Information Warfare

Part 1: What You Need to Know

by Deborah A. Liptak
President, info2go

In a former life, Deb was a communications-electronics officer in the U.S. Air Force. Now, go to http://www.businessinformationresearchmethods.com and daliptak@sbcglobal.net.

The print article appears in the October 2009 issue of *Searcher: The Magazine for Database Professionals*. To purchase a PDF of the full article, go to www.iti-infocentral.com.

Chronology: *National Infrastructure Protection*

1963	National Communications System (NCS) established.
1982	National Security Telecommunications Advisory Committee (NSTAC) established.
1984	National Coordinating Center (NCC) established.
1988	Morris internet worm is an early example of a cyberattack.
	CERT Coordination Center (CERT/CC) established.
1995	Presidential Decision Directive (PPD) 39, *U.S. Policy on Counterterrorism* [http://www.fas.org/irp/offdocs/pdd39.htm]
	Critical Infrastructure Working Group, headed by the attorney general, makes recommendations to the president.
1996	Executive Order 13010, *Critical Infrastructure Protection* [http://www.fas.org/irp/offdocs/eo13010.htm], is the first national effort addressing the nation's critical vulnerabilities. It led to the formation of the President's Commission on Critical Infrastructure Protection (PCCIP).
1997	President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* [http://www.fas.org/sgp/library/pccip.pdf], identified five interconnected infrastructures and recommended a national strategy for protecting them from physical and cyberthreats.
1998	Presidential Decision Directive (PPD) 63, *Critical Infrastructure Protection*, [http://www.fas.org/irp/offdocs/pdd/pdd-63.htm], initiated a public-private partnership.
1999	General Accounting Office, *Comprehensive Strategy Can Draw on Year 2000 Experiences* [http://www.gao.gov/archive/2000/ai00001.pdf]
2000	*National Plan for Information Systems Protection, Version 1.0* [http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf]
2001	"Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities" [http://www.fas.org/irp/offdocs/pdd/CIP_2001_CongRept.pdf]
	Terrorist attacks on the World Trade Center and Pentagon, September 11, 2001
	Homeland Security Office established under Tom Ridge.
	Executive Order 13231, *Critical Infrastructure Protection, 2001* [http://www.ncs.gov/library/policy_docs/eo_13231.pdf]
	Critical Infrastructure Protection Board established under Richard Clark.
2002	*Critical Infrastructure Information Act of 2002*, Sections 721-724 of HR 5005, the Homeland Security Act of 2002 [http://www.dhs.gov/xlibrary/assets/CII_Act.pdf]
	Cyber Security Research and Development Act of 2002
2003	*National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* [http://www.whitehouse.gov/pcipb/physical_strategy.pdf]
	The National Strategy to Secure Cyberspace [http://www.whitehouse.gov/pcipb]
	Information Analysis and Infrastructure Protection (IAIP) directorate established.
	CAN-SPAM ACT: Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. § 7709 [http://uscode.house.gov/download/pls/15C103.txt]
2004	*National Response Plan* [http://www.dhs.gov/xlibrary/assets/NRPbaseplan.pdf]
2006	*National Asset Database* developed.
	Department of Homeland Security. *Procedures for Handling Critical Infrastructure Information*; Final Rule,

continued on page 2

2006 *continued from page 1*

FR Doc 06-7378 [http://edocket.access.gpo.gov/2006/pdf]/06-7378.pdf]

FY2006 Infrastructure Protection Program [http://www.dhs.gov/xlibrary/assets/FY2006IPPPressKit092506Final.pdf]

National Infrastructure Protection Plan (NIPP) 2006 [http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf]

2007 National Institute of Standards and Technology (NIST). *Guidelines on Securing Public Web Servers* [http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf]

April 27, 2007: Estonian CyberWar involved distributed denial of service attacks from Russian websites.

August 2007: Center for Strategic and International Studies (CSIS) establishes Commission on Cybersecurity for the 44th president [http://csis.org/program/commission-cybersecurity-44th-presidency] as a response to a wave of damaging attacks in cyberspace on the U.S.

Sept. 28 – Oct. 1, 2007: Burmese antigovernment protests result in Myanmar government cutting internet access.

2008 Commission to Assess the Threat to United States from Electromagnetic Pulse (EMP), Critical National Infrastructure [http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf]

January 2008: Defense Science Board (DSB) releases "Task Force on Strategic Communication in the 21st Century" [http://www.acq.osd.mil/dsb/reports/2008-01-Strategic_Communication.pdf].

Director of National Intelligence releases *Vision 2015: A Globally Networked and Integrated Intelligence Enterprise* [http://www.dni.gov/Vision_2015.pdf].

January 2008: U.S. Secret Service and CERT/SEI release *Insider Threat Study: Illicit Cyber Activity in the Government Sector* [www.cert.org/archive/pdf/insiderthreat_gov2008.pdf].

