IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP5229

This paper appears in *Managing Modern Organizations Through Information Technology*, Proceedings of the 2005 Information Resources Management Association International Conference, edited by Mehdi Khosrow-Pour. Copyright 2005, Idea Group Inc.

Cyber-Terrorism: A Threat to Australia?

Christopher Beggs
School of Multimedia Systems, Monash University, Clyde Rd., Berwick, Victoria, Australia 3806, cjbeg1@student.monash.edu.au

ABSTRACT

Terrorism has become a major concern for the Australian Government and the Australian community since the September 11 2001 attacks in the US and the Bali bombings in 2002. This paper explores the potential threat of cyber-terrorism to Australia's security and highlights the measures the Australian Government has taken towards countering this new form of terrorism. The paper acknowledges the lack of overall strategy for a comprehensive cyber-terrorism defence plan, as well as underlining the need for future initiatives and developments to protect Australia from a possible cyber-terrorist attack.

INTRODUCTION

Australia's political climate and security environment has changed dramatically in the last century, especially since the atrocities of September 11 2001 in the US and the Bali bombings in 2002. Prior to these events, Australia's political and security environment was vastly different, as violent threats were generally faced offshore. Australia now faces the threat of possible cyber-terrorism, due to its dependence on Information Communication Technologies (ICTs). This reliance exposes new vulnerabilities within Australia's critical infrastructure and information systems and highlights the need for a cyber-terrorism defence plan. Currently, the Australian Government is developing counter measures for conventional terrorism; however, so far, preventative measures against cyber-terrorism have been limited.

NATIONAL SECURITY IN AUSTRALIA

In the past, Australia has been involved in various offshore conflicts including the two World Wars (1914-1918; 1939-1945), Korea (1951-1953) and Vietnam (1962-1972). More recently, Australia has been involved in the Gulf War, the East Timor War and currently, the Iraq War (Brodie 1990). In the 21st century, despite the fact that major power relations are more established and the threat of a conventional military attack on Australia has declined, the potential threat from global terrorism and the proliferation of weapons of mass destruction has grown (DPMC 2004).

Concerns about terrorism in Australia - which first arose following the Hilton bombings in 1978 - have been magnified since the September 11 2001 US attacks and the Bali bombings (2002). Consequently, the Australian Government has prioritised terrorism along with the need to develop an international response. In 2003, a global coalition against terrorism: The Coalition of the Willing (COTW) was formed. Comprising 70 nations - including America's North Atlantic Treaty Organisation (NATO) allies, Japan and Australia, as well as China, Russia, Pakistan and India - its diversity is unprecedented. The Australian Government, along with Britain, has committed military forces to the COTW operations against Osama Bin Laden's terrorist network and the Taliban regime (Dibb 2001).

Australia is also a member of the Asia Pacific Economic Cooperation (APEC): the premier forum for facilitating economic growth, cooperation, trade and investment in the Asia Pacific region. Special Task groups inside APEC such as the Counter Terrorism Task Force (CTTF) are committed to coordinating the implementation of the leader's statement on fighting terrorism and the promoting of growth agreed to in October 2002 (APEC Organisation 2004). The political standing that Australia has with APEC and its involvement with the CTTF enables the Australian Government to identify and assess counter-terrorism needs, coordinate capacity building and technical assistance programs, and co-operate with international and regional organisations.

Globalization itself has been an important factor in the international response to terrorism. On a political and economic level, globalization is the process of denationalization of markets, politics and legal systems (Globalization Limited Copyright 2001-2004). Organisations such as APEC can now globally allocate different task groups such as the CTFF by using new Internet technologies, as well as by implementing task groups to protect critical infrastructures such as power, military, water and gas. For example, CTFF members, including Australia, have signed the International UN Convention for the suppression of the financing of terrorism. The security of airports has been upgraded; coordination between enforcement intelligence officials has been strengthened; new cyber security standards have been developed; and the Energy Security Initiative has been advanced to address disruptions to energy markets (APEC 2004). Bodies such as the CTFF demonstrate the beneficial effects of globalization in combating global terrorism, as relationships between nations can be more readily established and allies can collaborate and share ideas more efficiently.

On the other hand, ICTs, particularly the Internet, have opened up new arenas and means of combat for terrorist organisations. The September 11 attacks and the Bali bombings revealed that terrorist organisations are using the Internet to orchestrate their attacks; to buy airplane tickets online and to send emails to communicate with other terrorists. New technologies enable them to legally gather information prior to their attacks. For example, computerized financial systems enable the transfer of funds, financing and logistical aid required for the support of terrorist activities, as well as allowing terrorist organisations to communicate with their members all over the world in a rapid, efficient and safe way (Schweitzer 2003).

