a computer without authorisation; damaging a computer by introducing a worm, virus or other attack device; or using unauthorised access to a government, banking, or commerce computer to commit fraud. Violations also include trafficking in passwords for a government computer, a

bank computer, or a computer used in interstate or foreign commerce, as well as accessing a computer to commit espionage.

In addition, international agreements are also emerging, such as the Council of Europe's *Convention on Cybercrime* signed by the United States and 29 other countries on 23 November 2001, as a multilateral instrument to address the problems posed by criminal activity on computer networks.

In one example of cyber-crime, a person in the United States was convicted of aggravated identity theft, access device fraud, and conspiracy to commit bank fraud in February 2007. He held over 4300 compromised account numbers and full identity information (i.e. name, address, date of birth, Social Security number, and mother's maiden name) for over 1600 individual victims.⁶⁸

US Department of Defense officials stated that its information network, representing approximately 20 per cent of the entire Internet, receives approximately six million probes/scans a day. Further, representatives from DOD stated that between January 2005 and July 2006, the agency initiated 92 cyber-crime cases, the majority of which involved intrusions or malicious activities directed against its information network.⁶⁹

Indonesian police officials believe the 2002 terrorist bombings in Bali were partially financed through online credit card fraud, according to press reports.⁷⁰ As the GAO Report argues:

As larger amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defence and intelligence communities increasingly rely on commercially available IT, the likelihood increases that information attacks will threaten vital national interests.⁷¹

The effectiveness of the systems put in place to audit and monitor systems, including intrusion detection systems, intrusion protection systems, security event correlation tools, and computer forensics tools,⁷² have limitations that impact their ability to detect a crime occurring.⁷³

Addressing our critical information infrastructure

When the Estonian authorities began removing a statue of a Soviet soldier (a Second World War memorial) from a park at the end of April 2007, a number of DDoS attacks disabled various websites such as the Estonian parliament, banks, ministries, newspapers and broadcasters. The attacks overloaded the bandwidths for the servers running the websites.⁷⁴

These attacks were not initiated by the Russian Government or its security service as was initially suggested. Fake Internet Protocol (IP) addresses were used, which pointed to a Russian Government computer. The attacks were low-tech and probably carried out by large numbers of 'script

kiddies'—teenagers with relatively little real computer expertise, who use readily available techniques and programs to search for and exploit weaknesses in computers via the Internet.

This reinforced the concern of many that Critical Infrastructure Protection (CIP) needs greater attention. There are two interlinked and at times reinforcing factors that concern nations: the expansion of the threat spectrum in recent years, especially in terms of malicious actors and their capabilities; and a new kind of vulnerability due to modern society's dependence on inherently insecure information systems.⁷⁵

Both of these factors combine to pose challenges that involve uncertainty over who, how, where, what, why, and when.⁷⁶ The notion of an imminent, direct and certain threat, which is how we treat most military threats, does not describe these challenges adequately. They are actually indirect, uncertain and future risks rather than threats.⁷⁷ For this reason, the focus needs to be as much on general vulnerabilities of society as it is on actors, capabilities and motivations.

Critical infrastructure is deemed critical because its incapacitation or destruction would have a debilitating impact on the national security and the economic and social welfare of a nation. Examples are telecommunications, power grids, transport and storage of gas and oil, banking and finance, traffic, water supply systems, emergency rescue services, and public administration. Fear of asymmetric measures being perpetrated against such targets has been aggravated by the information revolution.

Today, almost all critical infrastructure relies on various forms of software-based control systems for effective, reliable and continuous operation. Information and communication technologies (ICTs) connect infrastructure systems in such a way as to make them interrelated and interdependent. Thus, CII has joined the lexicon, and includes computers, software, the Internet, satellites and fibre-optics.

