

# References

- Abdo, Alex. "You May Have 'Nothing to Hide' But You Still Have Something to Fear." American Civil Liberties Union Blog of Rights. August 2, 2013. Retrieved May 17, 2014, from <https://www.aclu.org/blog/national-security/you-may-have-nothing-hide-you-still-have-something-fear>.
- Abrams, Lawrence. "CryptoLocker Ransomware Information Guide and FAQ." December 20, 2014. Retrieved March 30, 2014, from <http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information>.
- Abrams, Marshall D., and Joe Weiss. "Malicious Control System Cyber Security Attack Case Study—Maroochy Water Services, Australia." August 2008. Retrieved May 1, 2014, from [http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study\\_briefing.pdf](http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_briefing.pdf).
- Adair, Steven, and Ned Moran. "Cyber Espionage & Strategic Web Compromises—Trusted Websites Serving Dangerous Results." May 15, 2012. Retrieved May 19, 2014, from <http://blog.shadowserver.org/2012/05/15/cyber-espionage-strategic-web-compromises-trusted-websites-serving-dangerous-results/>.
- Aid, Matthew M. "Inside the NSA's Ultra-Secret China Hacking Group." *Foreign Policy*, June 10, 2013. Retrieved March 10, 2014, from [http://www.foreignpolicy.com/articles/2013/06/10/inside\\_the\\_nsa\\_s\\_ultra\\_secret\\_china\\_hacking\\_group](http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group).
- Alexander, Keith B. "Statement of General Keith B. Alexander Commander United States Cyber Command Before the Senate Committee on Armed Services." Defense.gov. March 12, 2013. Retrieved June 1, 2014, from [http://www.defense.gov/home/features/2013/0713\\_cyberdomain/docs/Alexander%20testimony%20March%202013.pdf](http://www.defense.gov/home/features/2013/0713_cyberdomain/docs/Alexander%20testimony%20March%202013.pdf).
- . "Statement of General Keith B. Alexander Commander United States Cyber Command Before the Senate Committee on Armed Services." Defense Innovation Marketplace. February 27, 2014. Retrieved May 11, 2014, from [http://www.defenseinnovationmarketplace.mil/resources/Cyber\\_Command\\_Alexander\\_02-27-14.pdf](http://www.defenseinnovationmarketplace.mil/resources/Cyber_Command_Alexander_02-27-14.pdf).
- Alford, Lionel D. "Cyber Warfare: The Threat to Weapons Systems." *Weapon Systems Technology Information Analysis Center Quarterly* 9, no. 4. Retrieved April 29, 2014, from [https://wstiac.alionscience.com/pdf/WQV9N4\\_ART01.pdf](https://wstiac.alionscience.com/pdf/WQV9N4_ART01.pdf).
- Alperovitch, Dmitri. "Active Defense: Time for a New Security Strategy." February 25, 2013. Retrieved May 12, 2014, from <http://www.crowdstrike.com/blog/active-defense-time-new-security-strategy/>.
- . "Revealed: Operation Shady RAT." Vers. 1.1. McAfee Web site. August 8, 2011. Retrieved March 23, 2014, from <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>.
- Anderson, Nate. "'Operation Payback' Attacks to Go on Until 'We Stop Being Angry.'" Ars Technica Web site. September 30, 2010. Retrieved May 5, 2014, from <http://arstechnica.com/tech-policy/2010/09/operation-payback-attacks-continue-until-we-stop-being-angry/>.

- Anderson, Ross. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2nd ed. New York: John Wiley & Sons, Inc., 2008.
- Applebaum, Jacob, Judith Horchert, and Christian Stocker. "Shopping for Spy Gear: Catalog Advertises NSA Toolbox." *Der Spiegel*, December 29, 2013. Retrieved March 23, 2014, from <http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html>.
- Applegate, Scott D. "The Principle of Maneuver in Cyberspace Operations." *4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2012, 183–195.
- Arquilla, John. Interview with FRONTLINE. March 4, 2003. Transcript retrieved on May 3, 2014, from <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html>.
- Arquilla, John, and David Ronfeldt. "Cyberwar Is Coming!" Spring 1993. Retrieved June 1, 2014, from [http://www.rand.org/content/dam/rand/pubs/monograph\\_reports/MR880/MR880.ch2.pdf](http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch2.pdf).
- Arquilla, John, and David F. Ronfeldt. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: Rand, 2001.
- Bamford, James. *Body of Secrets*. New York: Anchor Books, 2002.
- Banks, William. "The Role of Counterterrorism Law in Shaping ad Bellum Norms for Cyber Warfare." *International Law Studies* (U.S. Naval War College) 89 (April 2013): 157–197.
- Bencsath, Boldizsar et al. "Duqu: A Stuxnet-like Malware Found in the Wild." Laboratory of Cryptography and System Security (CrySyS). October 14, 2011. Retrieved May 4, 2014, from <http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf>.
- Bender, Jason M. "The Cyberspace Operations Planner." Small Wars Journal Web site. November 5, 2013. Retrieved May 18, 2014, from <http://smallwarsjournal.com/jrnl/art/the-cyberspace-operations-planner>.
- Bennett, James T., Ned Moran, and Nart Villeneuve. "Poison Ivy: Assessing Damage and Extracting Intelligence." FireEye Labs blog. August 21, 2013. Retrieved March 26, 2014, from <http://www.fireeye.com/resources/pdfs/fireeye-poison-ivy-report.pdf>.
- Blank, Laurie R. "International Law and Cyber Threats from Non-State Actors." *International Law Studies* 89 (2013): 406–437.
- Borger, Julian. "Hacking Trail Leads to Swedish Teen." *The Guardian*, May 10, 2005. Retrieved May 4, 2014, from <http://www.theguardian.com/technology/2005/may/11/usnews.internationalnews>.
- Braun, Stephen. "U.S. Network to Scan Workers with Secret Clearances." The Associated Press, March 10, 2014. Retrieved March 12, 2014, from [http://hosted.ap.org/dynamic/stories/U/US\\_EYES\\_ON\\_SPIES](http://hosted.ap.org/dynamic/stories/U/US_EYES_ON_SPIES).
- Brown, Anthony Cave. *Bodyguard of Lies: The Extraordinary True Story Behind D-Day*. New York: Lyons Press, 2007.
- Burgess, Ronald L. Remarks to the Association of Former Intelligence Officers. August 12, 2011. Retrieved May 23, 2014, from <https://web.archive.org/web/20131004054724/http://www.dia.mil/public-affairs/testimonies/2011-08-12.html>.
- Butler, Sean C. "Refocusing Cyber Warfare Thought." *Air & Space Power Journal* (2013): 44–57. Retrieved May 24, 2014, from <http://www.airpower.maxwell.af.mil/digital/pdf/articles/Jan-Feb-2013/F-Butler.pdf>.
- Center for Strategic and International Studies Defense-Industrial Initiatives Group. "An Assessment of the National Security Software Industrial Base." Center for Strategic and International Studies Web site. October 19, 2006. Retrieved April 27, 2014, from [https://csis.org/files/media/csis/pubs/061019\\_softwareindustrialbase.pdf](https://csis.org/files/media/csis/pubs/061019_softwareindustrialbase.pdf).