March 2008: *The National Security Strategy of the United Kingdom: Security in an interdependent world* presented to British Parliament [http://interactive.cabinetoffice.gov.uk/documents/security/national_security_strategy.pdf].

August 2008: South Ossetia War, also known as the Russia–Georgia War, included hacking of local servers and distributed denial of service.

October 2008: *National Cyber Security Awareness Month*

October 2008: Arbor Networks' "Worldwide Infrastructure Security Report, vol. IV" [http://www.arbornetworks.com/report] released.

Oct. 15, 2008: Georgia Tech Information Security Center (GTISC) releases "Emerging Cyber Threats Report for 2009: Data, Mobility and Questions of Responsibility Will Drive Cyber Threats in 2009 and Beyond" [http://www.gtisc.gatech.edu/pdf]/CyberThreatsReport2009.pdf].

November 2008: U.S. Department of Energy releases audit report, "Cyber Security Risk Management Practice at the Southeastern, Southwestern, and Western Area

November 2008 *continued*

Power Administrations DOE/IG-0805" [http://www.ig.energy.gov/documents/IG-0805.pdf].

December 2008: Center for Strategic and International Studies releases "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency" [http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf].

2009 **Jan. 18, 2009:** Kyrgyzstan experiences denial-of-service attacks originating in Russia.

Jan. 29, 2009: U.S. Department of Homeland Security releases *2009 National Infrastructure Protection Plan* [http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf].

February 2009: U.K.'s Chatham House releases *Cyber-Security and Politically, Socially and Religiously Motivated Cyber-Attacks* [http://www.chathamhouse.org.uk/files/13346_0209_eu_cybersecurity.pdf].

April 1, 2009: Senate Bill 773, *Cybersecurity Act of 2009*, introduced in U.S. Senate [http://thomas.loc.gov/cgi-bin/bdquery/z?d111:s.00773:].

April 29, 2009: National Research Council (NRC) releases *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* [http://www.nap.edu/catalog.php?record_id=12651].

May 1, 2009: Liberation Tigers of Tamil Eelam (LTTE) briefly hacked into the Sri Lankan Army and Sri Lanka Government's website, inserting gruesome pictures.

May 4, 2009: U.S. Department of Transportation releases the report "Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems FI-2009-049" [http://www.oig.dot.gov/StreamFile?file=/data/pdf]docs/ATC_Web_Report.pdf].

May 8, 2009: Gen. Kevin Chilton announces that the Law of Armed Conflict will apply to cyberwar.

May 11, 2009: Cyberwar Games conducted at West Point with help of National Security Agency.

May 29, 2009: White House announced Cybersecurity Policy Review and creation of White House Cybersecurity Office.

June 10, 2009: Georgia accuses Russia of jamming FM Radio.

June 16, 2009: Iranian election protests result in denial of service and censoring of the internet.

June 23, 2009: Defense Secretary Robert M. Gates announces the creation of the United States Cybercommand, nominating Lt. Gen. Keith Alexander, currently director of the National Security Agency, as commander.

June 27, 2009: Keesler AFB in Biloxi, Miss., selected for cybersecurity training.

July 4–9, 2009: Distributed denial of service and botnet cyberattacks against South Korean and United States government and commercial websites.

July 16, 2009: U.S. Department of Energy Argonne develops cyber Neighborhood Watch.

Reading List

Adams, Shar. "Cyber Threats Escalating Around the World," *The Epoch Times*, July 3, 2009 [http://www.theepochtimes.com/n2/content/view/19055].

"Al-Qaida plans cyber war against Britain: Top UK minister," *Times of India*, June 25, 2009 [http://timesofindia.indiatimes.com/World/UK/Al-Qaida-plans-cyber-war-against-Britain-Top-UK-minister/articleshow/4702632.cms].

Ambinder, Marc. "Six Things You Need To Know About Cyber," *Atlantic*, May 29 2009 [http://politics.theatlantic.com/2009/05/five_things_you_need_to_know_about_cyber.php].

"America's cybersecurity threat: The US is right to improve its cybersecurity defenses. But would it respond to cyber-attacks with military force?" *The Guardian*, June 1, 2009 [http://www.guardian.co.uk/commentisfree/cifamerica/2009/jun/01/obama-us-cybersecurity-tsar].

Arbor Networks' Worldwide Infrastructure Security Report, vol. IV. Arbor Networks, October 2008 [http://www.arbornetworks.com/report].

Arquilla, John and David Ronfeldt. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. RAND Corporation, 2001 [http://www.rand.org/publications/MR/MR1382].

Austin, Greg. *From Cyber-war to Cyber-peace: "Geek" Diplomacy is coming*. Brussels, Belgium: New Europe, June 7, 2009 [http://www.neurope.eu/articles/94607.php].

Baldor, Lolita C.