CIIs are generally regarded as inherently insecure. Most of the components are developed in the private sector, where the pressure of competition means security does not drive system design. Computer and network vulnerabilities are therefore to be expected, and these lead to information infrastructures with in-built instabilities and critical points of failure.⁷⁸

A relatively small attack on infrastructure can achieve a great impact, thus offering a 'force-multiplier' effect to those carrying out infrastructure attacks.⁷⁹ The spread of ICT has facilitated access to the tools for attack, and made the success of an attack more likely. In other words, asymmetric attacks against powerful countries have become that much easier to carry out and more likely to occur.

These risks (or asymmetric threats) are of two types—unstructured and structured. The former is random and relatively limited. It consists of adversaries with restricted funds and organisation and short-term goals, such as individual hackers and crackers as well as small groups of organised criminals. The resources, tools, skills and funding available to the actors are too limited to accomplish a sophisticated attack against critical infrastructure and, more important, the actors lack the motivation to do so. They do it for thrill, prestige or monetary gain.

In contrast, structured threats or risks are considerably more methodical and better supported. Adversaries from this group have extensive funding, organised professional support and access to intelligence products, and long-term strategic goals. Foreign intelligence services, well-organised terrorists, professional hackers involved in IW, larger criminal groups and industrial spies fall into this category.

Unfortunately, there are no clear boundaries between the two categories. Even though an unstructured threat is not usually considered of direct concern to national security, there is a possibility that a structured threat actor could masquerade as an unstructured threat actor, or that structured actors could seek the help of technologically skilled individuals from the other group.

Because of the uncertainty of threat, we need to focus on the risk of an event occurring. In this respect, the important question is not what caused the loss of information integrity, but rather what the possible result and complications may be. A power grid might fail because of a simple operating error without any kind of external influence or sophisticated hacker attack.⁸⁰ In all cases, the result is the same: a possible power outage that may set off a cascading effect of successive failures in interlinked systems. Analysing whether a failure was caused by a terrorist, a criminal, simple human error or spontaneous collapse will not help to stop or reduce the effect.

Thus, it would seem to be more appropriate to adopt an ‘all hazards’ approach, designed for protection efforts irrespective of the nature of the threat, with a focus on the capability to respond to a range of unanticipated events. The key is to create greater resilience, commonly defined as the ability of a system to recover from adversity and either revert to its original state or assume an adjusted state based on new requirements.⁸¹

Structural approaches, and attempts to prohibit the means of IW altogether or to restrict their availability, are largely not feasible because of the ubiquity and dual-use nature of IT.⁸² There are also concerns over military reliance on advanced ICT and the extensive IT infrastructure used to conduct operations, as discussed earlier.

Cyber-crime is considered a menace to the economic prosperity and social stability of all nations that are linked into the GII. All nations therefore have an

interest in working together to devise an international regime⁸³ that will ensure the reliability and survivability of information networks. Again, this is more of a resilience strategy than a threat-focused approach. Multilateral conventions on computer crime, such as the Council of Europe's *Convention on Cybercrime* of 2001,⁸⁴ could be expanded and built on. International organisations could help develop and promulgate information security standards and disseminate recommendations and guidelines on best practices. International law enforcement institutions and mechanisms, like Interpol, could be used for information exchange—in order to provide early warning of any attack—and cyber-crime investigations. Enhanced cooperative policing mechanisms could also be created.

Comprehensive protection against the entire range of threats and risks at all times is virtually impossible, not only for technical and practical reasons, but also because of the associated costs. What is possible is to focus protective measures on preventive strategies and on trying to minimise the impact of an attack when it occurs.

A key problem currently is that standard procedures do not exist for assessing the risks to critical infrastructure or for recommending security improvements. Furthermore, a framework for agreeing priorities for security remediation of those critical infrastructures deemed the most vulnerable does not exist.

As Stephen Gale (co-chair of the Foreign Policy Research Institute's Center on Terrorism, Counter-Terrorism, and Homeland Security) argued recently,⁸⁵ a key initiative for addressing these shortfalls would be the development and deployment of a Security Impact Statement (SIS), analogous to the Environmental Impact Statement (EIS) that exists to protect the environment. Like the EIS, the SIS would be designed as a means for both identifying vulnerabilities and determining the standards and methods to be used in protection and remediation.