- Central Intelligence Agency. "Centers in the CIA." June 18, 2013. Retrieved May 23, 2014, from <https://www.cia.gov/library/publications/additional-publications/the-work-of-a-nation/cia-director-and-principles/centers-in-the-cia.html>.
- Cialdini, Robert. *Influence: Science and Practice*. 5th ed. Boston: Allyn & Bacon, 2008.
- Clapper, James R. "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community: Senate Select Committee on Intelligence." Office of the Director of National Intelligence. Washington, DC, March 12, 2013. Retrieved March 10, 2014, from <http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf>.
- . "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community: Senate Select Committee on Intelligence." Office of the Director of National Intelligence. Washington, DC, January 29, 2014. Retrieved March 12, 2014, from [http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR\\_SSCI\\_29\\_Jan.pdf](http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf).
- Committee on National Security Systems. "CNSS Instruction 1253." CNSS Web site. March 27, 2014. Retrieved May 13, 2014, from <https://www.cnss.gov/CNSS/openDoc.cfm?UoK1JHI3+7FhQcOk1ZPE4A==>.
- Constantin, Lucian. "Researchers Identify Stuxnet-like Cyberespionage Malware Called 'Flame.'" *PCWorld*, May 28, 2012. Retrieved February 27, 2014, from [http://www.pcworld.com/article/256370/researchers\\_identify\\_stuxnetlike\\_cyberespionage\\_malware\\_called\\_flame.html](http://www.pcworld.com/article/256370/researchers_identify_stuxnetlike_cyberespionage_malware_called_flame.html).
- Convertino, Sebastian. "Flying and Fighting in Cyberspace." July 2007. Air University.
- Conway, Tom. "DoD Can Use USB Securely." McAfee blogs. March 9, 2010. Retrieved May 27, 2014, from <http://blogs.mcafee.com/business/security-connected/dod-can-use-usb-securely>.
- Cooney, Michael. "Healthcare Industry Group Builds Cybersecurity Threat Center." April 24, 2012. Retrieved June 8, 2014, from <http://www.networkworld.com/article/2187972/data-center/healthcare-industry-group-builds-cybersecurity-threat-center.html>.
- . "Statement of General Keith B. Alexander Commander United States Cyber Command Before the Senate Committee on Armed Services." Defense Innovation Marketplace. February 27, 2014. Retrieved May 11, 2014, from [http://www.defenseinnovationmarketplace.mil/resources/Cyber\\_Command\\_Alexander\\_02-27-14.pdf](http://www.defenseinnovationmarketplace.mil/resources/Cyber_Command_Alexander_02-27-14.pdf).
- Corbin, Jane. Cyber Attack! Interview with Senator John Kyl. British Broadcasting Company. June 3, 2000. Transcript retrieved on May 3, 2014, from [http://news.bbc.co.uk/hi/english/static/audio\\_video/programmes/panorama/transcripts/transcript\\_03\\_07\\_00.txt](http://news.bbc.co.uk/hi/english/static/audio_video/programmes/panorama/transcripts/transcript_03_07_00.txt).
- Crowdstrike. "Crowdstrike Global Threat Report: 2013 Year in Review." Crowdstrike Web site. January 22, 2014. Retrieved March 19, 2014, from [https://s3.amazonaws.com/download.crowdstrike.com/papers/CrowdStrike\\_Global\\_Threat\\_Report\\_2013.pdf](https://s3.amazonaws.com/download.crowdstrike.com/papers/CrowdStrike_Global_Threat_Report_2013.pdf).
- Danchev, Dancho. "The Russian Business Network." Dancho Danchev's blog. October 18, 2007. Retrieved April 23, 2014, from <http://ddanchev.blogspot.com/2007/10/russian-business-network.html>.
- Deeks, Ashley. "The Geography of Cyber Conflict: Through a Glass Darkly." *International Law Studies* 89 (2013): 1–20.
- Defense Information Systems Agency. "CNDSP Subscription Services." disa.mil Web site. 2014. Retrieved May 13, 2014, from <http://www.disa.mil/Services/Information-Assurance/CNDSP>.
- . "Continuous Monitoring and Risk Scoring." Retrieved May 22, 2014, from <http://www.disa.mil/Services/Information-Assurance/CMRS>.

- . “Frequently Asked Questions: DoD Policy Memorandum ‘Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media.’” DISA Information Assurance Support Environment. March 19, 2008. Retrieved May 27, 2014, from [http://iase.disa.mil/policy-guidance/faq\\_dar\\_encryption\\_policy\\_memo\\_18mar08\\_update-6\\_final.doc](http://iase.disa.mil/policy-guidance/faq_dar_encryption_policy_memo_18mar08_update-6_final.doc).
- . “Host Based Security System: Components.” DISA Web site. n.d. Retrieved April 29, 2014, from <http://www.disa.mil/Services/Information-Assurance/HBSS/Components>.
- . “Network Defense.” *disa.mil* Web site. 2014. Retrieved May 13, 2014, from <http://www.disa.mil/Services/Information-Assurance/CNDSP>.
- Defense Logistics Agency. “Data Loss Prevention Solicitation.” September 2011. Retrieved May 24, 2014, from [https://www.fbo.gov/?s=opportunity&mode=form&tab=core&id=bd9cb808b5bd73f37dd74390455560ad&\\_cview=0](https://www.fbo.gov/?s=opportunity&mode=form&tab=core&id=bd9cb808b5bd73f37dd74390455560ad&_cview=0).
- . “HBSS Components.” DISA Web site. n.d. Retrieved May 27, 2014, from <http://www.disa.mil/Services/Information-Assurance/HBSS/Components>.
- Defense Science Board. “Resilient Military Systems and the Advanced Cyber Threat.” ACQ Web. January 2013. Retrieved May 18, 2014, from <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>.
- Defense Systems. “Al-Qaeda Reportedly Targeting U.S. Drones.” Defense Systems Web site. September 2013. Retrieved April 27, 2014, from <http://defensesystems.com/articles/2013/09/05/counter-drone.aspx>.
- Dennesen, Kristen, John Feker, Tonya Feyes, and Sean Kern. *Strategic Cyber Intelligence*. Intelligence and National Security Alliance Cyber Intelligence Task Force, March 2014. Retrieved March 27, 2014, from <http://www.insaonline.org/i/d/a/Resources/StrategicCyber.aspx>.
- Department of the Navy. “Computer Network Defense Roadmap.” May 2009. Retrieved March 29, 2014, from <http://www.doncio.navy.mil/uploads/1019TSI85933.pdf>.
- DISA Field Security Operations. “Enclave Security Technical Implementation Guide, Version 4, Release 4.” DISA Information Assurance Support Environment. January 9, 2014. Retrieved March 18, 2014, from [http://iase.disa.mil/stigs/net\\_perimeter/enclave\\_dmzs/u\\_enclave\\_v4r4\\_stig.zip](http://iase.disa.mil/stigs/net_perimeter/enclave_dmzs/u_enclave_v4r4_stig.zip).
- Dorp, Evan. “CryptoLocker—A New Ransomware Variant.” Emsisoft blog. September 10, 2013. Retrieved March 30, 2014, from <http://blog.emsisoft.com/2013/09/10/cryptolocker-a-new-ransomware-variant/>.
- Drogin, Bob. “NSA Blackout Reveals Downside of Secrecy.” *Los Angeles Times*, March 13, 2000. Retrieved May 3, 2014, from <https://www.fas.org/irp/news/2000/03/e20000313nsa.htm>.
- Dvorak, Daniel L., ed. “NASA Study on Flight Software Complexity.” NASA Web site. March 5, 2009. Retrieved April 27, 2014, from [http://www.nasa.gov/pdf/418878main\\_FSWC\\_Final\\_Report.pdf](http://www.nasa.gov/pdf/418878main_FSWC_Final_Report.pdf).
- Elkjaer, Bo, and Kenan Seeberg. “Echelon Singles Out the Red Cross.” Cryptome. March 8, 2000. Retrieved May 17, 2014, from <http://cryptome.org/echelon-red.htm>.
- “Eligible Receiver.” GlobalSecurity.org. Retrieved May 4, 2014, from <http://www.globalsecurity.org/military/ops/eligible-receiver.htm>.
- Fahrenkrug, David T. “Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy.” *4th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE Publications, 2012, 197–207.
- Federal Bureau of Investigation. “Intelligence Cycle.” n.d. Retrieved March 22, 2014, from <http://www.fbi.gov/about-us/intelligence/intelligence-cycle>.