- "Air traffic systems vulnerable to cyber attack: Support systems have been breached by hackers in recent months," Associated Press, May 6, 2009 [http://www.msnbc.msn.com/id/30602242/ns/technology_and_science-security].
- "Pentagon girds for cyber warfare Attacks from well-funded nations, terror groups are biggest threats," Associated Press, May 7, 2009 [http://www.msnbc.msn.com/id/30630807].
- "U.S. use of cyber warfare needs more oversight," *Baltimore Sun*: April 30, 2009 [http://www.newsfactor.com/story.xhtml].?story_id=00100018OXI6&full_skip=1].

Brandt, Andrew. "The 10 Biggest Security Risks You Don't Know About," *PC World*, June 22, 2006 [http://www.pcworld.com/article/126083-1/article.html].

"Britain gets ready for cyber-war," *Brisbane Times*, June 27, 2009 [http://www.brisbanetimes.com.au/technology/britain-gets-ready-for-cyberwar-20090627-d035.html].

Budeiri, Ahmad. *Israel and foes in internet war*. Jerusalem: BBC Arabic, June 15, 2009 [http://news.bbc.co.uk/2/hi/middle_east/8079774.stm].

Center for History and New Media. *Critical Infrastructure Protection Digital Archive Bibliography* [http://chnm.gmu.edu/cipdigitalarchive/bibliography.php].

Center for Strategic and International Studies. "Securing Cyberspace for the 44th Presidency: A Report of the CSIS

continued

Commission on Cybersecurity for the 44th Presidency," Washington, DC: Center for Strategic and International Studies, December 2008 [http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf].

Chenard, Celeste. "Burma's cyber war rages on," *Mizzima News*, June 29, 2009 [http://www.mizzima.com/edop/commentary/2373-burmas-cyber-war-rages-on-.html].

China Turns Unix Into a Weapon. Strategy Page: May 14, 2009 [http://www.strategypage.com/htmw/htiw/20090514.aspx].

Choate, Trish. "Cyber training mission won't come to Texas," *Abilene Reporter News*: June 27, 2009.

Choe Sang-Hun and John Markoff. "Cyberattacks Hit U.S. and South Korean Web Sites," *The New York Times*: July 9, 2009.

Cohen, Reuven. "A Federal CloudBursting & Cyber Defense Contingency Plan: What are the legitimate responses available in America's arsenal?" Cloud Computing, July 10, 2009 [http://cloudcomputing.sys-con.com/node/1031271].

Coming to terms with cyber warfare. Cupertino, Calif.: *Security Focus*, June 17, 2009 [http://www.securityfocus.com/brief/972].

Corera, Gordon. *Cyber-security strategy launched*. BBC, 25 June 2009 [http://news.bbc.co.uk/2/hi/uk_news/politics/8118348.stm].

Crovitz, L. Gordon. "Obama and Cyber Defense Government should protect our e-infrastructure," *Wall Street Journal*, June 29, 2009 [http://online.wsj.com/article/SB124623073971766069.html].

Cryptome [http://cryptome.org].

"Cyber attacks lay bare S. Korea's security loopholes," *Yonhap News* (Seoul, South Korea), Jul 13, 2009 [http://www.tmcnet.com/usubmit/2009/07/13/4268922.htm].

"Cyber-Security and Politically, Socially and Religiously Motivated Cyber-Attacks," Chatham House, February 2009 [http://www.chathamhouse.org.uk/files/13346_0209_eu_cybersecurity.pdf].

Deleon, Nicholas. "Defcon founder named to Homeland Security Advisory Council," CrunchGear, June 6, 2009 [http://www.crunchgear.com/2009/06/06/defcon-founder-named-to-homeland-security-advisory-council].

Denning, D. *Information warfare and security*. New York: ACM Press; Reading, Mass.: Addison-Wesley, 1999.

Eaglen, MacKenzie and Rebecca Grant. *Commentary: A misguided quest to reform the Pentagon*. Washington, DC: The Heritage Foundation, June 23, 2009 [http://www.heritage.org/press/commentary/ed062309c.cfm].

Eaton, Kit. *Iranian Protests Becoming Crowd-Sourced Cyber War*. *Fast Company*, June 17, 2009 [http://www.fastcompany.com/blog/kit-eaton/technomix/iranian-protests-becoming-crowd-sourced-cyber-war-sorts].

"Emerging Cyber Threats Report for 2009: Data, Mobility and Questions of Responsibility will Drive Cyber," Federation of American Scientists. *Information Warfare and Information Security on the Web* [http://www.fas.org/irp/wwwinfo.html].

"Fending Off Attacks in Cyberspace," *The New York Times*, May 29, 2009 [http://roomfordebate.blogs.nytimes.com/2009/05/29/a-plan-of-attack-in-cyberspace].

