Bibliography

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

Ackerman, Robert K., '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.

Alberts, David S., John J. Garstka, Richard E. Hayes, David A. Signori, *Understanding Information Age Warfare*, CCRP Publication Series, Washington, DC, August 2001, available at <http://www.dodccrp.org/files/Alberts_UIAW.pdf>, accessed 4 March 2008.

Arquilla John, and David Ronfeldt, *The Advent of Netwar*, RAND Corporation, Santa Monica, CA, 1996.

Ashley, Bradley K. 'The United States is Vulnerable to Cyberterrorism', *SIGNAL*, March 2004, p. 61.

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.

Australian Government, Department of Defence, *A Concept for Enabling Information Superiority and Support*, Department of Defence, Canberra, August 2004.

———, *Australia's National Information Infrastructure: Threats and Vulnerabilities*, Defence Signals Directorate, February 1997.

———, *Australia's National Security: A Defence Update 2007*, Department of Defence, July 2007, available at <http://www.defence.gov.au/ans/2007/pdf/Defence_update.pdf>, accessed 25 February 2008.

———, Director General Capability and Plans, *NCW Roadmap 2007*, Defence Publishing Service, Canberra, February 2007, available at <http://www.defence.gov.au/capability/ncwi/docs/2007NCW_Roadmap.pdf>, accessed 4 March 2008.

———, 'DSTO and ADI Forge New Links in Network Centric Warfare', Defence Science and Technology Organisation, 2 September 2004, available at <http://www.dsto.defence.gov.au/news/3283/>, accessed 4 March 2008.

———, *Enabling Future Warfighting: Network Centric Warfare*, ADDP-D.3.1, Australian Defence Headquarters, Canberra, February 2004, available

at <http://www.defence.gov.au/strategy/fwc/documents/NCW_Concept.pdf>, accessed 4 March 2008.

———, *Executive Summary. Draft Environmental Impact Statement (EIS): Defence Headquarters Australian Theatre*, Department of Defence, Canberra, September 2003, p. ES-8.

———, *Explaining NCW*, Department of Defence, Canberra, 21 February 2006, available at <http://www.defence.gov.au/capability/NCWI/docs/Explaining_NCW-21feb06.pdf>, accessed 25 February 2008.

———, *Force 2020*, Department of Defence, Canberra, June 2002, available at <http://www.defence.gov.au/publications/f2020.pdf>, accessed 25 February 2008.

———, *Future Warfighting Concept*, Australian Defence Doctrine Publication (ADDP)-D.02, Department of Defence, Canberra, 2003, available at <http://www.defence.gov.au/publications/fwc.pdf>, accessed 25 February 2008.

———, 'Infosec', Defence Signals Directorate, available at <http://www.dsd.gov.au/ infosec/>, accessed 4 March 2008.

———, *Information Operations*, ADDP 3-13, Australian Defence Headquarters, 2006.

———, *Joint Operations for the 21st Century*, Department of Defence, Canberra, May 2007, available at <http://www.defence.gov.au/publications/FJOC.pdf>, accessed 25 February 2008.

———, *NCW Roadmap*, Department of Defence, Canberra, October 2005, updated in Director General Capability and Plans, *NCW Roadmap 2007*, Defence Publishing Service, Canberra, March 2007, available at <http://www.defence.gov.au/capability/ncwi/docs/2007NCW_Roadmap.pdf>, accessed 25 February 2008.

———, 'Network-Centric Warfare', Defence Science and Technology Organisation, available at <http://www.dsto.defence.gov.au/research/4051/page/4387/>, accessed 4 March 2008.

———, *The Australian Approach to Warfare*, Department of Defence, Canberra, June 2002, available at <http://www.defence.gov.au/publications/taatw.pdf>, accessed 4 March 2008.

Australian Government, Department of the Attorney-General, 'Budget 2001-2002 Fact Sheet. Protecting the National Information Infrastructure: Part of the Government's E-security Initiative'.

———, joint news release by the Minister for Communications, Information Technology and the Arts, and the Minister for Defence, 'Security in the Electronic Environment', 27 September 2001.