The system would need to be able to estimate both the likelihood of specific events occurring and the impacts of alternative security measures to deal with those events. It would need to drive the prioritisation process of investing in security improvements. Experts would be used in determining the likelihood of specific threat scenarios and the likely outcomes of such threats. The optimal system would be one that could provide quantitative estimates of risks and vulnerabilities; clear indicators of priorities for investments in security; and standards for making specific, effective, and efficient improvements in security.

Under such a system, organisations would be required to undertake due diligence reviews for protecting infrastructure and be offered, say, tax credits as partial cost relief in recognition of their improvements in minimising risks to critical infrastructure.

Cryptography

The entire computing industry needs to work together to improve security, as businesses continue facing cyber-attacks. Experts believe that hardware, software, and networks can be made much safer by creating a multi-layered solution. Bill Gates has suggested replacing password protections, often too easily defeated by phishing and other forms of low-tech hacking, with an InfoCard—a digital identity that can be stored in the microchip of a smart card and used to access password-protected websites.⁸⁶

Of course Microsoft has a keen interest in promoting more secure computing environments, since its operating systems are routinely the target of virus attacks. Gates noted, however, that the shift away from passwords would likely take as long as four years because it requires the collaboration of numerous vendors.

While the InfoCard technology should be useful for personal data security, large institutions, such as banks, are looking at large-scale defences to tackle Internet scams. By using the very networks that hackers exploit, companies can fight fraud and cyber-crime at different nodes, instead of in isolation. For instance, if a cyber-criminal in a third-world country exploits a stolen credit card number and then tries to hide behind a proxy server in New York, that New York IP address could be quickly blacklisted and banks and other organisations immediately notified.

While creating more secure technology requires the coordination of software, networks, and hardware, cryptography is at the heart of it. And while no encryption scheme will be completely foolproof, there is a strong effort underway to address security issues before they become major problems.

Conclusion

This chapter has highlighted the value of information to Australia and the ADF today, and discussed the potential forms of IW that could be used against us. There are certain actions an adversary might take against us and certain things we can do to protect ourselves. And there are cyber-crime activities that need to be addressed, as well as CII aspects. This discussion on cyber-attacks and broad network defence flows neatly into the next two chapters, which examine information infrastructure attack in more detail and how we might best secure the Defence and national information infrastructures in Australia.