- . “Safety and Security for the Business Professional Traveling Abroad.” n.d. Retrieved May 17, 2014, from <http://www.fbi.gov/about-us/investigate/counterintelligence/business-travel-brochure>.
- . “U.S. Charges Five Chinese Military Hackers with Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage.” May 19, 2014. Retrieved June 8, 2014, from <http://www.fbi.gov/pittsburgh/press-releases/2014/u.s.-charges-five-chinese-military-hackers-with-cyber-espionage-against-u.s.-corporations-and-a-labor-organization-for-commercial-advantage/>.
- Ferrer, Zarestel, and Methusela Cebrian Ferrer. “In-Depth Analysis of Hydraq: The Face of Cyberwar Enemies Unfolds.” Computer Associates Web site. 2010. Retrieved March 23, 2014, from [http://www.ca.com/us/~/media/files/securityadvisornews/in-depth\\_analysis\\_of\\_hydraq\\_final\\_231538.aspx](http://www.ca.com/us/~/media/files/securityadvisornews/in-depth_analysis_of_hydraq_final_231538.aspx).
- Field Manual 2-0: Intelligence*. Washington, DC: Department of the Army, May 17, 2004. Retrieved March 23, 2014, from <http://www.globalsecurity.org/intell/library/policy/army/fm/2-0/index.html>.
- Field Manual 3-05.30: Psychological Operations*. Washington, DC: Department of the Army, April 2005. Retrieved March 10, 2014, from <http://www.fas.org/irp/doddir/army/fm3-05-30.pdf>.
- Field Manual 34-52: Intelligence Interrogation*. Washington, DC: Department of the Army, September 28, 1992. Retrieved March 23, 2014, from [http://www.loc.gov/rr/frd/Military\\_Law/pdf/intel\\_interrogation\\_sept-1992.pdf](http://www.loc.gov/rr/frd/Military_Law/pdf/intel_interrogation_sept-1992.pdf).
- “Follow the Money: NSA Spies on International Payments.” *Der Spiegel*, September 15, 2013. Retrieved March 23, 2014, from <http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html>.
- Foster, Peter. “‘Bogus’ AP Tweet About Explosion at the White House Wipes Billions Off US Markets.” *The Telegraph*, April 23, 2013. Retrieved May 17, 2014, from <http://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html>.
- FoxIT. “Black Tulip: Report of the Investigation into the DigiNotar Certificate Authority Breach.” August 13, 2012. Retrieved April 6, 2014, from <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf>.
- “Frontline Interview with John Hamre.” PBS Web site. February 18, 2003. Retrieved May 18, 2014, from <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/hamre.html>.
- Fryer-Biggs, Zachary. “DoD’s New Cyber Doctrine.” *Defense News*, October 13, 2012. Retrieved May 24, 2014, from <http://www.defensenews.com/article/20121013/DEFREG02/310130001/DoD-8217-s-New-Cyber-Doctrine>.
- Fulghum, David A. “Black Surprises.” *Aviation Week and Space Technology* 162, no. 7 (February 14, 2005): 68–69.
- Gellman, Barton, and Ashkan Soltani. “NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say.” *Washington Post*, October 30, 2013. Retrieved March 9, 2014, from [http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd\\_story.html](http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html).
- Gentry, Craig. “A Fully Homomorphic Encryption Scheme.” Doctoral Thesis, Computer Sciences, Palo Alto: Stanford University, 2009.

- Gentry, Craig, and Shai Halevi. "Implementing Gentry's Fully-Homomorphic Encryption Scheme." *Advances in Cryptology—EUROCRYPT 2011*, 2011: 129–148.
- Gertz, Bill. "Commander: U.S. Military Not Ready for Cyber Warfare." The Washington Free Beacon Web site. February 27, 2014. Retrieved May 11, 2014, from <http://freebeacon.com/national-security/commander-u-s-military-not-ready-for-cyber-warfare/>.
- Google. "A New Approach to China." Google Official blog Web site. January 12, 2010. Retrieved March 23, 2014, from <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>.
- Goodchild, Joan. "The Robin Sage Experiment: Fake Profile Fools Security Pros." NetworkWorld Web site. July 8, 2010. Retrieved April 7, 2014, from <http://www.networkworld.com/news/2010/070810-the-robin-sage-experiment-fake.html>.
- Gorman, Siobhan, Yochi J. Dreazen, and August Cole. "Insurgents Hack U.S. Drones." *Wall Street Journal*, December 17, 2009. Retrieved March 1, 2014, from <http://online.wsj.com/news/articles/SB126102247889095011>.
- Graham, Bradley. "Hackers Attack Via Chinese Web Sites." *Washington Post*, August 25, 2005. Retrieved May 4, 2014, from <http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html>.
- Greenberg, Andy. "Hackers Reveal Nasty New Car Attacks—With Me Behind the Wheel." *Forbes*, July 24, 2013. Retrieved June 3, 2014, from <http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/>.
- . "How the Syrian Electronic Army Hacked Us: A Detailed Timeline." *Forbes*, February 20, 2014. Retrieved March 4, 2014, from <http://www.forbes.com/sites/andygreenberg/2014/02/20/how-the-syrian-electronic-army-hacked-us-a-detailed-timeline/>.
- Greene, Thomas C. "Chapter One: Kevin Mitnick's Story: Here It Is." *The Register*, January 13, 2003. Retrieved April 19, 2014, from [http://www.theregister.co.uk/2003/01/13/chapter\\_one\\_kevin\\_mitnicks\\_story/](http://www.theregister.co.uk/2003/01/13/chapter_one_kevin_mitnicks_story/).
- Greenwald, Glenn. "NSA Collecting Phone Records of Millions of Verizon Customers Daily." *The Guardian*, June 5, 2013. Retrieved March 23, 2014, from <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.
- Greenwald, Glenn, and Ewan MacAskill. "NSA Prism Program Taps into User Data of Apple, Google and Others." *The Guardian*, June 6, 2013. Retrieved May 17, 2014, from <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.
- Grow, Brian, and Mark Hosenball. "Special Report: In Cyberspy vs. Cyberspy, China Has the Edge." Reuters. April 14, 2011. Retrieved May 4, 2014, from <http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTRE73D24220110414?pageNumber=1>.
- Hagen, Christian, and Jeff Sorenson. "Delivering Military Software Affordably." *Defense AT&L Magazine* (March/April 2013): 30–34.
- Halperin, Daniel, et al. "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero Power Defenses." Retrieved April 28, 2014, from <http://www.secure-medicine.org/public/publications/icd-study.pdf>.
- Hang, Teo Cheng. "Non-Kinetic Warfare: The Reality and the Response." Singapore Ministry of Defense. 2010. Retrieved April 19, 2014, from [http://www.mindef.gov.sg/imindef/publications/pointer/journals/2010/v36n1/feature5/\\_jcr\\_content/imindefPars/0003/file.res/Pointer%20V36N1%20inside%2045-57.pdf](http://www.mindef.gov.sg/imindef/publications/pointer/journals/2010/v36n1/feature5/_jcr_content/imindefPars/0003/file.res/Pointer%20V36N1%20inside%2045-57.pdf).
- Hansen, Marc, and Robert F. Nesbit. *Report of Defense Science Board Task Force on Defense Software*. Advisory Report, Washington, DC: Defense Science Board, 2000.
- Harris, Shane. "Hack Attack." ForeignPolicy.com. March 3, 2014. Retrieved June 17, 2014, from [http://www.foreignpolicy.com/articles/2014/03/03/hack\\_attack](http://www.foreignpolicy.com/articles/2014/03/03/hack_attack).