———, news release by Attorney-General Philip Ruddock MP, *Protecting Australia's Critical Infrastructure*, Parliament House, 11 May 2004, available at <http://ag.gov.au/www/agd/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~MR03CriticalInfrastructure07May04.doc/$file/MR03CriticalInfrastructure07May04.doc>, accessed 3 March 2008.

———, *Protecting Australia's National Information Infrastructure*, December 1998, available at <http://law.gov.au/publications/niirpt.ptl>.

Australian Government, Department of the Prime Minister and Cabinet, *Protecting Australia Against Terrorism 2006: Australia's National Counter-Terrorism Policy and Arrangements*, Department of the Prime Minister and Cabinet, Canberra, 2006, p. 60, available at <http://cipp.gmu.edu/archive/Australia_ProtectAUTerrorism_2006.pdf>, accessed 3 March 2008.

Australian Homeland Security Research Centre, *National Security Briefing Notes—Advancing domestic and national security practice: 2007 E-Security National Agenda*, July 2007, available at <http://www.homelandsecurity.org.au/files/2007_e-security_agenda.pdf>, accessed 3 March 2008.

Ball, Desmond, *Australia's Secret Space Programs*, Canberra Papers on Strategy and Defence no. 43, Strategic and Defence Studies Centre, The Australian National University, Canberra, 1988, chapter 3.

———, *Signals Intelligence in the Post-Cold War Era: Developments in the Asia-Pacific Region*, Institute of Southeast Asian Studies, Singapore, 1993.

———, 'Silent Witness: Australian Intelligence and East Timor', in Richard Tanter, Desmond Ball and Gerry van Klinken, *Masters of Terror: Indonesia's Military and Violence in East Timor*, Rowman & Littlefield, New York, 2006, pp. 177–201.

Bamford, James, *Body of Secrets: How America's NSA and Britain's GCHQ Eavesdrop on the World*, Century, London, 2001.

Bean, Hamilton, '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.

'Behind the Firewall—The Insider Threat', 15 April 2003, ARTICLE ID: 2122. See <http://enterprisesecurity.symantec.com/article.cfm?articleid=2122&PID= 14615847&EID=389>.

Bennett, Ralph, *Behind the Battle: Intelligence in the War with Germany 1939-1945*, Pimlico, London, 1999.

Best, Jr. Richard A. and Alfred Cumming, *Open Source Intelligence (OSINT): Issues for Congress*, CRS Report for Congress, Congressional Research Service, 5 December 2007, available at <http://www.fas.org/sgp/crs/intel/RL34270.pdf>, accessed 4 March 2008.

Bickers, Charles, 'Cyberwar: Combat on the Web', *Far Eastern Economic Review*, 16 August 2001, p. 30.

Blakely, Rhys, 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.

Blau, John, '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.

Blaxland, John, 'On Operations in East Timor—The experiences of the Intelligence Officer, 3rd Brigade', *Australian Army Journal*, 2000.

Bodeen, Christopher, 'Mainland Asks Taiwan to Stop Interference', *Washington Times*, 26 September 2002.

Bristow, Damon, 'Asia: Grasping Information Warfare?', *Jane's Intelligence Review, December 2000*, p. 34–35.

Carnegie Mellon Software Engineering Institute, 'Cert/CC Statistics 1998-2005', undated.

Cass, Stephen, 'Listening In', *IEEE Spectrum Special Report on Intelligence and Technology*, vol. 40, no. 4, April 2003, pp. 32–37, available at <http://www.estig.ipbeja.pt/~lmgt/st/other/Listening%20In.pdf>, accessed 4 March 2008.

Cavelty, Myriam Dunn, 'Critical information infrastructure: vulnerabilities, threats and responses', in *Disarmament Forum* (Three), 2007, pp. 15–22, available at <http://se2.isn.ch/serviceengine/FileContent?serviceID=CRN&fileid=20009CBA-C36C-C7AC-D7C0-5E43B2974BC5&lng=en>, accessed 4 March 2008.

Cebrowski, Ret. Admiral Arthur, speech to Network Centric Warfare 2003 Conference, January 2003, available at <http://www.oft.osd.mil>, accessed 25 February 2008.