ENDNOTES

- ¹ J.V. McGee, L. Prusak, and P.J. Pyburn, *Managing Information Strategically: Increase your Company's Competitiveness and Efficiency by Using Information as a Strategic Tool*, John Wiley & Sons, New York, 1993, pp. 68–69.
- ² Edward Waltz, *Information Warfare: Principles and Operations*, Artech House Publications, Boston and London, 1998, pp. 54–55.
- ³ Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*, Little Brown, London, 1994, p. 140.
- ⁴ See John Arquilla and David Ronfeldt, *The Advent of Netwar*, RAND Corporation, Santa Monica, CA, 1996; and David F. Ronfeldt and John Arquilla, *Networks and Netwars*, RAND Corporation, Santa Monica, CA, January 2002.
- ⁵ Toffler, *War and Anti-War*, p. 142.
- ⁶ Toffler, *War and Anti-War*, p. 148.
- ⁷ See US Department of Defense, *Joint Doctrine for Information Operations*, Joint Publication 3-13, 9 October 1998, available at <http://www.iwar.org.uk/iwar/resources/us/jp3_13.pdf>, accessed 4 March 2008; and the subsequent *Information Operations*, Joint Publication 3-13, 13 February 2006, available at <http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf>, accessed 4 March 2008.
- ⁸ Discussed generically in Waltz, *Information Warfare: Principles and Operations*, p. 160.
- ⁹ David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*, Frank Cass, London and New York, 2004, pp. 91–92.
- ¹⁰ Amy Sands, 'Integrating Open Sources into Transnational Threat Assessments', in Jennifer E. Sims and Burton Gerber, *Transforming U.S. Intelligence*, Georgetown University Press, Washington, DC, 2005, p. 64.
- ¹¹ Richard A. Best, Jr. and Alfred Cumming, *Open Source Intelligence (OSINT): Issues for Congress*, CRS Report for Congress, Congressional Research Service, 5 December 2007, p. CRS-1, available at <<http://www.fas.org/sgp/crs/intel/RL34270.pdf>>, accessed 4 March 2008. Richard Best is a specialist in National Defense and Alfred Cumming is a specialist in Intelligence and National Security; both are within the Foreign Affairs, Defense, and Trade Division of CRS.
- ¹² See Mark M. Lowenthal, *Intelligence, From Secrets to Policy*, Second Edition, CQ Press, Washington, DC, 2003, p. 79.
- ¹³ Sands, 'Integrating Open Sources into Transnational Threat Assessments', pp. 64–65.
- ¹⁴ Sands, 'Integrating Open Sources into Transnational Threat Assessments', p. 65.
- ¹⁵ Hamilton Bean, 'The DNI's Open Source Center: An Organizational Communication Perspective', *International Journal of Intelligence and Counterintelligence*, vol. 20, no. 2, Summer 2007, pp. 240–57; and Robert K. Ackerman, 'Intelligence Center Mines Open Sources', *Signal*, March 2006, available at <http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=1102&zoneid=31>, accessed 4 March 2008.
- ¹⁶ This is discussed further in Lonsdale, *The Nature of War in the Information Age*, p. 73.
- ¹⁷ Ralph Bennett, *Behind the Battle: Intelligence in the War with Germany 1939-1945*, Pimlico, London, 1999, p. 9.
- ¹⁸ Ajay Singh, 'Time: The New Dimension in War', *Joint Force Quarterly*, no. 10, Winter 1995–96, pp. 56–61(60), available at <http://www.dtic.mil/doctrine/jel/jfq_pubs/1510.pdf>, accessed 4 March 2008.
- ¹⁹ Waltz, *Information Warfare: Principles and Operations*, pp. 6–7. Waltz also explains on page 27 how IW applies to the physical, information and cognitive domains viz:
 - physical—destruction or theft of computers and destruction of facilities, databases, communications nodes or lines;
 - information—electronic attack against information content or processes either in the network or during transmission; and
 - cognitive—targeted attacks against the human mind via electronic, printed or oral means.
- ²⁰ Samuel B. Griffith, *Sun Tzu: The Art of War*, Oxford University Press, London, Oxford, New York, 1963, p. 77.
- ²¹ Colonel R. Szafranski, US Air Force, 'A Theory of Information Warfare: Preparing for 2020', *Airpower Journal*, vol. 9, no. 1, Spring 1995, available at <<http://www.iwar.org.uk/iwar/resources/airchronicles/szfran.htm>>, accessed 4 March 2008.