- . “Inside the FBI’s Fight Against Chinese Cyber-Espionage.” *ForeignPolicy.com*. May 27, 2014. Retrieved June 1, 2014, from [http://www.foreignpolicy.com/articles/2014/05/27/exclusive\\_inside\\_the\\_fbi\\_s\\_fight\\_against\\_chinese\\_cyber\\_espionage](http://www.foreignpolicy.com/articles/2014/05/27/exclusive_inside_the_fbi_s_fight_against_chinese_cyber_espionage).
- Hayden, Michael. Address to Kennedy Political Union of American University. February 17, 2000. Transcript retrieved on May 3, 2014, from <http://www.fas.org/irp/news/2000/02/dir021700.htm>.
- Healey, Jason, and Karl Frindal (editors). *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association, June 2013.
- “Heartbleed Bug.” *Heartbleed.com*. April 29, 2014. Retrieved May 13, 2014, from <http://heartbleed.com/>.
- Holmes, James, and John Posner. “Presentation to the House Armed Services Committee Subcommittee on Tactical Air and Land Forces U.S. House of Representatives.” March 20, 2012. Retrieved May 23, 2014, from [http://armedservices.house.gov/index.cfm/files/serve?File\\_id=2cb71c16-223f-4421-8272-279666f034ce](http://armedservices.house.gov/index.cfm/files/serve?File_id=2cb71c16-223f-4421-8272-279666f034ce).
- Hoover, J. Nicholas. “Stolen VA Laptop Contains Personal Data.” *Dark Reading Web site*. May 14, 2010. Retrieved May 27, 2014, from <http://www.darkreading.com/risk-management/stolen-va-laptop-contains-personal-data/d/d-id/1089135>.
- Howard, Michael, and David LeBlanc. *Writing Secure Code*. 2nd ed. Redmond: Microsoft Press, 2002.
- HP Security Research. “Companion to HPSR Threat Intelligence Podcast Episode 11.” HP Security Research blog. February 2014. Retrieved March 26, 2014, from <http://h30499.www3.hp.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/177/1/Companion%20to%20HPSR%20Threat%20Intelligence%20Briefing%20Episode%2011%20Final.pdf>.
- “H.R. 1960—113th Congress: National Defense Authorization Act for Fiscal Year 2014.” U.S. Government Printing Office. July 8, 2013. Retrieved April 14, 2014, <http://www.gpo.gov/fdsys/pkg/BILLS-113hr1960pcs/pdf/BILLS-113hr1960pcs.pdf>.
- Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.” *6th Annual International Conference on Information Warfare & Security*. Washington, DC: Academic Publishing International Limited, 2011.
- “Information Operations Roadmap.” Washington, DC: Department of Defense, October 30, 2003. Retrieved March 10, 2014, from [http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info\\_ops\\_roadmap.pdf](http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf).
- InformationWeek. “Cloud Providers Align With FedRAMP Security Standards.” January 21, 2014. Retrieved June 7, 2014, from <http://www.informationweek.com/government/cybersecurity/cloud-providers-align-with-fedramp-security-standards/d/d-id/1113499>.
- Internet Crime Complaint Center. “CryptoLocker Ransomware Encrypts User’s Files.” October 28, 2013. Retrieved May 17, 2014, from <http://www.ic3.gov/media/2013/131028.aspx>.
- Israeli Defense Forces. “Yesterday the IDF Thwarted Cyber Attack; Today the IDF General Speaks About Future of Cyber Warfare.” April 8, 2014. Retrieved June 1, 2014, from <http://www.idfblog.com/2014/04/08/future-cyber-warfare-speech-head-idf-telecommunications-branch/>.
- Jardin, Xeni. “Prominent Tibetan Dissident Blogger Hacked, Impersonated on Skype.” *Boing Boing*. May 28, 2008. Retrieved May 3, 2014, from <http://boingboing.net/2008/05/28/prominent-tibetan-di.html>.
- Jensen, Eric Talbot. “Cyber Attacks: Proportionality and Precautions in Attack.” *International Law Studies* 89 (2013): 198–217.
- “Joint Publication 2-0: Joint Intelligence.” Washington, DC: Joint Chiefs of Staff, October 22, 2013. Retrieved March 22, 2014, from [http://www.dtic.mil/doctrine/new\\_pubs/jp2\\_0.pdf](http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf).