CERT, 'CERT Advisory CA-2001-14 Cisco IOS HTTP Server Authentication Vulnerability', 28 June 2001, available at <http://www.cert.org/advisories/CA-2001-14.html>, accessed 4 March 2008.

'Chinese Cyber Espionage "Routine" in Australia', *Canberra Times*, 11 February 2008, p. 5.

Chulov, Martin, 'A Win Against Terror', *Australian*, 7 October 2007, p. 17, available at <http://www.theaustralian.news.com.au/story/0,20867,20536940-5001561,00.html>, accessed 4 March 2008.

Cilluffo Frank J., and J. Paul Nicholas, 'Cyberstrategy 2.0', *Journal of International Security Affairs*, No. 10, Spring 2006, available at <http://www.securityaffairs.org/issues/2006/10/cilluffo_nicholas.php>, accessed 3 March 2008.

CISCO, 'Multiple Vulnerabilities in Cisco Secure Access Control Server', 7 January 2007, available at <http://www.securiteam.com/securitynews/5DP0420KAG.html>, accessed 4 March 2008.

———, 'Optus Charts Future with Cisco Service Oriented Network at Macquarie Park Campus', 19 October 2006, available at <http://newsroom.cisco.com/dlls/global/asiapac/news/2006/pr_10-19.html>, accessed 4 March 2008.

———, 'CISCO Security Advisories', available at <http://www.cisco.com/en/US/products/products_security_advisories_listing.html>, accessed 4 March 2008.

Clark, Drew, 'Computer security officials discount chances of "digital Pearl Harbor"', *National Journal's Technology Daily*, 3 June 2003, available at <http://www.govexec.com/dailyfed/0603/060303td2.htm>, accessed 3 March 2008.

Coleman, Kevin, 'Inside DPRK's Unit 121', DefenseTech.org. 24 December 2007, available at <http://www.defensetech.org/archives/003920.html>, accessed 4 March 2008.

Computer Fraud and Abuse Act, 1986 (18 USC 1030) (amended 1994, 1996, and 2001).

Cornford, Philip, and Rob O'Neill, 'Bali Nine Phone Cards Cracked', *Age*, 4 May 2005.

Cosgrove, Peter, 'Innovation, People, Partnerships: Continuous Modernisation in the ADF'; speech to the Network Centric Warfare Conference on 20 May 2003, available at <http://www.defence.gov.au/cdf/speeches/past/speech20030520.htm>, accessed 25 February 2008.

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.

Counterfeit Access Device and Computer Fraud and Abuse Act, 1984 (Public Law 99-474).

Crawley, Vince and Amy Svitak, 'Is Predator the Future of Warfare?', *Defense News*, 11–17 November 2002, p. 8.

Crompton, Malcolm, 'Proof of ID Required? Getting Identity Management Right', keynote address to the Australian IT Security Forum, Sydney, 30 March 2004, available at <http://www.privacy.gov.au/news/speeches/sp1_04p.pdf>, accessed 3 March 2008.

Datz, Todd, 'Out of Control', *CSO*, vol. 2, no. 1, 2005, p. 28.

Davis, Mark, 'Canberra, CEOs extend forum on Terrorism', *Australian Financial Review*, 24 June 2004, p. 3.

Dawnay, Ivo, 'Beijing Launches Computer Virus War on the West', *Age* (Melbourne), 16 June 1997, p. 8.

Dawson, Chester, 'Cyber Attack', *Far Eastern Economic Review*, 10 February 2000, p. 21.

de Nysschen, Heinrich, 'Homeland Security', *Image & Data Manager*, May/June 2005, p. 36.

Denning, Dorothy E., '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.

———, *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.

Dudgeon, Ian,'Intelligence Support to the Development and Implementation of Foreign Policies and Strategies', *Security Challenges*, vol. 2, no. 2, July 2006, pp. 61–80, available at <http://securitychallenges.org.au/SC%20Vol%202%20No%202/vol%202%20no%202%20Dudgeon.pdf>, accessed 26 February 2008.

Fidler, Stephen, '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.

'Fighting the worms of mass destruction', *Economist*, 27 November 2003, available at <http://www.economist.com/science/displayStory.cfm?story_id=2246018>, accessed 3 March 2008.