CYBER-TERRORISM AND ITS POTENTIAL THREAT TO AUSTRALIA

Cyber security expert Dorothy Denning defines cyber-terrorism as

> *the convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objections. Further, to qualify as cyber-terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear (in Lawson 2001, p.1).*

However, Lewis (2002, p.1) claims that cyber-terrorism is "the use of computer network tools to shut down critical infrastructure such as energy, transportation, government operations or to coerce or intimidate a government or civilian population. Cyber-terrorism is not the same as hacking. Hackers take a delight in experimenting with system hardware, software and communications systems in an attempt to gain unauthorized access into a computer system. Unlike cyber-terrorists, they do not spread fear or cause harm to people - rather, they demonstrate their prowess, as well as revealing the fallibility of computer security (Warren 1999).

Potential cyber-terrorist acts include:

- An attack on an aircraft control system, causing two planes to collide.
- The alteration of the formulas of medication at pharmaceutical manufacture, causing several lethal dosages.
- Changing pressure in gas lines causing a valve failure, resulting in an explosion.
- Contamination of the water supplies causing many deaths.
- Attacking the share market causing economic chaos.
- Attacking electrical power supplies causing blackouts.
  (Collins 2000)

Meng (2002) claims that critical information infrastructures such as gas, water and electricity can be attacked through the application of cyber-terrorism in five mediums:

- Through corrupted systems hardware or software.
- Through electronic jamming devices.
- Through the use of an insider.
- By means of an external hackers.
- By physical attack.

He notes that cyber-weapons employed for the purpose of disrupting the information infrastructure include:

- Computer Viruses.
- Logic Bombs.
- Trojan Horses.
- Worms.
- Sniffer or Electronic Eavesdropping Programs.
- Next Generation Automated Computer Hacking Tools.

It is likely, however, that cyber-terrorist attacks would generally aid conventional terrorism. For example, if a bomb was to exploded in the Rialto building in Melbourne, Australia in conjunction with a cyber attack such as blocking the emergency phone lines and disabling power supplies in the CBD, the number of casualties would be increased, because rescue teams could not assist wounded casualties.

Australia's reliance on interconnected technologies has exposed them to new vulnerabilities which they have not before encountered. Pollitt (1999, p.1) claims that we are at risk because of our dependence on computers. "They control power delivery, communications, aviation and financial services. They are used to store vital information, from medical records to business plans to criminal records." However, the most dangerous threat we face is damage to our critical infrastructures: gas, banking and finances, emergency services, electrical power systems, health services, air and road transport and water supply systems; as these now rely on networked technologies to perform critical operations. Australia's dependence on global technologies which are incorporated within these systems and its current alliances with nations such as the US means that it faces the very real possibility of cyber-terrorism.

Many of Australia's critical infrastructures are controlled by industrial control systems. These systems can include distributed control systems (DCS) and programmable logic controllers (PLC) as well as supervisory control and data acquisitions (SCADA) systems (Shea 2003). Consequently, industrial control systems such as SCADA systems are becoming linked to corporate computer systems, potentially making them vulnerable to cyber attack through the Internet (Shea 2003). Like most computer systems, they have vulnerabilities. This is exemplified by an incident which occurred in November 2001 in Queensland Australia, when Vitek Boden hacked into an industrial control system using the Internet, a wireless radio and stolen control software. Boden, a former consultant on the water project, had attempted to gain access to the system 45 times. On his last attempt, he managed to release up to 1 million litres of sewage into the river and coastal waters of Maroochydore. As a result, marine life died, the creek water turned black and the stench was unbearable for residents (Lemos 2002).

Vulnerabilities within Australian systems are being exposed daily and more frequently as technology is advancing. Donovan (2003), Managing Director of Symantec, a world leading Internet Security organisation, claims that 2,524 new vulnerabilities were discovered in 2002: an increase of 81.5% over the prior six months. Jenkins (2004) also notes that Australia has jumped from 14th to 5th place in a global ranking of the sources of Internet attacks. In addition, a 2004 Australian Computer Crime and Security survey suggested that computer crime cost in Australia's private and public sectors had increased by 20% since 2003 (AusCERT 2004).