- "Joint Publication 3-13: Information Operations." Washington, DC: Joint Chiefs of Staff, February 13, 2006. Retrieved March 10, 2014, from [http://www.carlisle.army.mil/DIME/documents/jp3\\_13.pdf](http://www.carlisle.army.mil/DIME/documents/jp3_13.pdf).
- "Joint Publication 3-13.1: Electronic Warfare." Washington, DC: Joint Chiefs of Staff, January 25, 2007. Retrieved March 10, 2014, from <http://www.fas.org/irp/doddir/dod/jp3-13-1.pdf>.
- "Joint Publication 3-13.3: Operations Security." Washington, DC: Joint Chiefs of Staff, January 4, 2012. Retrieved March 10, 2014, from [http://www.jfsc.ndu.edu/schools\\_programs/jc2ios/io/student\\_readings/1C2\\_JP\\_3-13-3\\_OPSEC\\_Process.pdf](http://www.jfsc.ndu.edu/schools_programs/jc2ios/io/student_readings/1C2_JP_3-13-3_OPSEC_Process.pdf).
- "Joint Publication 3-60: Joint Targeting." Washington, DC: Joint Chiefs of Staff, January 31, 2013. Retrieved March 30, 2014, from [http://www.fas.org/irp/doddir/dod/jp3\\_60.pdf](http://www.fas.org/irp/doddir/dod/jp3_60.pdf).
- Kahn, David. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Rev. Sub. ed. New York: Scribner, 1996.
- Kahn, David. *Seizing the Enigma: The Race to Break the German U-Boats Codes, 1939–1943*. Boston: Houghton Mifflin, 1991.
- Kan, Michael. "China Accuses Cisco of Supporting US Cyberwar Efforts." May 27, 2014. Retrieved June 8, 2014, from [http://www.computerworld.com/s/article/9248595/China\\_accuses\\_Cisco\\_of\\_supporting\\_US\\_cyberwar\\_efforts](http://www.computerworld.com/s/article/9248595/China_accuses_Cisco_of_supporting_US_cyberwar_efforts).
- Kaplan, David A. "Suspensions and Spies in Silicon Valley." *Newsweek*, September 17, 2006. Retrieved April 19, 2014, from <http://www.newsweek.com/suspensions-and-spies-silicon-valley-109827>.
- Kelley, Michael. "The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought." *Business Insider*, November 20, 2013. Retrieved May 4, 2014, from <http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previously-thought-2013-11#lfUEr>.
- Kissel, Richard, Matthew Scholl, Steven Skolochenko, and Xing Li. "NIST Special Publication 800-88: Guidelines for Media Sanitization." National Institute of Standards and Technology Web site. September 2006. Retrieved May 27, 2014, from [http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88\\_with-errata.pdf](http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf).
- Krebs, Brian. "Amnesty International Site Serving Java Exploit." Krebs on Security. December 22, 2011. Retrieved May 17, 2014, from <https://krebsonsecurity.com/2011/12/amnesty-international-site-serving-java-exploit/>.
- . "The New Normal: 200-400 Gbps DDoS Attacks." Krebs on Security. February 14, 2014. Retrieved March 2, 2014, from <http://krebsonsecurity.com/2014/02/the-new-normal-200-400-gbps-ddos-attacks/>.
- . "Shadowy Russian Firm Seen as Conduit for Cybercrime." *Washingtonpost.com*. October 13, 2007. Retrieved April 23, 2014, from <http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html?sid=ST2007101202661>.
- . "Stolen Laptop Exposes Personal Data on 207,000 Army Reservists." Krebs on Security. May 13, 2010. Retrieved May 27, 2014, from <http://krebsonsecurity.com/2010/05/stolen-laptop-exposes-personal-data-on-207000-army-reservists/>.
- Krekel, Bryan A., Patton Adams, and George Bakos. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*. Washington, DC: U.S.-China Economic and Security Review Commission, 2012.
- Langner, Ralph. "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve." The Langner Group Web site. November 2013. Retrieved April 10, 2014, from <http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf>.



- Le, Dong. "China Hopes to Dispel 'Copy Others' Reputation." British Broadcasting Corporation Web site. January 30, 2014. Retrieved June 3, 2014, from <http://www.bbc.com/news/business-25944840>.
- Leed, Maren. "Offensive Cyber Capabilities at the Operational Level: The Way Ahead." Center for Strategic and International Studies Web site. September 2013. Retrieved April 10, 2014, from [http://csis.org/files/publication/130916\\_Leed\\_OffensiveCyberCapabilities\\_Web.pdf](http://csis.org/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf).
- Levy, Steven. *Hackers: Heroes of the Computer Revolution*. Garden City, NY: Anchor Press/Doubleday, 1984.
- Leyden, John. "Anonymous Joins Forces with Arch-Enemy The Jester Against Norks." *The Register*. April 4, 2014. Retrieved April 6, 2014, from [http://www.theregister.co.uk/2013/04/04/anon\\_nork\\_cyber\\_offensive/](http://www.theregister.co.uk/2013/04/04/anon_nork_cyber_offensive/).
- Libicki, Martin C. "Cyberdeterrence and Cyberwar." RAND Corporation. 2009. Retrieved May 8, 2014, from [http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND\\_MG877.pdf](http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf).
- Lieber, Francis. "General Orders No. 100." Retrieved March 11, 2014, from [http://avalon.law.yale.edu/19th\\_century/lieber.asp](http://avalon.law.yale.edu/19th_century/lieber.asp).
- Lipsky, Jessica. "China Bets on Homegrown OS." EE Times Web site. January 31, 2014. Retrieved June 3, 2014, from [http://www.eetimes.com/document.asp?doc\\_id=1320848](http://www.eetimes.com/document.asp?doc_id=1320848).
- Lynn, William J., III. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs Magazine* (September/October 2010). Retrieved April 29, 2014, from <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain>.
- Mandiant. "APT1: Exposing One of China's Cyber Espionage Units." Mandiant Intelligence Center. February 18, 2013. Retrieved March 2, 2014, from [http://intelreport.mandiant.com/Mandiant\\_APT1\\_Report.pdf](http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf).
- Manning, David. "The Secret Downing Street Memo." *The Sunday Times*, May 1, 2005. Retrieved March 10, 2014, from <http://web.archive.org/web/20110723222004/http://www.timesonline.co.uk/tol/news/uk/article387374.ece>.
- Markoff, John, and Thom Shanker. "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk." *New York Times*, August 1, 2009. Retrieved March 13, 2014, from <http://www.nytimes.com/2009/08/02/us/politics/02cyber.html>.
- Marlatt, Greta. "Information Warfare and Information Operations (IW/IO): A Bibliography." Naval Postgraduate School, January 2008. Retrieved March 10, 2014, from [http://edocs.nps.edu/npspubs/scholarly/biblio/Jan08-IWall\\_biblio.pdf](http://edocs.nps.edu/npspubs/scholarly/biblio/Jan08-IWall_biblio.pdf).
- Maurer, Kevin. "'Psychological Operations' Are Now 'Military Information Support Operations.'" The Associated Press, July 2, 2010. Retrieved May 23, 2014, from <http://publicintelligence.net/psychological-operations-are-now-military-information-support-operations/>.
- Maurer, Tim. "Cyber Norm Emergence at the United Nations—An Analysis of the UN's Activities Regarding Cyber-Security." Discussion paper 2011–11, Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.
- Melzer, Nils. "Cyberwarfare and International Law." United Nations Institute for Disarmament Research. 2011. Retrieved April 20, 2014, from <http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>.
- Menga, Rich. "How Long Does Backup Media Last?" March 2009. Retrieved May 26, 2014, from <http://www.pcmec.com/article/how-long-does-backup-media-last/>.
- Moore, David, and Colleen Shannon. "The Spread of the Code-Red Worm (CRv2)." The Cooperative Association for Internet Data Analysis. 2001. Retrieved May 3, 2014, from [http://www.caida.org/research/security/code-red/coderedv2\\_analysis.xml](http://www.caida.org/research/security/code-red/coderedv2_analysis.xml).