Filippidis, Arthur, Tan Doan and Brad Tobin, 'Net Warrior—DSTO Battlelab Interoperability', Simulation Industry Association of Australia, June 2007, available at <http://www.siaa.asn.au/simtect/2007/Abstracts/70.html>, accessed 4 March 2008.

Flood, Philip, *Report of the Inquiry into Australia's Intelligence Agencies*, Canberra, July 2004, available at <http://www.pmc.gov.au/publications/intelligence_inquiry/index.htm>, accessed 4 March 2008.

'14 Tbps Over a Single Optical Fiber: Successful Demonstration of World's Largest Capacity', *NTT Press Release*, 29 September 2006, available at <http://www.ntt.co.jp/news/news06e/0609/060929a.html>, accessed 4 March 2008.

Freer, John R., *Computer Communications and Networks*, UCL Press, University College London, London, 2nd edition, 1996.

Fulghum, David A., 'Infowar to Invade Air Defense Networks', *Aviation Week & Space Technology*, 4 November 2002, p. 30.

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

Goldman, Emily O., '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.

Gonsalves, Antone, 'Gartner: Dependence On Internet Boosts Risks of Cyberwar', *InformationWeek*, 15 January 2004, available at <http://www.informationweek.com/story/showArticle.jhtml?articleID=17301666>, accessed 3 March 2008.

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.

Grabosky, Peter, *Electronic Crime*, Prentice Hall, Upper Saddle River, NJ, 2007.

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

Greenfield, Heather, 'Industry Officials Sketch Priorities for DHS Cyber Czar', *National Journal's Technology Daily*, 2 October 2006, available at

<http://www.govexec.com/dailyfed/1006/100206tdpm1.htm>, accessed 3 March 2008.

Griffith, Samuel B., *Sun Tzu: The Art of War*, Oxford University Press, London, Oxford and New York, 1963, p. 77.

'Half the world has a mobile phone', *ITU News*, January–February 2008.

Hindell, Juliet, 'Japan Wages "Cyber War" Against Hackers', *Internet Security News*, 24 October 2000, available at <http://www.landfield.com/isn/mail-archive/2000/Oct/0116.html>, accessed 4 March 2008.

Homer-Dixon, Thomas, 'The Rise of Complex Terrorism', *Foreign Policy*, Issue No. 128, January//February 2002, pp. 52–62.

Hoyle, Craig and Andrew Koch, 'Yemen Drone Strike: Just the Start?', *Jane's Defence Weekly*, 13 November 2002, p. 3.

Huxley, Tim, *Defending the Lion City: The Armed Forces of Singapore*, Allen & Unwin, Sydney, 2000.

Tseng, I-Ling, *Chinese Information Warfare (IW): Theory Versus Practice in Military Exercises (1996–2005)*, MA Sub-thesis, Graduate Studies in Strategy and Defence, Strategic and Defence Studies Centre, The Australian National University, Canberra, March 2005.

'Increased Telephone Interception Capacity', in Australian Federal Police, *National Illicit Drug Strategy Initiatives, November 1997—April 2001* (Second edition), p. 13, available at <http://www.afp.gov.au/__data/assets/pdf_file/6634/ nids.pdf>, accessed 4 March 2008.

International Institute for Strategic Studies, *International Institute for Strategic Studies (IISS) Strategic Survey 2003/4*, Oxford University Press, Oxford, May 2004.

International Organization for Standardization, *Information technology—Security techniques—Code of practice for information security management*, ISO/IEC, Second edition, Geneva, Switzerland, 16 June 2005.

'Japan/Crime: Cyber-terror Task Force Established', *Bangkok Post*, 27 January 2000, p. 6.

Japan Defense Agency, *Defense of Japan 2000*, Japan Defense Agency, Tokyo, 2000, chapter 3, section 3(ii), and chapter 4, section 5(3).

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

Jenkins, Chris, 'Internet Terrorism Fears as Virus Hits', *Australian*, 28 January 2004, p. 3.

Kaufman, Gail, 'New Eyes, New Rules', *Defense News*, 2–8 December 2002, pp. 1–2.

Kellner, Mark A., '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.

Kenyon, Henry S., 'Networking Moves Into the High Frontier', *SIGNAL*, April 2004, pp. 59–62.