Forsloff, Carol. "Terrorists Prepare for Cyber War," *Digital Journal*, Jun 19, 2009 [http://www.digitaljournal.com/article/274468].

Fox, Stuart. "Again with the Cyber War The media gets in on the cyberwar act," *Popular Science*, May 11, 2009 [http://www.popsci.com/military-aviation-amp-space/article/2009-05/again-cyber-war].

Fulghum, David A. "Network Attack Weapons Emerge," *Aviation Week*: May 21, 2009. http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/CYBER052109.xml].

Gardham, Duncan. "Al-Qaeda, China and Russia 'pose cyber war threat to Britain," *Telegraph*, June 25, 2009 [http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/5634820/Al-Qaeda-China-and-Russia-pose-cyber-war-threat-to-Britain-warns-Lord-West.html].

Tech Information Security Center (GTISC), *Threats in 2009 and Beyond*. Georgia Oct. 15, 2008 [http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf].

Georgetown University. *Dorothy Denning's Links* [http://www.cs.georgetown.edu/~denning/links.html].

Glenny, Misha. "NATO hawks are circling as the Web readies for tighter surveillance," *The Guardian*, June 30, 2009 [http://www.taipeitimes.com/News/editorials/archives/2009/06/30/2003447431].

Gorman, Siobhan. "Troubles Plague Cyberspy Defense," *The Wall Street Journal*: July 2, 2009, p. A1.

Gorman, Siobhan and Evan Ramstad. "Cyber Blitz hits U.S., Korea," *The Wall Street Journal*: July 8, 2009 [http://s.wsj.net/article/SB124701806176209691.html].

Gorman, Siobhan and Yochi Dreazen. "Military Command Is Created for Cyber Security," *The Wall Street Journal*, June 24, 2009, p. A6.

Harrowell, Alex. "What is cyberwar?" Paris, France: Agoravox, June 18, 2009 [http://www.agoravox.com/article.php/3?id_article=10166].

Harwood, Matthew. "Pentagon Plans New Military Command to Prepare for Cyber War," *Security Management*, May 29, 2009 [http://www.securitymanagement.com/news/pentagon-plans-new-military-command-prepare-cyberwar-005722].

"How Can Cyberspace Be Defended?" *National Journal*, June 8, 2009 [http://security.nationaljournal.com/2009/06/how-can-cyberspace-be-protecte.php].

"How secret guardians uphold online honor," Beijing,China: *People's Daily Online*, July 2, 2009 [http://english.peopledaily.com.cn/90001/90782/6691378.html].

Hughes, Michael. "U.S. should launch cyber attack against North Korea," *Examiner*, July 9, 2009 [http://www.examiner.com/x-4454-Chicago-Geopolitics-Examiner~y2009m7d9-US-should-launch-cyber-attack-against-North-Korea].

"IDF and Iran already Engaged in 'Cyber War,'" Israel National News, July 10, 2009 [http://www.israelnationalnews.com/News/Flash.aspx/167783].

"In cyber war, Pentagon may victimize privacy," Tehran, Iran: PRESS TV, June 13, 2009 [http://www.presstv.ir/detail.aspx?id=98031&sectionid=3510203].

India a Big Place Where Compromised Computers are Controlled. Copenhagen,Denmark: SPAMfighter News, April 29, 2009 [http://www.spamfighter.com/News-12273-India-a-Big-Place-Where-Compromised-Computers-are-Controlled.htm].

Information Warfare Monitor [http://www.infowar-monitor.net].

Infosecwriters.com [http://www.infosecwriters.com/texts.php].

Institute for the Advanced Study of Information Warfare. *Glossary of Information Warfare Terms*. Compiled by, Dr. Ivan K. Goldberg [http://www.psycom.net/iwar.2.html].

Institute for the Advanced Study of Information Warfare. *Information Warfare, I-War, IW, C4I, Cyberwar* [http://www.psycom.net/iwar.1.html].

"IRAN: Message from Tehran: 'I am scared and worried,'" *Los Angeles Times* blog, June 21, 2009

[http://latimesblogs.latimes.com/babylonbeyond/2009/06/iran-message-from-tehran-i-am-scared-and-worried.html].

IWS The Information Warfare Site [http://www.iwar.org.uk/iwar].

Jelinek, Pauline. "Is this cyber war? Possible US responses limited," The Associated Press, July 9, 2009 [http://news.yahoo.com/s/ap/20090710/ap_on_re_us/us_is_this_cyber_war].

Jones, Candice. "SA could face cyber war SA's strong ties with China places it at high risk of cyber war attacks," Gauteng, South Africa: ITWeb, May 29, 2009 [http://www.itweb.co.za/sections/internet/2009/0905291159.asp?A=BSR&S=BestRead&O=TB].

Kanalley, Craig. "Iran says West is waging 'cyber war,'" Chicago,IL: Breaking Tweets, June 22, 2009 [http://www.breakingtweets.com/2009/06/22/iran-says-west-is-waging-cyber-war].