- Muncaster, Phil. "Honker Union Sniffs 270 Hactivism Targets." *The Register*. September 18, 2013. Retrieved May 3, 2014, from [http://www.theregister.co.uk/2013/09/18/honker\\_union\\_270\\_japan\\_targets\\_manchurian\\_incident/](http://www.theregister.co.uk/2013/09/18/honker_union_270_japan_targets_manchurian_incident/).
- Mulrine, Anna. "Welcome to CyberCity." *Air Force Magazine*, June 2013. Retrieved June 2, 2014, from <http://www.airforcemag.com/MagazineArchive/Pages/2013/june%202013/0613cybercity.aspx>.
- Nakashima, Ellen. "Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say." *Washington Post*, May 20, 2013. Retrieved March 23, 2014, from [http://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767\\_story.html](http://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html).
- Nakashima, Ellen et al. "U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say." *Washington Post*, June 19, 2012. Retrieved May 4, 2014, from [http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV\\_story.html](http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html).
- National Archives. "Frequently Asked Questions (FAQs) About Optical Storage Media: Storing Records on CDs and DVDs." n.d. Retrieved May 24, 2014, from <http://www.archives.gov/records-mgmt/initiatives/temp-opmedia-faq.html>.
- National Geospatial-Intelligence Agency. "About NGA." Retrieved May 23, 2014, from <https://www1.nga.mil/About/Pages/default.aspx>.
- National Institute of Standards and Technology. "NIST Guide for Applying the Risk Management Framework to Federal Information Systems." February 2010. Retrieved May 11, 2014, from <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>.
- . "Special Publication 800-60, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories." August 2008. Retrieved May 24, 2014, from [http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60\\_Vol1-Rev1.pdf](http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf).
- National Security Agency. "IAD's Top 10 Information Assurance Mitigation Strategies." National Security Agency Web site. November 2013. Retrieved March 16, 2014, from [http://www.nsa.gov/ia/\\_files/factsheets/I43V\\_Slick\\_Sheets/Slicksheet\\_Top10IAMitigationStrategies\\_Web.pdf](http://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_Top10IAMitigationStrategies_Web.pdf).
- . "Manageable Network Plan." April 2012. Retrieved May 23, 2014, from [http://iase.disa.mil/cgs/downloads/implementation/Manageable\\_Network\\_Plan.pdf](http://iase.disa.mil/cgs/downloads/implementation/Manageable_Network_Plan.pdf).
- . "Securing Data and Handling Spillage Events." October 2012. Retrieved May 22, 2014, from [http://www.nsa.gov/ia/\\_files/factsheets/Final\\_Data\\_Spill.pdf](http://www.nsa.gov/ia/_files/factsheets/Final_Data_Spill.pdf).
- Neil Jr. "Spy Agency Taps into Undersea Cable." May 23, 2001. Retrieved May 18, 2014, from <http://www.zdnet.com/news/spy-agency-taps-into-undersea-cable/115877>.
- "NSA Spied on Vatican and Top Catholic Cardinals, Says Italian Report." *Huffington Post*, October 31, 2013. Retrieved May 17, 2014, from [http://www.huffingtonpost.com/2013/10/30/nsa-vatican\\_n\\_4177882.html](http://www.huffingtonpost.com/2013/10/30/nsa-vatican_n_4177882.html).
- Obama, Barack H. "Executive Order 13526 - Classified National Security Information." Whitehouse.gov Web site. December 29, 2009. Retrieved May 11, 2014, from <http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information>.
- . "Executive Order 13556—Controlled Unclassified Information." Whitehouse.gov Web site. November 4, 2010. Retrieved May 11, 2014, from <http://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-controlled-unclassified-information>.
- . "Guide to Recordkeeping in the Army." August 2008. Retrieved May 26, 2014, from [http://www.apd.army.mil/jw2/xmldemo/p25\\_403/main.asp](http://www.apd.army.mil/jw2/xmldemo/p25_403/main.asp).

- . *National Security Strategy*. Washington, DC: The White House, May 2010. Retrieved March 10, 2014, from [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/national\\_security\\_strategy.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf).
- O'Connor, T. J. "An Analysis of Jester's QR Code Attack. (Guest Diary)." Infosec Handlers Diary blog. March 3, 2012. Retrieved April 6, 2014, from <http://isc.sans.edu/diary/An+Analysis+of+Jester+s+QR+Code+Attack+Guest+Diary+/12760>.
- . "The Jester Dynamic: A Lesson in Asymmetric Unmanaged Cyber Warfare." SANS Institute Reading Room. December 30, 2011. Retrieved April 6, 2014, from <http://www.sans.org/reading-room/whitepapers/attacking/jester-dynamic-lesson-asymmetric-unmanaged-cyber-warfare-33889>.
- Office of the Director of National Intelligence. "Data Gathering." Intelligence.gov. Retrieved March 6, 2014, from <http://www.intelligence.gov/mission/data-gathering.html>.
- Office of the Director of National Intelligence: Office of General Counsel. *Intelligence Community Legal Reference Book—2012*. dni.gov, 2012. Retrieved March 7, 2014, from [http://www.dni.gov/files/documents/IC\\_Legal\\_Ref\\_2012.pdf](http://www.dni.gov/files/documents/IC_Legal_Ref_2012.pdf).
- Office of the National Counterintelligence Executive. "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage." February 2004. Retrieved on May 17, 2014, from [http://www.ncix.gov/publications/reports/fecie\\_all/fecie\\_2003/fecie\\_2003.pdf](http://www.ncix.gov/publications/reports/fecie_all/fecie_2003/fecie_2003.pdf).
- . "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: A Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011." Office of the National Counterintelligence Executive, October 2011. Retrieved March 9, 2014, from [http://www.ncix.gov/publications/reports/fecie\\_all/Foreign\\_Economic\\_Collection\\_2011.pdf](http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf).
- Office of the Secretary of Defense. "Report of the Office of the Secretary of Defense Vietnam Task Force." January 15, 1969. Retrieved May 17, 2014, from <http://www.archives.gov/research/pentagon-papers/>.
- Olson, Parmy. *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. New York: Little, Brown and Company, 2012.
- Panda Security. "Annual Report PandaLabs 2013 Summary." Retrieved June 7, 2014, from [http://press.pandasecurity.com/wp-content/uploads/2010/05/PandaLabs-Annual-Report\\_2013.pdf](http://press.pandasecurity.com/wp-content/uploads/2010/05/PandaLabs-Annual-Report_2013.pdf).
- Parrish, Karen. "Lynn: Cyber Strategy's Thrust Is Defensive." July 14, 2011. American Forces Press Service. Retrieved June 1, 2014, from <http://www.defense.gov/news/newsarticle.aspx?id=64682>.
- Perlroth, Nicole. "Cyberattack on Saudi Firm Disquiets U.S." *New York Times*, October 24, 2012: A1.
- Perrone, Jane. "The Echelon Spy Network." *The Guardian*, May 29, 2001. Retrieved March 23, 2014, from <http://www.theguardian.com/world/2001/may/29/qanda.janeperrone>.
- Power, Richard. "The Solar Sunrise Case: Mak, Stimpny and Analyzer Give the DoD a Run for Its Money." InformIT. October 30, 2000. Retrieved May 3, 2014, from <http://www.informit.com/articles/article.aspx?p=19603&seqNum=4>.
- Reuters. "Aramco Says Cyberattack Was Aimed at Production." *New York Times*, December 10, 2012: B2.
- Riley, Michael. "Obama Invokes Cold-War Security Powers to Unmask Chinese Telecom Spyware." Bloomberg Web site. November 30, 2011. Retrieved May 18, 2014, from <http://www.bloomberg.com/news/2011-11-30/obama-invokes-cold-war-security-powers-to-unmask-chinese-telecom-spyware.html>.
- Roculan, Jensen et al. "SQLExp SQL Server Worm Analysis." Symantec DeepSight Threat Management System Threat Analysis. January 28, 2003. Retrieved May 4, 2014, from <http://securityresponse.symantec.com/avcenter/Analysis-SQLExp.pdf>.