Kerfoot, Frank W., and William C. Marra, 'Undersea Fiber Optic Networks: Past, Present, and Future', *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 7, September 1998, pp. 1220–25, available at <http://ieeexplore.ieee.org/iel4/49/15642/00725191.pdf?arnumber=725191>, accessed 4 March 2008.

Knights, Michael, 'Options for Electronic Attack in the Iraq Scenario', *Jane's Intelligence Review*, December 2002, pp. 52–53.

Koch, Andrew, 'Information Warfare Tools Rolled Out in Iraq', *Jane's Defence Weekly*, 6 August 2003, p. 7.

———, 'New Powers for Info Operations Chiefs', *Jane's Defence Weekly*, 17 September 2003, p. 6.

Krasner, Stephen D. (ed.), *International Regimes*, Cornell University Press, Ithaca, New York, 1983, p. 2.

Lake, Darren, 'Taiwan Sets Up IW Command', *Jane's Defence Weekly*, 10 January 2001, p. 17.

Landler, Mark, 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.

Larkin, John, 'Preparing for Cyberwar', *Far Eastern Economic Review*, 25 October 2001, p. 64.

Lentz, Robert F., testimony before the House Armed Services Committee on Terrorism, Unconventional Threats and Capabilities, hearing on 'Cyber Terrorism: The New Asymmetric Threat', 24 July 2003, available at <http://www.iwar.org.uk/cip/resources/status-of-dod-ia/03-07-24lentz.htm>, accessed 3 March 2008.

Libicki, Martin C., *What is Information Warfare?*, Center for Advanced Concepts and Technology, National Defense University, Washington, DC, 1995.

Lies, Elaine, 'Doomsday Cult Casts Shadow Over Japan', *Canberra Times*, 20 March 2000, p. 7.

Lonsdale, David J., *The Nature of War in the Information Age: Clausewitzian Future*, Frank Cass, London and New York, 2004.

Lowenthal, Mark M., *Intelligence, From Secrets to Policy*, Second Edition, CQ Press, Washington, DC, 2003.

Mahony, Trevor W., 'A Hybrid Civilian/Military Payload to Support Battlefield Communications', *Journal of Battlefield Technology*, vol. 1, no. 1, March 1998, pp. 29–32.

Makarenko, Tamara, 'The Crime-Terror Continuum: Tracing the Interplay Between Transnational Organised Crime and Terrorism', *Global Crime*, vol. 6, no.1, February 2004, pp. 129–45, available at <http://www.silkroadstudies.org/new/docs/publications/Makarenko_GlobalCrime.pdf>, accessed 26 February 2008.

Markoff, John, '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.

Markus, Francis, 'Taiwan's Computer Virus Arsenal', *BBC News*, 10 January 2000, available at <http://news.bbc.co.uk/1/hi/world/asia-pacific/597087.stm>, accessed 4 March 2008.

McCarthy, John A., '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 <http://cipp.gmu.edu/archive/CIPP_Resilience_Series_ Monograph.pdf>, accessed 4 March 2008.

McGee, J.V., 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.

McGlinchey, David, 'Agencies, Congress urged to upgrade computer security planning', GovExec.com, Washington DC, 17 March 2004, available at <http://www.govexec.com/dailyfed/0304/031704d1.htm>, accessed 3 March 2008.

McKenna, Tim, Terry Moon, Richard Davis and Leoni Warne, 'Science and Technology for Australian Network-Centric Warfare: Function, Form and Fit', *ADF Journal*, no. 17, pp. 62–75.

McLachlan, Kevin, 'Flaw Found in Cisco Secure Access Control Server', 26 June 2006, available at <http://www.crn.com/it-channel/189601708>, accessed 4 March 2008.

Merritt, Ira W., '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.

Milliken, Robert, 'Canberra Acts to Keep an Eye on its Spies', *Independent* (London), 2 June 1995, available at <http://findarticles.com/p/articles/mi_qn4158/is_19950602/ai_n13986087>, accessed 4 March 2008.

Ministry of National Defense, *Republic of China, 2002 National Defense Report*, Ministry of National Defense, Taipei, July 2002.