Keesler to train for Cyber Command. Sun Herald: July 16, 2009 [http://www.sunherald.com/newsupdates/story/1480105.html].

Kilgannon, Corey and Noam Cohen. "US Cyberwar Games at West Point: Cadets Trade the Trenches for Firewalls," *The New York Times*, May 11, 2009 [http://www.nytimes.com/2009/05/11/technology/11cybergames.html].

Kim Ji-hyun. "Seoul suffers fallout from cyber attacks," *Korea Herald*, July 11, 2009 [http://www.koreaherald.co.kr/NEWKHSITE/data/html_dir/2009/07/11/200907110021.asp].

Kim So Yeol.

- "Defense Systems Hacking on the Increase," Seoul, South Korea: Daily NK, June 17, 2009 [http://www.dailynk.com/english/read.php?cataId=nk00100&num=5058].
- "North Korean Cyber War At Least Four Years Old!" Seoul, South Korea: Daily NK, July 13, 2009 [http://www.dailynk.com/english/read.php].?cataId=nk00100&num=5159].

"KOREA: The Generals Take Over Up North," US: Strategy Page, May 10, 2009 [http://www.strategypage.com/qnd/korea/articles/20090510.aspx].

Kyu-ho Shim and Jang, Ji-yung. "Blue House, this is cyber war," Seoul, South Korea: Etnews, July 10, 2009 [http://english.etnews.co.kr/news/detail.html?id=200907100002].

"Law of Armed Conflict to Apply to Cyberwar," US: Slashdot, May 08, 2009, posted by Soulskill [http://news.slashdot.org/article.pl?sid=09/05/08/2219258].

"LTTE won first round in the cyber war: Hacked Army and Lankapuwath websites — Army site restored," *Asian Tribune*, May 1, 2009 [http://www.asiantribune.com/oldsite2/%E2%80%9Dhttp://www.asiantribune.com/?q=node/17204].

Markoff, John.
- "Tracking Cyberspies Through the Web Wilderness," *The New York Times*: May 12, 2009.
- "Iranians and Others Outwit Net Censors," *The New York Times*, May 1, 2009 [http://www.nytimes.com/2009/05/01/technology/01filter.html].
- "Web's Anonymity Makes Cyberattack Hard to Trace," *The New York Times*: July 17, 2009.

Markoff, John and Andrew E. Kramer. "Cyberwar: U.S. and Russia Differ on a Treaty for Cyberspace," *The New York Times*: June 28, 2009.

Messmer, Ellen. "PC World Preparing for Cyberwar," *PC World*, May 16, 2009 [http://www.pcworld.com/businesscenter/article/165033/preparing_for_cyberwar.html].

Mills, Elinor. "Hacker named to Homeland Security Advisory Council," CNet, June 5, 2009 [http://news.cnet.com/8301-1009_3-10258634-83.html].

Monroe, John S. "Cyber Command: So much still to know, Questions linger about newest command," Falls Church, VA: FCW.com, Jul 2, 2009 [http://www.fcw.com/Articles/2009/07/06/buzz-cyber-command.aspx].

Moteff, J.
- "Critical Infrastructures: Background, Policy, and Implementation," Congressional Research Service; updated Oct.10, 2008 [http://www.fas.org/sgp/crs/homesec/RL30153.pdf].
- "Critical Infrastructures: The National Asset Database," Congressional Research Service; updated July 16, 2007 [http://www.fas.org/sgp/crs/homesec/RL33648.pdf].

"Nasty Things You Can Do On The Internet. US: Strategy Page, July 10, 2009 [http://www.strategypage.com/htmw/htweap/20090710.aspx].

National Research Council (NRC). "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities," National Academies Press, April 29, 2009 [http://www.nap.edu/catalog.php?record_id=12651].

Naughton, John. "The end of cyber-innocence," *The Guardian*, June 30, 2009, page 9 [http://www.taipeitimes.com/News/editorials/archives/2009/06/30/2003447430].

"NSA Chief Visit Raises Cyber War Spectre in NZ," New Zealand: Newsroom America, July 9, 2009 [http://www.newsroomamerica.com/leadstory/story.php?id=459681].

"NSA Wages Cyberwar Against US Armed Forces Teams," USA: Slashdot, May 11, 2009, posted by ScuttleMonkey [http://it.slashdot.org/article.pl?sid=09/05/11/1951204].

OpenNet Initiative http://opennet.net/
- "OpenNet Initiative Releases Report on Filtering in Asia," Open Net Blog, June 17, 2009 [http://opennet.net/blog/2009/06/oni-releases-reports-filtering-asia-china].

Prandato, John. "Cyberspace: The New Battlefield," *Across the Aisle*, June 24, 2009 [http://blog.psaonline.org/2009/06/24/cyberspace-the-new-battlefield].