- ²² Waltz, *Information Warfare: Principles and Operations*, p. 10.
- ²³ Waltz, *Information Warfare: Principles and Operations*, p. 18; and Martin Libicki, *What is Information Warfare?*, Center for Advanced Concepts and Technology, National Defense University, Washington, DC, 1995, p. 7.
- ²⁴ Waltz, *Information Warfare: Principles and Operations*, p. 28.
- ²⁵ Waltz, *Information Warfare: Principles and Operations*, p. 22.
- ²⁶ David S. Alberts, John J. Garstka, Richard E. Hayes, David A. Signori, *Understanding Information Age Warfare*, CCRP Publication Series, Washington, DC, August 2001, p. 4, available at <http://www.dodccrp.org/files/Alberts_UIAW.pdf>, accessed 4 March 2008.
- ²⁷ See William G. Perry, *Information Warfare: An Emerging and Preferred Tool of the People's Republic of China*, Occasional Papers Series, no. 28, The Center for Security Policy, Washington, DC, October 2007, available at <<http://www.centerforsecuritypolicy.org/modules/newsmanager/center%20publication%20pdfs/perry%20china%20iw.pdf>>, accessed 4 March 2008.
- ²⁸ This is the stated intention of Chinese IW. See Toshi Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?*, Strategic Studies Institute, U.S. Army War College, Carlisle, PA, November 2001, available at <<http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB62.pdf>>, accessed 4 March 2008.
- ²⁹ Perry, *Information Warfare: An Emerging and Preferred Tool of the People's Republic of China*.
- ³⁰ Adapted from Wendell Minnick, 'Computer Attacks from China leave many questions', *Defense News*, 13 August 2007, available at <<http://www.taiwanmilitary.org/phpBB2/viewtopic.php?p=38438&sid=8f527c809bde63b7c174fd9b3fbd7dd>>, accessed 4 March 2008.
- ³¹ In the cyber-attack on Estonia in May 2007, some analysts suggest that the network employed may have enlisted more than one million 'botnets'. See Mark Landler and John Markoff, 'In Estonia, What May Be the First Cyberwar', *International Herald Tribune*, 28 May 2007, available at <<http://www.iht.com/bin/print.php?id=5901141>>, accessed 4 March 2008.
- ³² Toshi Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?*
- ³³ Derived from Gary Waters and Desmond Ball, *Transforming the Australian Defence Force (ADF) for Information Superiority*, Canberra Papers on Strategy and Defence no. 159, Strategic and Defence Studies Centre, The Australian National University, Canberra, 2005, p. 53.
- ³⁴ Waters and Ball, *Transforming the Australian Defence Force (ADF) for Information Superiority*, pp. 53–54.
- ³⁵ Ira W. Merritt, 'Proliferation and Significance of Radio Frequency Weapons Technology', Statement before the Joint Economic Committee, US Congress, Washington, DC, 25 February 1998, available at <<http://www.house.gov/jec/hearings/radio/merritt.htm>>, accessed 4 March 2008; David Schriner, 'The Design and Fabrication of a Damaging RF Weapon by "Back Yard" Methods', Statement before the Joint Economic Committee, US Congress, Washington, DC, 25 February 1998, available at <<http://www.house.gov/jec/hearings/02-25-8h.htm>>, accessed 4 March 2008; Michael Knights, 'Options for Electronic Attack in the Iraq Scenario', *Jane's Intelligence Review*, December 2002, pp. 52–53; and 'Use It But Don't Lose It', *Aviation Week & Space Technology*, 9 September 2002, p. 29. See also Waters and Ball, *Transforming the Australian Defence Force (ADF) for Information Superiority*, p. 54.
- ³⁶ Waters and Ball, *Transforming the Australian Defence Force (ADF) for Information Superiority*, p. 54.
- ³⁷ John Markoff, 'China Link Suspected in Lab Hacking', *New York Times*, 9 December 2007, p. A-03, available at <<http://www.nytimes.com/2007/12/09/us/nationalspecial3/09hack.html>>, accessed 4 March 2008.
- ³⁸ United States Congressional Committee Testimony, 29 March 2007.
- ³⁹ See John J. Tkacik, Jr., *Trojan Dragons: China's International Cyber Warriors*, WebMemo no. 1735, The Heritage Foundation, 12 December 2007, available at <http://www.heritage.org/Research/AsiaandthePacific/upload/wm_1735.pdf>, accessed 4 March 2008. Tkacik also cites a presentation by Dr Andrew Palowitch entitled, 'Cyber Warfare: Viable Component to the National Cyber Security Initiative?' delivered at Georgetown University, Washington, DC, on 27 November 2007.
- ⁴⁰ Stephen Fidler, 'Steep Rise in Hacking Attacks from China', *Financial Times*, 5 December 2007, available at <<http://www.ft.com/cms/s/0/c93e3ba2-a361-11dc-b229-0000779fd2ac.html>>, accessed 4 March 2008. The source cites Yuval Ben-Itzhak, chief technology officer for Finjan, a Web security group based in San Jose, California.