Minnick, Wendell, 'Computer Attacks from China leave many questions', *Defense News*, 13 August 2007, available at <http://www.taiwanmilitary.org/phpBB2/viewtopic.php?p=38438&sid=8f527c809bde63b7c174fd9b3fbdb7dd>, accessed 4 March 2008.

———, 'Taiwan Upgrades Cyber Warfare', *Jane's Defence Weekly*, 20 December 2000, p. 12.

'MND Sets Up Information Warfare Committee', *ADJ News Roundup*, August 1999, p. 14.

Näf, Michael, '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.

Nairne, Doug, 'State Hackers Spying On Us, Say Chinese Dissidents', *South China Morning Post*, 18 September 2002, available at <http://www.infosyssec.com/ securitynews/0209/6536.html>, accessed 4 March 2008.

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

'North Korea Operating Computer-hacking Unit', *Korea Herald*, 28 May 2004, available at <http://www.asiamedia.ucla.edu/article-eastasia.asp?parentid+11559>, accessed 4 March 2008.

'North Korea Ready to Launch Cyber War: Report', Computer Crime Research Center, 4 October 2004, available at <http://www.crime-research.org/news/04.10.2004/North_Korea_ready_to_launch_cyber_war/>, accessed 4 March 2008.

'North Korea's Information Technology Advances and Asymmetric Warfare', *WMD Insights*, April 2006, available at

<http://www.wmdinsights.org/I4/ EA1_NorthKoreaInfoTech.htm>, accessed 4 March 2008.

'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.

'NSA Tapping Underwater Fiber Optics', available at <http://slashdot.org/articles/01/05/23/2142216.shtml>, accessed 4 March 2008.

'Optus Positions for National Satellite Success', December 2001, available at <http://www.optus.net.au/portal/site/aboutoptus/menuitem.813c6f701cee5a14f0419f108c8ac7a0/?vgnextoid=a7ab8336054f4010VgnVCM1000009fa87c0aRCRD&vgnextchannel=b93cfaf924954010VgnVCM10000029a67c0aRCRD&vgnextfmt=default>, accessed 4 March 2008.

'Outrage in Berlin Over Chinese Cyber Attacks', 31 August 2007, available at <http://www.weeklystandard.com/weblogs/TWSFP/2007/08/outrage_in_berlin_over_chinese.asp>, accessed 4 March 2008.

Palowitch, Andrew, 'Cyber Warfare: Viable Component to the National Cyber Security Initiative?'speech delivered at Georgetown University, Washington, DC, 27 November 2007.

Perry, William G., '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.

———, *Information Warfare: An Emerging and Preferred Tool of the People's Republic of China*, Occasional Papers Series, no. 28, October 2007, The Center for Security Policy, Washington, DC, available at <http://www.centerforsecuritypolicy.org/modules/newsmanager/center%20publication%20pdfs/perry%20china%20iw.pdf>, accessed 4 March 2008.

———, 'The Science of Protecting the Nation's Critical Infrastructure', *Voices of Discovery*, Elon University, NC, 7 March 2007.

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

'Privacy exposed', *Sydney Morning Herald*, 19 February 2004, available at <http://smh.com.au/articles/2004/02/18/1077072702295.html>, accessed 3 March 2008.

'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.

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

Richelson, Jeffrey, 'Desperately Seeking Signals', *Bulletin of the Atomic Scientists*, vol. 56, no. 2, March/April 2000, pp. 47–51.

Ronfeldt, David F., and John Arquilla, *Networks and Netwars*, RAND Corporation, Santa Monica, CA, January 2002.

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

Sands, Amy , '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.

Saxton, Jim, opening statement before the House Armed Services Committee on Terrorism, Unconventional Threats and Capabilities; hearing on 'Cyber Terrorism: The New Asymmetric Threat', 24 July 2003, available at <http://www.iwar.org.uk/cip/resources/status-of-dod-ia/03-07-24saxton.htm>, accessed 3 March 2008.

Schmidtchen, David, *The Rise of the Strategic Private: Technology, Control and Change in a Network Enabled Military*, The General Sir Brudenell White Series, Land Warfare Studies Centre, Canberra, 2006.

Schriner, David, '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.