Qiu Wei and Wen Xian. "Pentagon cyber command causes arms race concern," New York: Alibaba News Channel, June 24, 2009 [http://news.alibaba.com/article/detail/world/100123801-1-pentagon-cyber-command-causes-arms.html].

Ramasastry, Anita.
- "Tracking Every Move You Make, Part Two: Government Monitoring of Drivers' Cell Phones. FindLaw's Writ," October 2005 [http://writ.news.findlaw.com/ramasastry/20051019.html].
- "Every Move You Make, Part Three: Why Law Enforcement Should Have to Get a Warrant Before Tracking Us Via our Cell Phones," FindLaw's Writ. November 2005 [http://writ.news.findlaw.com/ramasastry/20051110.html].
- "Printers and Privacy: Why Government-Sponsored Printer Identification Raises Serious Privacy Concerns," FindLaw's Modern Practice. December 2005 [http://writ.news.findlaw.com/ramasastry/20051114.html].
- "Tracking Every Move You Make: Can Car Rental Companies Use Technology to Monitor Our Driving?" FindLaw's Writ. August 2005 [http://writ.news.findlaw.com/ramasastry/20050823.html].

Rhodes, Christopher. "Kyrgyzstan Knocked Offline," *The Wall Street Journal*, Jan. 28, 2009, p. A10 [http://online.wsj.com].

Richtel, Matt. "Live Tracking of Mobile Phones Prompts Court Fights on Privacy," *The New York Times,* Dec. 10, 2005 [http://www.nytimes.com/2005/12/10/technology/10phone.html].

Rollins, J. "Terrorist Capabilities for Cyberattack: Overview and Policy Issues," US Congressional Research Service; updated Jan. 27, 2007 [http://fas.org/sgp/crs/terror/RL33123.pdf] on Oct. 6, 2008.

"Russia Jams Georgian FM Radio Channels in Occupied Territories," Tbilisi, Georgia: The Financial, June 10, 2009 [http://www.finchannel.com/index.php].?option=com_content&task=view&id=39766&Itemid=2].

Salkever, Alex.
- "The Day the Net Nearly Choked," *Business Week*, Nov. 1, 2002 [http://www.businessweek.com/technology/content/oct2002/tc20021030_3147.htm].
- "Special Report: Military Technology. The Network Is the Battlefield," *BusinessWeek*, Jan. 7, 2003 [http://www.businessweek.com/technology/content/jan2003/tc2003017_2464.htm].

Sanger, David E. and Thom Shanker. "Pentagon Plans New Arm to Wage Wars in Cyberspace," *The New York Times*, May 29, 2009.

Schatz, Amy. "Obama CTO Addresses Cloud Computing, Cybersecurity," *The Wall Street Journal,* May 22, 2009.

Schneier, Bruce. "Counterpane: Attack Trends 2004 and 2005," *Queue*, June 2005.

Schogol, Jeff. "Official: No options 'off the table' for U.S. response to cyber attacks," *Stars and Stripes*, May 8, 2009 [http://www.stripes.com/article.asp?section=104&article=62555].

Shanker, Thom. "New Military Command for Cyberspace," *The New York Times:* June 24, 2009.

Shanker, Thom and David E. Sanger. "Privacy May Be a Victim in Cyberdefense Plan," *The New York Times*, June 12, 2009.

Singel, Ryan. "Is the Hacking Threat to National Security Overblown?" *Wired News*, June 3, 2009 [http://www.wired.com/threatlevel/2009/06/cyberthreat].

Sirak, Michael. "US vulnerable to EMP attack," Jane's Information Group, July 26, 2004.

Solomont, E. B. "Winning the propaganda war, in 140 characters or less," *Jerusalem Post*, June 17, 2009 [http://www.jpost.com/servlet/Satellite?cid=1245184859500&pagename=JPost%2FJPArticle%2FPrinter].

"Sri Lankan army says its website hacked by LTTE," *Hindustan Times*, May 1, 2009 [http://www.hindustantimes.com/StoryPage/StoryPage.aspx?sectionName=NLetter&id=f1aac7fa-2e4f-42aa-81c8-15f7d457b06c&Headline=Sri+Lankan+army+says+its+website+hacked+by+LTTE].

Stanford University. Cybersecurity Library [http://www.stanford.edu/class/msande91si/library.htm].

Sutton, Mark. "A new cyber arms race," Dubai, United Arab Emirates: ITP.net, June 2, 2009 [http:?/www.itp.net/blogs/850-a-new-cyber-arms-race].

Swartz, Jon. "New breed of cyberattack takes aim at sensitive data; Difficult-to-spot e-mails called 'corporate espionage,'" *USA TODAY*, Dec. 27, 2005 [http://www.usatoday.com/money/industries/technology/2005-12-26-cyber-attack-usat_x.htm].