Although, so far, there have been no real cases of cyber-terrorism, these reports highlight system vulnerability and the ease of conducting a digital attack. Cyber-terrorism needs to be acknowledged by the Australian Government and private organisations as a potential security threat to our critical infrastructures which form the economic foundations of our country. Although the current Government is working on new security strategies to combat conventional terrorism, these are inadequate.

CURRENT METHODS AND STRATEGIES USED BY AUSTRALIA TO COMBAT CYBER-TERRORISM

In the wake of the September 11 and the Bali bombings the Australian Government's response to the threat of conventional terrorism has been reactive and has involved the development of new security protocols and policies. However, the emerging threat of cyber-terrorism has not received the same level of attention.

Combating terrorism requires complete co-operation from all parties involved. Prime Minister John Howard takes the lead role for counter-terrorism policy coordination, along with the Attorney-General, supported by the National Security Committee of Cabinet and other Ministers with responsibility for operational coordination on national security issues (AGAGD (b) 2004). The National Counter Terrorism Committee (NCTC) is the primary body for developing Australia's national counter-terrorism arrangements. The shift in Australia's security environment since September 11 has caused a significant impact on the PSCC (AGAD (a) 2004). The Australian Government's 2004-2005 budget includes an additional $755 million (including $144 million capital funding) over five years to counter the threat of terrorism in Australia. In total, the Government has committed $3.1 billion over the seven years from 2001-02 for a range of national security initiatives. Currently, there is no single Australian law enforcement or policy body which has responsibility for cyber-terrorism. Although there are various agencies which deal with cyber related crimes such as computer crime, each of these agencies has a different role ranging from the development of policy, to the policing and prosecution of crime. These include:

- Australian Crime Commission (ACC)
- Australian Hi Tech Crime Centre (AHTCC)
- Australian Securities and Investments Commission (ASIC) Australian Transactions Reporting and Analysis Centre (AUSTRAC)
- Action Group into the Law Enforcement Implications of Electronic Commerce (AGEC)
- Electronic Security Coordination Group (ESCG)
- Information Infrastructure Protection Group (IIPG
- Australian Computer Emergency Response Team (AUSCERT)
- Securities and E-business Assurance Research Group (SEAR)
- Trusted Information Sharing Network for Critical Infrastructure Protection (TISN)
  (Schneider 2003)

Although some of these agencies might assist in a cyber-security defence plan, there is a need for an agency to take direct responsibility for cyber-terrorism. Ford (2003) claims that the *Cybercrime Act 2001* was an important step towards achieving national consistency with the Council of Europe Convention and towards remedying deficiencies in existing laws. The computer offences laws are designed to protect the security, integrity and reliability of computer data and electronic communications.

The laws provide a strong deterrent to persons who engage in cyber crime activities such as hacking, computer virus propagation and denial of service attacks. For example, if a hacker obtains unauthorized access to a system or data, he or she now faces a maximum of 10 years imprisonment.

The Government also introduced the *Security Legislation Amendment (Terrorism) Act 2002* which for the first time makes specific reference to the concept of cyber-terrorism, that is the action or threat of action which seriously interferes with, seriously disrupts or destroys an electronic system including, but is not limited to information and telecommunications systems (Scale Plus Law Resource 2004). Other steps taken by the Australian Government towards the progress and co-operation between intelligence and law enforcement agencies in responding to cyber threats, vulnerabilities and incidents include the signing of an agreement with AusCERT, Australia's national Computer Emergency Response Team (CERT): an independent non-profit organisation which monitors and evaluates global computer network threats and vulnerabilities from numerous sources throughout the year, 24 hours a day. AusCERT also publishes security bulletins, drawing on material from a variety of sources, with recommended prevention and mitigation strategies (AusCERT 2004).

The Australian High Tech Crime Centre (AHTCC), hosted by the Australian Federal Police, is the main national level law enforcement body involved in the investigation of e-security incidents in public and private sector organisations. In 2003, the Australian Government committed $6.8 million to establish a high-tech crime capacity within the Australian Federal Police (DPMC (a) 2004). Likewise, in an APEC initiative, Australia is building on Computer Emergency Response Team (CERT) capacities in developing economies within the Asia Pacific Region. Australia is signatory to the Council of Europe Cyber Crime Convention (November 2001): the first multilateral instrument drafted to address the problems posed by the spread of criminal activity on computer networks (AGDFA (b) 2004).