Shen, Dan, 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.

Sherman, Jason, 'Report: China Developing Force to Tackle Information Warfare', *Defense News*, 27 November 2000, pp. 1 and 19.

Singh, Ajay, 'Time: The New Dimension in War', *Joint Force Quarterly*, no. 10, Winter 1995–96, pp. 56–61, available at <http://www.dtic.mil/doctrine/jel/jfq_pubs/1510.pdf>, accessed 4 March 2008.

Sipress, Alan, '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.

Smith, Edward A., *Complexity, Networking & Effects-Based Approaches to Operations*, Command and Control Research Program (CCRP), Department of Defense, July 2006, available at <http://www.dodccrp.org/files/Smith_Complexity.pdf>, accessed 26 February 2008.

Spafford, Eugene. H., testimony before the House Armed Services Committee on Terrorism, Unconventional Threats and Capabilities; hearing on 'Cyber Terrorism: The New Asymmetric Threat', 24 July 2003, available at <http://www.iwar.org.uk/cip/resources/status-of-dod-ia/03-07-24 spafford.pdf>, accessed 3 March 2008.

Spillius, Alex, 'America Prepares for Cyber War with China', *Telegraph* (London), 15 June 2007, available at <http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/06/15/wcyber115.xml>, accessed 4 March 2008.

Stewart, Cameron, 'Telstra Operation Helped Track Down Bali Bombers', *Australian*, 7 October 2006, p. 8, on-line version entitled 'Telstra Secretly helped Hunt Bali Bombers' at <http://www.news.com.au/story/0,23599,20537904-2,00.html>, accessed 4 March 2008.

Stiftung, Heinrich Böll, *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.

Szafranski, Colonel R., '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.

'Taiwan Prepares for Cyber Warfare', *CNN.Com*, 29 July 2002.

'Taiwan Report Finds Cyberthreat From China', *International Herald Tribune*, 30 July 2002.

'Taiwan to Conduct Cyber Warfare Drills', *Jane's Defence Weekly*, 16 August 2000, p. 10.

'Telecommunications Interception Law Dispute Shows Law Needs Overhaul', *Electronic Frontiers Australia*, 31 March 2004, available at <http://www.efa.org.au/Publish/PR040331.html>, accessed 4 March 2008.

Tenpas, Ronald J., Statement of 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.

Thompson, Clive, 'The Virus Underground', *New York Times*, 8 February 2004, available at <http://engineering.dartmouth.edu/courses/engs004/virusarticle.html>, accessed 26 February 2008.

'Timeline of Notable Computer Viruses and Worms', Wikipedia, available at <http://en.wikipedia.org/wiki/Timeline_of_notable_computer_viruses_and_worms>, accessed 4 March 2008.

Titheridge, Alan, Gary Waters, and Ross Babbage, *Firepower to Win: Australian Defence Force Joint Fires in 2020*, Kokoda Paper no. 5, The Kokoda Foundation, Canberra, October 2007.

Tkacik, John J. 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.

Toffler, Alvin and Heidi, *War and Anti-War: Survival at the Dawn of the 21st Century*, Little Brown, London, 1994.

'Tokyo's Claim to Tok-do Escalates Korea-Japan Cyber War', *Korea Times*, 14 May 2000.

United States Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, 17 October 2007, available at <http://www.dtic.mil/doctrine/jel/doddict/data/g/02329.html>, accessed 28 February 2008.

———, *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.

———, *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.

———, *Report on Network Centric Warfare*, 2001, available at <http://www.defenselink.mil/nii/NCW/ncw_sense.pdf>, accessed 25 February 2008.

United States 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.

United States Government Accountability Office (GAO), *CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO-07-705, Report to Congressional Requesters, Washington, DC, June 2007, available at <http://www.gao.gov/new.items/d07705.pdf>, accessed 4 March 2008.

———, *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.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, 2001 (Public Law 107-56).

US White House, *Critical Infrastructure Identification, Prioritization, and Protection*, Homeland Security Presidential Directive No. 7, White House, 17 December 2003, available at <http://www.whitehouse.gov/news/ releases/2003/ 12/20031217-5.html>, accessed 3 March 2008.