Tohn, David. "Digital trench warfare," *Boston Globe*, June 11, 2009 [http://www.boston.com/bostonglobe/editorial_opinion/oped/articles/2009/06/11/digital_trench_warfare].

Underwood, Harry. "Pentagon prepares for cyberwar," Cheltenham, England, UK: First Post, May 29, 2009 [http://www.thefirstpost.co.uk/48055,news,pentagon-prepars-for-cyberwar].

United Kingdom. Cabinet Office, "The National Security Strategy of the United Kingdom: Security in an interdependent world" [http://interactive.cabinetoffice.gov.uk/documents/security/national_security_strategy.pdf].

U.S. Commission to Assess the Threat to United States from Electromagnetic Pulse (EMP), "Critical National Infrastructure" [http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf].

U.S. Congress
- "CAN-SPAM ACT. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)," *15 U.S.C. § 7709* [http://uscode.house.gov/download/pls/15C103.txt].
- Cyber Security Research and Development Act of 2002 [http://www4.law.cornell.edu/uscode/uscode15/usc_sup_01_15_10_100.html].

U.S. Defense Science Board: Task Force on Strategic Communication, "2007 Task Force on Strategic Communication Study" [http://www.acq.osd.mil/dsb/reports/2008-01-Strategic_Communication.pdf].

U.S. Department of Commerce
- Computer Security Resource Center [http://csrc.nist.gov/
- National Institute of Standards and Technology (NIST), "Guidelines on Securing Public Web Servers" [http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf].

U.S. Department of Defense
- Department of the Air Force, Air University: Air War College, "Information Operations, Warfare, Info Ops, Infowar, Cyberwar" [http://www.au.af.mil/info-ops/index.htm].
- Department of the Air Force, "Information operations theory, theories, communications theory" [http://www.au.af.mil/info-ops/theory.htm].
- "DOD Dictionary of Military and Associated Terms," JP 1–02, April 12, 2001. Amended March 17, 2008 [http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf].
- "Information Operations," JP 3–13, 2006 [http://information-retrieval.info/docs/DoD-IO.html].
- Joint Command, Control and Information Warfare School, Joint Forces Staff College. "Information Operations The Hard Reality of Soft Power," April 2004 [http://www.iwar.org.uk/iwar/resources/jiopc/io-textbook.pdf].
- "Joint Doctrine for Information Warfare," JP3–13, Oct 9, 1998; second draft revision Dec. 14, 2004. Accessed through the Federation of American Scientists, after being removed from the DOD website April 8, 2005 [http://www.fas.org/irp/doddir/dod/index.html].
- "Electronic Warfare," JP 3–13.1 [http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf].
- "Joint Doctrine for Information Operations," JP 3-13 [http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf].
- "Joint Doctrine for PSYOPS," JP 3-53 2003 [http://information-retrieval.info/docs/DoD-IO.html].
- Information Operations Related Documents [http://information-retrieval.info/docs/DoD-IO.html].
- "Military Deception, JP 3-13.4. July 2006 [http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13_4.pdf].
- *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd ed. rev. Alberts, David S. 1999 [http://www.dodccrp.org/files/Alberts_NCW.pdf].
- "Operations Security," JP 3–3.3. June 2006 [http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13_3.pdf].
- "Understanding Information Age Warfare" [http://www.dodccrp.org/files/Alberts_UIAW.pdf].

U.S. Department of Energy
- "Argonne Develops Program for Cyber Security 'Neighborhood Watch,'" U.S. Department of Energy, July 16, 2009 [http://www.prweb.com/releases/Argonne/Cyber_Security/prweb2650814.htm].
- Audit Report: "Cyber Security Risk Management Practice at the Southeastern, Southwestern, and Western Area Power Administrations DOE/IG-0805," U.S. Department of Energy, Office of Inspector General, Office of Audit Services: November 2008 [http://www.ig.energy.gov/documents/IG-0805.pdf].
- Computer Incident Advisory Capability [http://www.ciac.org/ciac].

U.S. Department of Homeland Security
- CERT Cyber Security Tip ST06-007. "Defending Cell Phones and PDAs Against Attack" [http://www.us-cert.gov/cas/tips/ST06-007.html].
- National Infrastructure Protection Plan (NIPP) 2006 [http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf].
- National Response Plan [http://www.dhs.gov/xlibrary/assets/NRPbaseplan.pdf].
- Office of Inspector General. Progress in Developing the National Asset Database [http://www.nytimes.com/packages/pdf]./politics/20060711_DHS.pdf].
- Procedures for Handling Critical Infrastructure Information; Final Rule, FR Doc 06-7378 [http://edocket.access.gpo.gov/2006/pdf]./06-7378.pdf].
- 2009 National Infrastructure Protection Plan. U.S. Department of Homeland Security, Office of Infrastructure Protection: January 29, 2009.http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf].