- RSA FraudAction Research Labs. "Anatomy of an Attack." April 2011. Retrieved March 29, 2014, from <https://blogs.rsa.com/anatomy-of-an-attack/>.
- Rumsfeld, Donald. "Annual Report to Congress: The Military Power of the People's Republic of China 2005." Office of the Secretary of Defense. July 2005. Retrieved May 4, 2014, from <http://www.defense.gov/news/Jul2005/d20050719china.pdf>.
- Ryan, Thomas. "Getting In Bed with Robin Sage." Blackhat Web site. July 2010. Retrieved April 7, 2014, from <http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf>.
- Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran." *New York Times*, June 1, 2012. Retrieved May 23, 2014, from <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&r=0>.
- . "Syria War Stirs New U.S. Debate on Cyberattacks." *New York Times*, February 24, 2014.
- . Interview by Terry Gross. "While Warning of Chinese Cyberthreat, U.S. Launches Its Own Attack." *Fresh Air*. National Public Radio. April 2, 2014.
- Sanger, David E., and Thom Shanker. "NSA Devises Radio Pathway into Computers." *New York Times*, January 14, 2014. Retrieved March 23, 2014, from <http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?hp&r=0>.
- Satter, Raphael. "U.S. General: We Hacked the Enemy in Afghanistan." *USA Today*, August 24, 2012.
- Schafer, Sarah. "With Capital in Panic, Pizza Deliveries Soar." *Washington Post*, December 19, 1998. Retrieved March 10, 2014, from <http://www.washingtonpost.com/wp-srv/politics/special/clinton/stories/pizza121998.htm>.
- Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press, 2013.
- Schneier, Bruce. "How the NSA Attacks Tor/Firefox Users with QUANTUM and FOXACID." Schneier on Security. October 7, 2013. Retrieved March 12, 2014, from [https://www.schneier.com/blog/archives/2013/10/how\\_the\\_nsa\\_att.html](https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html).
- . "The NSA's New Risk Analysis." Schneier on Security. October 9, 2013. Retrieved May 4, 2014, from [https://www.schneier.com/blog/archives/2013/10/the\\_nsas\\_new\\_risk.html](https://www.schneier.com/blog/archives/2013/10/the_nsas_new_risk.html).
- Schwartz, Winn. *Information Warfare: Chaos on the Electronic Superhighway*. Berkeley, CA: Publishers Group West, 1994.
- Secretary of the Air Force. "Legal Reviews of Weapons and Cyber Capabilities." Federation of American Scientists. July 27, 2011. Retrieved April 10, 2014, from [http://static.e-publishing.af.mil/production/1/af\\_a3\\_5/publication/afi51-402/afi51-402.pdf](http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi51-402/afi51-402.pdf).
- Shakarian, Paulo. "The 2008 Russian Cyber Campaign Against Georgia." *Military Review* (2011): 63–68.
- Shimomura, Tsutomu, and John Markoff. *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw—By the Man Who Did It*. New York: Hyperion, 1996.
- Sieberg, Daniel. "Report: Hacker Infiltrated Government Computers." CNN.com. May 10, 2005. Retrieved April 23, 2014, from <http://www.cnn.com/2005/TECH/05/10/govt.computer.hacker/>.
- Singer, Abe. "Tempting Fate." ;login (February 2005).
- Singh, Simon. *The Code Book*. New York: Doubleday, 1999.
- Soumenkov, Igor. "The Mystery of the Duqu Framework Solved." SecureList. March 14, 2012. Retrieved June 7, 2014, from [https://www.securelist.com/en/blog/677/The\\_mystery\\_of\\_Duqu\\_Framework\\_solved](https://www.securelist.com/en/blog/677/The_mystery_of_Duqu_Framework_solved).

- Speigel Staff. "Inside TAO: Documents Reveal Top NSA Hacking Unit." Speigel Online: International Web site. December 29, 2013. Retrieved May 5, 2014, from <http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html>.
- Stamos, Alex. "Aurora Response Recommendations." iSEC Partners. February 17, 2010. Retrieved May 4, 2014, from [https://www.isecpartners.com/media/10932/isec\\_aurora\\_response\\_recommendations.pdf](https://www.isecpartners.com/media/10932/isec_aurora_response_recommendations.pdf).
- Stewart, Joe. "Operation Aurora: Clues in the Code." Dell SecureWorks Research blog. January 19, 2010. Retrieved May 3, 2014, from <http://www.secureworks.com/resources/blog/research/research-20913/>.
- Stoll, Clifford. "Stalking the Wily Hacker." *Communications of the ACM* 31, no. 5 (May 1988): 484–500.
- Tenable Network Security, Inc. "Tenable Delivers Best-of-Breed Configuration Compliance and Vulnerability Managment for U.S. Department of Defense." Tenable Web site. 2013. Retrieved April 29, 2014, from [http://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/case-studies/ACAS\\_CS\\_\(EN\)\\_v3\\_web.pdf](http://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/case-studies/ACAS_CS_(EN)_v3_web.pdf).
- Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian*, May 16, 2007. Retrieved May 17, 2014, from <http://www.theguardian.com/world/2007/may/17/topstories3.russia>.
- Tzu, Sun. *The Art of War*. Calgary, Alberta: Theophania Publishing, 2011.
- "U.K. 'Spied on UN's Kofi Annan.'" British Broadcasting Company. February 26, 2004. Retrieved May 17, 2014, from [http://news.bbc.co.uk/2/hi/uk\\_news/politics/3488548.stm](http://news.bbc.co.uk/2/hi/uk_news/politics/3488548.stm).
- United Nations. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." The United Nations Web site. June 24, 2013. Retrieved March 12, 2014, from [http://www.un.org/ga/search/view\\_doc.asp?symbol=A/68/98](http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98).
- . "Responsibility of States for Internationally Wrongful Acts. The United Nations International Law Commission. Retrieved April 22, 2014, from [http://legal.un.org/ilc/texts/instruments/english/draft%20articles/9\\_6\\_2001.pdf](http://legal.un.org/ilc/texts/instruments/english/draft%20articles/9_6_2001.pdf).
- United Nations Office on Drugs and Crime. "Comprehensive Study on Cybercrime." United Nations Office on Drugs and Crime Web site. February 2013. Retrieved April 23, 2014, from [http://www.unodc.org/documents/organized-crime/UNODC\\_CCPCJ\\_EG.4\\_2013/CYBERCRIME\\_STUDY\\_210213.pdf](http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf).
- United States Air Force. "Air Force Doctrine Document 3-12, Cyberspace Operations." July 15, 2010. Retrieved May 18, 2014, from <http://www.fas.org/irp/doddir/usaf/afdd3-12.pdf>.
- United States Army. "Army Doctrine Publication 3-0, Unified Land Operations." October 2011. Retrieved May 24, 2014, from [http://usarmy.vo.llnwd.net/e2/rv5\\_downloads/info/references/ADP\\_3-0\\_ULQ\\_Oct\\_2011\\_APD.pdf](http://usarmy.vo.llnwd.net/e2/rv5_downloads/info/references/ADP_3-0_ULQ_Oct_2011_APD.pdf).
- United States Army. "Army Field Manual 3-0, Operations." February 27, 2008. Retrieved May 24, 2014, from <http://www.fas.org/irp/doddir/army/fm3-0.pdf>.
- United States Department of Defense. *CAC Security*. March 30, 2014. Retrieved March 30, 2014, from <http://cac.mil/common-access-card/cac-security/>.
- . "Compendium of Key Joint Doctrine Publications." Defense Technical Information Center. November 8, 2010. Retrieved May 24, 2014, from [http://www.dtic.mil/doctrine/new\\_pubs/jp1\\_02.pdf](http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf).
- . "Department of Defense Information Enterprise Strategic Plan 2010–2012." April 2010. Retrieved May 23, 2014, from <http://dodcio.defense.gov/Portals/0/Documents/ISE/DoDIESP-r16.pdf>.