⁴¹ Rhys Blakely, Jonathan Richards, James Rossiter, and Richard Beeston, 'MI5 Alert on China's Cyberspace Spy Threat', *TimesOnline*, 1 December 2007, available at <http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece>, accessed 20 December 2007.

⁴² 'Now France Comes Under Attack from PRC Hackers', *Agence France Presse*, 9 September 2007, available at <<http://www.taipeitimes.com/News/front/archives/2007/09/09/2003377917>>, accessed 4 March 2008.

⁴³ John Blau, 'German Gov't PCs Hacked, China Offers to Investigate: China Offers to Help Track Down the Chinese Hackers Who Broke into German Computers', *PC World*, 27 August 2007, available at <<http://www.washingtonpost.com/wp-dyn/content/article/2007/08/27/AR2007082700595.html>>, accessed 4 March 2008.

⁴⁴ Mark A. Kellner, 'China a "Latent Threat, Potential Enemy": Expert', *DefenseNews Weekly*, 4 December 2006, available at <<http://www.defensenews.com/story.php?F=2389588&C=america>>, accessed 4 March 2008.

⁴⁵ 'Red storm rising: DoD's efforts to stave off nation-state cyberattacks begin with China', *Government Computer News*, 21 August 2006, available at <http://www.gcn.com/print/25_25/41716-1.html>, accessed 4 March 2008.

⁴⁶ Hearing of the House Armed Services Committee on 'Recent Security Developments In China'; witnesses: Richard P. Lawless, Deputy Undersecretary of Defense For Asia-Pacific Affairs, and Major General Philip M. Breedlove, Vice Director For Strategic Plans and Policy, Joint Chiefs Of Staff; 13 June 2007. Transcript provided by Federal News Service.

⁴⁷ Hearing of the House Armed Services Committee on 'Recent Security Developments In China', 13 June 2007.

⁴⁸ Tkacik, *Trojan Dragons: China's International Cyber Warriors*.

⁴⁹ See Dan Shen, Genshe Chen, Jose B. Cruz, Jr., Erik Blasch, and Martin Kruger, *Game Theoretic Solutions to Cyber Attack and Network Defense Problems*, paper given to 12th ICCRTS Conference, entitled 'Adapting C2 to the 21st Century', 2007, available at <http://www.dodccrp.org/events/12th_ICCRTS/CD/html/papers/062.pdf>, accessed 4 March 2008.

⁵⁰ Shen, Chen, Cruz, Blasch, and Kruger, *Game Theoretic Solutions to Cyber Attack and Network Defense Problems*.

⁵¹ The URL identifies a resource and its network 'location' so it can be accessed.

⁵² The CGI is a standard protocol for interfacing external application software with an information server, commonly a web server. This allows the server to pass requests from a client web browser to the external application. The web server can then return the output from the application to the web browser.

⁵³ Cookies are parcels of text sent by a server to a web browser and then sent back unchanged by the browser each time it accesses that server. Cookies are used for authenticating, tracking, and maintaining specific information about users.

⁵⁴ Shen, Chen, Cruz, Blasch, and Kruger, *Game Theoretic Solutions to Cyber Attack and Network Defense Problems*.

⁵⁵ These are extracted from Perry, *Information Warfare: An Emerging and Preferred Tool of the People's Republic of China*.

⁵⁶ ISO/IEC 17799 is a set of international information security practices and standards. They specify accepted security practices related to securing information assets. The ISO/IEC 17799 standards (to become ISO 27000 in the future) seek to serve as 'a starting point for developing organization specific (information security) guidelines'. See International Organization for Standardization, *Information technology—Security techniques—Code of practice for information security management*, ISO/IEC, Second edition, Geneva, Switzerland, 16 June 2005.

⁵⁷ William G. Perry, 'Enhanced data mining information assurance by using ISO 17799', *Information: Assurance and Security, Data Mining, Intrusion Detection, Information Assurance and Data Networks Security*, Defense & Security Symposium, The International Society for Optical Engineering, 17 April 2006.