———, *The National Strategy to Secure Cyberspace*, White House, Office of the Press Secretary, February 2003, available at <http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf>, accessed 4 March 2008.

'Use It But Don't Lose It', *Aviation Week & Space Technology*, 9 September 2002, p. 29.

van Loon, J. '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.

Wall, Robert, 'Focus on Iraq Shapes Electronic, Info Warfare', *Aviation Week & Space Technology*, 4 November 2002, p. 34.

Waltz, Edward, *Information Warfare: Principles and Operations*, Artech House Publications, Boston and London, 1998.

Waters, Gary 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.

Wilson, Clay, *Information Operations and Cyberwar: Capabilities and Related Policy Issues*, Congressional Research Service, Library of Congress, Washington, DC, 14 September 2006, p. 8, available at <http://www.fas.org/irp/crs/RL31787.pdf>, accessed 4 March 2008.

———, *Network Centric Warfare: Background and Oversight Issues for Congress*, Congressional Research Service (CRS) Report for Congress, 2 June 2004, available at <http://www.fas.org/man/crs/RL32411.pdf>, accessed 25 February 2008.

Yang Kuo-wen, Lin Ching-chuan and Rich Chang, 'Bureau Warns on Tainted Discs', *Taipei Times*, 11 November 2007, p. 2, available at <http://www.taipeitimes.com/News/taiwan/archives/2007/11/11/2003387202>, accessed 4 March 2008.

Yoshihara, Toshi, *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.

Websites

Armed Forces Communications and Electronics Association: <http://www.afcea.org/>

Australian Computer Emergency Response Team: <http://www.auscert.org.au/>

Australian Federal Police: <http://www.afp.gov.au/home.html>

Australian Government Attorney General's Department: <http://ag.gov.au/>

Australian Government Department of Defence: <http://www.defence.gov.au/>

Australian Government Department of Defence, Defence Signals Directorate: <http://www.dsd.gov.au/>

Australian Government Department of Defence, Defence Science and Technology Organisation: <http://www.dsto.defence.gov.au/>

Australian Government Department of the Prime Minister and Cabinet: <http://www.pmc.gov.au/>

Australian Government Initiative, Stay Smart Online: <http://www.staysmartonline.gov.au/>

Australian Government Office of the Privacy Commissioner: <http://www.privacy.gov.au/>

Australian High Tech Crime Centre: <http://www.ahtcc.gov.au>

Australian Homeland Security Research Centre: <http://www.homelandsecurity.org.au/>

Center for Security Policy: <http://www.centerforsecuritypolicy.org/>

CERT Coordination Center: <http://www.cert.org/certcc.html>

Cisco Systems, Inc: <http://www.cisco.com/>

Computer Crime Research Center: <http://www.crime-research.org/>

Council of Europe Treaty Office: <http://conventions.coe.int/>

Electronic Frontiers Australia: <http://www.efa.org.au/>

Federation of American Scientists: <http://www.fas.org/>

Foreign Policy Research Institute: <http://www.fpri.org/>

International Organization for Standardization:
<http://www.iso.org/iso/home.htm>

Military.com, DefenseTech.org: <http://www.defensetech.org/>

Rand Corporation: <http://www.rand.org/>

Simulation Industry Association of Australia: <http://www.siaa.asn.au/>

Strategic Studies Institute of the U.S. Army War College:
<http://www.strategicstudiesinstitute.army.mil/>

The Heritage Foundation: <http://www.heritage.org/>

United States Department of Defense: <http://www.defenselink.mil/>

United States Department of Defense, Chief Information Officer, Assistant Secretary of Defense (Networks & Information Integration):
<http://www.defenselink.mil/cio-nii/>

United States Department of Defense, Command and Control Research Program:
<http://www.dodccrp.org/>

United States Department of Defense, Defense Technical Information Center:
<http://www.dtic.mil/>

United States Department of Defense, Office of Force Transformation:
<http://www.oft.osd.mil>

United States Department of Homeland Security:
<http://www.dhs.gov/index.shtm>

United States Government Accountability Office: <http://www.gao.gov/>

United States House of Representatives: <http://www.house.gov/>

United States House of Representatives Joint Economic Committee:
<http://www.house.gov/jec/>