- . “Department of Defense Instruction 8500.01: Cybersecurity.” Defense Technical Information Center Online. March 14, 2014. Retrieved May 18, 2014, from [http://www.dtic.mil/whs/directives/corres/pdf/850001\\_2014.pdf](http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf).
- . “Department of Defense Instruction 8510.01: Risk Management Framework (RMF) for DoD Information Technology (IT).” Defense Technology Information Center Online. March 12, 2014. Retrieved May 13, 2014, from [http://www.dtic.mil/whs/directives/corres/pdf/851001\\_2014.pdf](http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf).
- . “Department of Defense Strategy for Operating in Cyberspace.” U.S. Department of Defense Web site. July 2011. Retrieved April 27, 2014, from [http://www.defense.gov/home/features/2011/0411\\_cyberstrategy/docs/DoD\\_Strategy\\_for\\_Operating\\_in\\_Cyberspace\\_July\\_2011.pdf](http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf).
- . “DOD Directive 2311.01E: Law of War Program.” Defense Technical Information Center Online. May 9, 2006. Retrieved February 27, 2014, from <http://www.dtic.mil/whs/directives/corres/pdf/231101e.pdf>.
- . “Joint Publication 1: Doctrine for the Armed Forces of the United States.” Defense Technical Information Center. March 25, 2013. Retrieved May 24, 2014, from [http://www.dtic.mil/doctrine/new\\_pubs/jp1.pdf](http://www.dtic.mil/doctrine/new_pubs/jp1.pdf).
- . “Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms.” Defense Technical Information Center. November 8, 2010. Retrieved March 17, 2014, from [http://www.dtic.mil/doctrine/new\\_pubs/jp1\\_02.pdf](http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf).
- . “Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies.” October 2009. Retrieved March 21, 2014, from [https://ics-cert.us-cert.gov/sites/default/files/recommended\\_practices/Defense\\_in\\_Depth\\_Oct09.pdf](https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf).
- United States Department of Defense CIO. “Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media.” DISA Information Assurance Support Environment. July 3, 2007. Retrieved May 27, 2014, from <http://iase.disa.mil/policy-guidance/dod-dar-tpm-decree07-03-07.pdf>.
- United States Department of Justice. “Overview of the Law Enforcement Strategy to Combat International Organized Crime.” April 2008. Retrieved May 17, 2014, from <http://www.justice.gov/criminal/icitap/pr/2008/04-23-08combat-intl-crime-overview.pdf>.
- United States Government Accountability Office. “GAO-11-421: Defense Department Cyber Efforts—More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities.” General Accountability Office Web site. May 2011. Retrieved May 18, 2014, from <http://www.gao.gov/assets/320/318604.pdf>.
- United States Supreme Court. *New York Times Co. v. United States*. June 30, 1971. Retrieved May 17, 2014, from <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB48/decision.pdf>.
- “Unveiling ‘Careto’—The Masked APT.” Kaspersky Lab. February 2014. Retrieved May 4, 2014, from [http://www.securelist.com/en/downloads/vlpdfs/unveilingtheface\\_v1.0.pdf](http://www.securelist.com/en/downloads/vlpdfs/unveilingtheface_v1.0.pdf).
- Verton, Dan. E-mail Correspondence. InfoSec News mailing list. October 12, 2001. Retrieved May 4, 2014, from <http://seclists.org/isn/2001/Oct/88>.
- Vise, David A. *The Bureau and the Mole: The Unmasking of Robert Philip Hanssen, the Most Dangerous Double Agent in FBI History*. New York: Grove Publishers, 2001.
- Vistica, Gregory. “Inside the Secret Cyberwar: Facing Unseen Enemies, the Feds Try to Stay a Step Ahead.” *Newsweek*, February 21, 2000: 48.
- . “We’re in the Middle of a Cyberwar.” *Newsweek*, September 20, 1999: 50.
- “W32.Duqu: The Precursor to the Next Stuxnet.” Symantec Security Response. November 23, 2011. Retrieved May 4, 2014, from [http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32-duqu\\_the\\_precursor\\_to\\_the\\_next\\_stuxnet.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32-duqu_the_precursor_to_the_next_stuxnet.pdf).

- Waterman, Shaun. "Fictitious Femme Fatale Fooled Cybersecurity." *Washington Times*, July 18, 2010. Retrieved April 7, 2014, from <http://www.washingtontimes.com/news/2010/jul/18/fictitious-femme-fatale-fooled-cybersecurity/>.
- Webster, William H. *A Review of FBI Security Programs*. Commission for the Review of FBI Security Programs, U.S. Department of Justice, March 2002. Retrieved March 23, 2014, from <http://www.fas.org/irp/agency/doj/fbi/websterreport.html>.
- Welsh, William. "Cyber Warriors: The Next Generation." Defense Systems Web site. January 23, 2014. Retrieved May 18, 2014, from <http://defensesystems.com/Articles/2014/01/23/Next-generation-cyber-warriors.aspx>.
- Winkler, J. R., C. J. O'Shea, and M. C. Stokrp. "Information Warfare, INFOSEC, and Dynamic Information Defense." PRC, Inc. 1996. Retrieved March 29, 2014, from <http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper016/jrwink.pdf>.
- Zetter, Kim. "'The Analyzer' Gets Time Served for Million-Dollar Bank Heist." *Wired Threat Level*. July 5, 2012. Retrieved May 3, 2014, from <http://www.wired.com/2012/07/tenenbaum-sentenced/>.
- . "Obama: NSA Must Reveal Bugs Like Heartbleed, Unless They Help the NSA." *Wired Threat Level*. April 15, 2014. Retrieved May 18, 2014, from <http://www.wired.com/2014/04/obama-zero-day/>.