More importantly, as Microsoft has noted, a number of industry-government partnerships have been established to tackle Internet security challenges. These include the creation of the Information Technology, Information Sharing and Analysis Centre which coordinates information sharing on cyber vulnerabilities among information technology companies. For example, in 2004 Microsoft Australia outlined its strategic direction for security by highlighting its forthcoming security products and previewing security initiatives from Microsoft Research as part of the Australian Security Summit at Darling Harbour in Sydney (Microsoft (a) 2004). However, more involvement from the private sector is needed to ensure a safer online security environment. For example, if private industry established several bodies which directly dealt with cyber-terrorism, organisations could use their services to protect their systems from a possible cyber-terrorist attack.

Private industry has also been involved in the development of security technologies. Many organisations believe that technical treatment at the technical level would seem to be the most effective preventative measure when dealing with cyber-terrorism. Technical treatment has the following advantages:

- It may identify risks at the front end.
- It provides a corporation an opportunity to treat the risk in a technical way.
- It forms the foundation for an effective risk management place. (Blyth 1999)

\However, Blyth (1999) suggests that technical risk treatment should not be viewed as the final word in risk management and computer related risks. Effective technical risk identification and treatment remain the foundations of proper risk management of cyber-terrorism.

Technical treatment of cyber-terrorism can include such security mechanisms as:

- Encryption
- Firewalls
- Intrusion Detection Systems
- Smart Cards
- Automated Biometrics Systems (a costly measure)

The above technologies are currently being used by many organisations to prevent cyber attacks but they should not be the sole method of prevention. According to Ellsmore (2002) 96% of companies surveyed (including utilities) in the 2002 Australian Computer Crime and Security Survey use firewalls; 100% use password protection and 99% use antivirus products. Despite these measures, 67% of these companies still suffered computer security incidents. Technology alone does not solve the problem of cyber attacks.

The author acknowledges that the level of security inside an organisation depends on the organisation's needs and requirements and its perception of risk. Generally, medium to large organisations would use all of the prevention technologies mentioned, but whilst organisations need to evaluate the most balanced and adequate solution for their needs, new strategies need to be developed in acquiring an effective security solution.

RECOMMENDATIONS

Technology alone is not proving to be successful in an overall cyber defence strategy, as new vulnerabilities continue to appear in information systems. An effective cyber security defence plans needs to have a greater focus on:

- **Strategy:** 3-5 year strategic planning (new strategies and methods).
- **Policy:** policy alignment (eg password changes).
- **Education:** of employees about security mechanisms.
- **Funding:** private sector input (agencies and communication).
- **Responsibility:** organisations need to take responsibility to secure networks.
- **Technology:** new technologies need to be developed and improved.
- **Auditing:** quality assurance of security systems.
- **Legislation:** deters terrorists and gain control.
- **Co-operation:** working together will close security gaps.
- **Communication:** communication channels will increase information sharing.
- **Commitment:** staying committed will reduce communication barriers

The author is currently developing such a plan, as well as a risk assessment of the likelihood of a cyber-terrorist attack in Australia. Together, these measures will go a long way towards protecting Australia's critical infrastructures and organisations; however, this research lies beyond the scope of this paper.

CONCLUSION

The Australian Government, together with private industry, need to re-evaluate their current online security environment in order to develop a comprehensive and effective cyber defence strategy. Although the government has taken some initial measures, further initiatives are needed in order to protect organisations assets from cyber attack and possible cyber-terrorism. The author's recommendations are currently under review and when finished will provide a comprehensive methodology to combat cyber-terrorism in Australia.

REFERENCES

Australian Computer Emergency Response Team (AusCERT) 2004 (Online) Available: http://www.auscert.org.au/render.html?cid=2 (Accessed 2004, July 28).

Australian Government Attorney Generals Department (AGAGD) (a) 2004 (Online) Available: http://www.ag.gov.au/www/protectivesecurityHome.nsf/HeadingPagesDisplay/History+and+Structure?OpenDocument (Accessed 2004, August 17).

AGAGD (b) 2004 (Online) Available: http://www.ag.gov.au/www/protectivesecurityHome.nsf (Accessed 2004, August 23).

Australian Government of Department of Foreign Affairs (AGDFA (b) (Online) Available: http://www.dfat.gov.au/apec/mexico2002/cybersecurity.html (Accessed 2004, August 26).

Asia Pacific Economic Cooperation (APEC) Copyright 2004 (Online) http://www.apecsec.org.sg/content/apec/apec_groups/som_special_task_groups/counter_terrorism.html (Accessed 2004, March 27).

Blyth, Toby (1999) "Cyber-terrorism and Private Corporations" *Supreme Courts of NSW* (Online) Available: http://www.terrorism.com/documents/TRC-Analysis/iw-privatrisk.pdf (Accessed 2004, July 28).