U.S. Department of Transportation. "Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems FI-2009-049" [http://www.oig.dot.gov/StreamFile?file=/data/pdf].docs/ATC_Web_Report.pdf].

U.S. Federal Trade Commission (FTC). "FTC's Cyber Security Site Gets an Upgrade: Makeover Marks National Cyber Security Awareness Month," Federal Trade Commission: Oct. 1, 2008 [http://www.ftc.gov/opa/2008/10/onguard.shtm].

U.S. General Accounting Office (GAO). "Cybersecurity for Critical Infrastructure Protection, Table 6: Threats to Critical Infrastructure," May 2004 [http://www.gao.gov/new.items/d04321.pdf].

U.S. Interagency OPSEC Support Staff (IOSS) [http://www.ioss.gov].

U.S. National Communications System. "Cyber Vulnerabilities within the National Infrastructure's Supervisory Control and Data Acquisition Systems," Evan T. Grim and Michael W. Raschke, Southwest Research Institute. May 2005 [http://www.ncs.gov/library/tech_bulletins/2005/tib_05-4.pdf].

U.S. National Coordination Office (NCO) for Networking and Information Technology Research and Development (NITRD). NCO Publications [http://www.nitrd.gov/pubs].

U.S. National Security Agency [http://www.nsa.gov].

U.S. Office of the Director of National Intelligence. "Vision 2015: A Globally Networked and Integrated Intelligence Enterprise" [http://www.dni.gov/Vision_2015.pdf].

U.S. Senate. Senate Bill 773. Cybersecurity Act of 2009, April 1, 2009 [http://thomas.loc.gov/cgi-bin/bdquery/z?d111:s.00773:].

U.S. White House.
- Cyberspace Policy Review: "Assuring a Trusted and Resilient Information and Communications Infrastructure," United States, Office of the White House: May 26, 2009 [http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf].
- Executive Order 13010, Critical Infrastructure Protection [http://www.fas.org/irp/offdocs/eo13010.htm].
- Executive Order 13231, Critical Infrastructure Protection, 2001 [http://www.ncs.gov/library/policy_docs/eo_13231].
- National Plan for Information Systems Protection, Version 1.0 [http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf].
- The National Strategy to Secure Cyberspace [http://www.whitehouse.gov/pcipb].
- National Strategy for the Physical Protection of Critical Infrastructures and Key Assets [http://www.whitehouse.gov/pcipb/physical_strategy.pdf].
- Presidential Decision Directive (PPD) 39. U.S. Policy on Counterterrorism [http://www.fas.org/irp/offdocs/pdd39.htm].
- Presidential Decision Directive (PPD) 63. Critical Infrastructure Protection [http://www.fas.org/irp/offdocs/pdd/pdd-63.htm].
- President's Commission on Critical Infrastructure Protection. Critical Foundations: Protecting America's Infrastructures [http://www.fas.org/sgp/library/pccip.pdf].
- Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities [http://www.fas.org/irp/offdocs/pdd/CIP_2001_CongRept.pdf].

U.S. Secret Service and CERT/SEI. "Insider Threat Study: Illicit Cyber Activity in the Government Sector" [http://www.cert.org/archive/pdf]./insiderthreat_gov2008.pdf].

"U.S. fights cyber war," Singapore: Straits Times, June 3, 2009 [http://www.straitstimes.com/Breaking%2BNews/World/Story/STIStory_385185.html].

"U.S. military recruiting 'hacker soldiers,'" Tehran, Iran: *PRESS TV*, May 31, 2009 [http://www.presstv.ir/detail.aspx?id=96621&sectionid=3510203].

Walsh, Larry. "Cyberwar Arms Race May Create New Channel Opportunities," New York, NY: Channel Insider, June 2, 2009 [http://www.channelinsider.com/c/a/Security/Cyberwar-Arms-Race-May-Create-New-Channel-Opportunities-239793].

Vegh, S. "Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking," First Monday. October 2002 [http://www.firstmonday.org/issues/issue7_10/vegh].

"What rules apply in cyber-wars?" UK: BBC News, Jun 21, 2009 [http://128.100.171.10/modules.php].?op=modload&name=News&file=article&sid=2375].

"What's Lincoln Group?" GovExec.com; Dec. 1, 2005 [http://www.govexec.com/story_page.cfm?articleid=32892].

Wilson, Clay. "Network Centric Warfare background and oversight issues for Congress," Congressional Research Service, June 2, 2004. Updated March 15, 2007 [http://www.fas.org/sgp/crs/natsec/RL32411.pdf].

Zhuang, F. and J. Tygar. "Keyboard Acoustic Emanations Revisited," *Proceedings of the 12th ACM Conference on Computer and Communications Security.* University of California–Berkeley, 2005 [http://www.cs.berkeley.edu/~tygar/papers/Keyboard_Acoustic_Emanations_Revisited/ccs.pdf].