⁵⁸ Adapted from William G. Perry, 'The Science of Protecting the Nation's Critical Infrastructure', *Voices of Discovery*, Elon University, NC, 7 March 2007.

⁵⁹ See US Government Accountability Office (GAO), *CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO-07-705, Washington, D.C., June 2007, available at <<http://www.gao.gov/new.items/d07705.pdf>>, accessed 4 March 2008.

⁶⁰ Cyber-crime, as used in the GAO Report, refers to criminal activities that specifically target a computer or network for damage or infiltration and also refers to the use of computers as tools to conduct criminal activity.

⁶¹ Javelin Strategy & Research, *2007 Identity Fraud Survey Report: Identity Fraud is Dropping, Continued Vigilance Necessary*, Pleasanton, CA, February 2007.

⁶² US Department of Homeland Security, Remarks by Assistant Secretary Gregory Garcia at the RSA Conference on IT and Communications Security, San Francisco, CA, 8 February 2007, available at <http://www.dhs.gov/xnews/speeches/sp_1171386545551.shtm>, accessed 4 March 2008.

⁶³ Identity theft is the wrongful obtaining and using of another person's identifying information in some way that involves fraud or deception. Phishing is a high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information.

⁶⁴ Cyber-forensics employs electronic tools to extract data from computer media storage without altering the data retrieved. Cyber-forensics techniques may also require the reconstruction of media to retrieve digital evidence after attempts to hide, disguise, or destroy it.

⁶⁵ GAO, *CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats*, pp. 7–8.

⁶⁶ Australian Government, *Cybercrime Act: An Act to amend the law relating to computer offences, and other purposes*, No. 161, Canberra, 2001, available at <<http://scaleplus.law.gov.au/html/comact/11/6458/pdf/161of2001.pdf>>, accessed 11 March 2008.

⁶⁷ The *Computer Fraud and Abuse Act* (18 USC 1030), passed by the US Congress in 1986, was subsequently amended in 1994 and 1996, and again in 2001 by reference to the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, 2001* (Public Law 107-56). The *Computer Fraud and Abuse Act* was itself an amendment to somewhat limited *Counterfeit Access Device and Computer Fraud and Abuse Act, 1984* (Public Law 99-474), which was the first comprehensive US legislation to identify and provide for the prosecution of crimes committed through and against computer systems.

⁶⁸ Statement of Ronald J. Tenpas, Associate Deputy Attorney General before the Subcommittee on Terrorism, Technology and Homeland Security the Committee on the Judiciary, 21 March 2007, available at <http://judiciary.senate.gov/testimony.cfm?id=2582&wit_id=6194>, accessed 4 March 2008.

⁶⁹ GAO, *CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats*, p. 20.

⁷⁰ Alan Sipress, 'An Indonesian's Prison Memoir Takes Holy War Into Cyberspace', *Washington Post*, 14 December 2004, p. A19, available at <<http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html>>, accessed 4 March 2008.

⁷¹ GAO, *CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats*, p. 22.

⁷² Intrusion detection systems detect inappropriate, incorrect, or anomalous activity on a network or computer system. Intrusion prevention systems build on intrusion detection systems to detect attacks on a network and take action to prevent them from being successful. Security event correlation tools monitor and document actions on network devices and analyse the actions to determine if an attack is ongoing or has occurred. Computer forensic tools identify, preserve, extract, and document computer-based evidence.

⁷³ GAO, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*, GAO-04-321, Washington, DC, 28 May 2004, available at <<http://www.gao.gov/new.items/d04321.pdf>>, accessed 4 March 2008.

⁷⁴ See Myriam Dunn Cavely, 'Critical information infrastructure: vulnerabilities, threats and responses', in *Disarmament Forum* (Three), 2007, pp. 15–22. Myriam Dunn Cavely is head of the New Risks Research Unit at the Center for Security Studies at ETH Zurich, Switzerland and coordinator of the Crisis and Risk Network, available at <<http://se2.isn.ch/serviceengine/FileContent?serviceID=CRN&fileid=20009CBA-C36C-C7AC-D7C0-5E43B2974BC5&lng=en>>, accessed 4 March 2008.