Brodie, Scott 1990, *Australia in the Vietnam War* PR Books NSW Australia.

Collin, Barry (2000) "The Future of Cyber-terrorism" *Institute for Security and Intelligence* (Online) Available: http://afgen.com/terrorism1.html (Accessed 2004, May 28).

Dibb, Paul, 2001 "The Utility and Limits of the International Coalition against Terrorism" *The Strategic and Defence Studies Centre*, The National Library of Australia.

Donovan, John (2003) "Parliamentary Joint Committee on the Australian Crime Commission Inquiry Into Cyber-crime" *Symantec Australia* Available: http://www.aph.gov.au/Senate/committee/acc_ctte/cybercrime/submissions/sub13.pdf (Accessed 2004, May 11).

Ellsmore, Nick (2002) "Cyber-Terrorism in Australia" *Sift Tactical Information Control* (Online) Available: http://www.sift.com.au/research/2002/SIFT_CyberTerrorism_Report.pdf (Accessed 2004, July 25).

Ford, Peter (2003)"Implementing a Culture of Security in Australia" Australian Government (Online) Available: http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf/viewHtml/index/$FILE/Australia.pdf (Accessed 2004, July 28).

Globalization Limited Copyright 2001-2004 (Online) Available: http://www.globalization.com/index.cfm?MyCatID=1&PageID=1321 (Accessed 2004, April 24).

Jenkins, Chris (2004) "Australia jumps net threat list" *Australian IT* (Online) Available: http://australianit.news.com.au/articles/0,7204,8975723%5e16123%5e%5enbv%5e,00.html (Accessed 2004, June 3).

Lawson, M. S. (2002) "Information Warfare: An Analysis of the Threat of Cyber-terrorism Towards the US Critical Infrastructure" *SANS* (Online) Available: http://www.sans.org (Accessed 2004, May 17).

Lemos, Robert (2002) "E-terrorism: Safety: Assessing the Infrastructure Risk" *CNET Networks* (Online) Available: http://news.com.com/2009-1001-954780.html (Accessed 2004, May 20).

Lewis, James (2002) "Assessing the Risks of Cyber-terrorism, Cyber War and Other Cyber Threats" *Centre for Strategic and International Studies* (Online) Available: http://www.csis.org/tech/0211_lewis.pdf (Accessed 2004, May 28).

Meng, Kim (2002) "Cyber-terrorism: An Emerging Security Threat of the New Millennium" *iMINDEF* (Online) Available: http://www.mindef.gov.sg/safti/pointer/back/journals/2002/Vol28_3/6.htm (Accessed 2004, June 1).

Microsoft Corporation 2004 (a) (Online) Available: http://www.microsoft.com/issues/essays/12-04cyberterrorism.asp (Accessed 2004, August 5).

Pollitt, Mark (1999) "Cyber-terrorism Fact or Fancy?" *Georgetown University USA* (Online) Available: http://www.cs.georgetown.deu/~denning/infosec/pollitt.html (Accessed 2004, May 28).

Scale Plus Law Resource 2004 (Online) Available: http://scaletext.law.gov.au/html/comact/11/6499/0/CM000080.htm (Accessed 2004, 25 August).

Schneider, Anton (2003) "Parliamentary Joint Committee on the Australian Crime Commission - Inquiry into Cyber crime" *AGD* (Online) Available: http://www.aph.gov.au/Senate/committee/acc_ctte/cybercrime/submissions/sub21.doc (Accessed 2004, August 24).

Schweitzer, Y 2003, *The Globalization of Terror*, Transaction New Brunswick USA.

Shea, Dana (2003) "Critical Infrastructure: Control Systems and the Terrorist Threat" *Congressional Research Services* (Online) Available: http://www.fas.org/irp/crs/RL31534.pdf (Accessed 2004, June 1).

The Department of the Prime Minster and Cabinet Copyright 2004 (DPMC) (Online) Available: http://www.dpmc.gov.au/pm/challenges/pm_challenges_toc_2004.cfm (Accessed 2004, April 22).

DPMC (a) (Online) Available: http://www.dpmc.gov.au/protecting_australia/preparedness/5_infrastructure.htm (Accessed 2004, 23 August).

Warren, M J (1999) "Cyber-terrorism –The Political Evolution of the Computer Hacker" *CISSR* (Online) Available: www.cissr.com/whitepapers/cyberterrorism4.pdf (Accessed 2004, June 1).