⁷⁵ Cavely, 'Critical information infrastructure: vulnerabilities, threats and responses', p. 16.

⁷⁶ Emily O. Goldman, 'New Threats, New Identities, and New Ways of War: The Sources of Change in National Security Doctrine', *Journal of Strategic Studies*, vol. 24, no. 2, 2001, pp. 43–76 (45).

⁷⁷ J. van Loon, 'Virtual Risks in an Age of Cybernetic Reproduction', in B. Adam, U. Beck and J. van Loon (eds), *The Risk Society and Beyond: Critical Issues for Social Theory*, Sage, London, 2000, pp. 165–82.

⁷⁸ Michael Näf, 'Ubiquitous Insecurity? How to "Hack" IT Systems', *Information & Security: An International Journal*, no. 7, 2001, pp. 104–18, available at <<http://se1.isn.ch/serviceengine/FileContent?serviceID=PublishingHouse&fileid=9F1EA165-76C6-BF34-7522-6D4EA03FB0F5&lng=en>>, accessed 4 March 2008.

⁷⁹ Government of Canada, Office of Critical Infrastructure Protection and Emergency Preparedness, Threat Analysis No. TA03-001, 12 March 2003, available at <http://www.ocipep-bpiepc.gc.ca/opsprods/other/TA03-001_e.pdf>, accessed 4 March 2008.

⁸⁰ Of greater concern than simply hackers is 'hacktivism'. This is the blend of hacking and activism, and describes operations that use hacking techniques against a target's Internet site with the intent of disrupting normal operations but not causing serious damage. Examples are web 'sit-ins' and virtual blockades, automated email bombs, web hacks, computer break-ins, and computer viruses and worms. See Dorothy E. Denning, 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy', in J. Arquilla and D. Ronfeldt (eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, RAND Corporation, Santa Monica, CA, 2001, pp. 239–88, available at <http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf>, accessed 4 March 2008.

⁸¹ John A. McCarthy, 'Introduction: From Protection to Resilience: Injecting 'Moxie' into the Infrastructure Security Continuum', in *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, CIP Program Discussion Paper Series, George Mason University, Washington, DC, 2007, pp. 2–3, available at <cipp.gmu.edu/archive/CIPP_Resilience_Series_Monograph.pdf>, accessed 4 March 2008.

⁸² Heinrich Böll Stiftung, *Perspectives for Peace Policy in the Age of Computer Network Attacks*, Conference Proceedings, 2001, available at <<http://www.boell.de/downloads/medien/DokuNr20.pdf>>, accessed 4 March 2008; and Dorothy E. Denning, *Obstacles and Options for Cyber Arms Controls*, paper presented at Arms Control in Cyberspace Conference, Heinrich Böll Foundation, Berlin, 29–30 June 2001, available at <<http://www.cs.georgetown.edu/~denning/infosec/berlin.doc>>, accessed 4 March 2008.

⁸³ A regime can be defined as 'sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations'. See Stephen D. Krasner (ed.), *International Regimes*, Cornell University Press, Ithaca, New York, 1983, p. 2.

⁸⁴ Council of Europe Treaty Office, *Convention on Cybercrime*, CETS No. 185, opened for signature in Budapest, Hungary on 23 November 2001, available at <<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=16/04/04&CL=ENG>>, accessed 11 March 2008.

⁸⁵ See Stephen Gale, *Protecting Critical Infrastructure*, Foreign Policy Research Institute, November 2007, available at <<http://www.fpri.org/enotes/200711.gale.infrastructure.html>>, accessed 4 March 2008.

⁸⁶ Kate Greene, 'Calling Cryptographers', *MIT Technology Review*, 16 February 2006, available at <<http://www.technologyreview.com/Infotech/16347/?a=f>>, accessed 4 March 2008.