U. S. Department of Justice
Federal Bureau of Investigation
FBI Academy Library
Quantico, Virginia 22135

Subject Bibliography RED TEAMING

Bumgarner, John N. "Facing Your Flaws: The red team probes the network for a company to identify possible vulnerabilities and design flaws." *Security Management*. Vol. 46, Iss. 2, (February 2002): 62-66+.
Abstract: The article looks at use of red teams focusing on computer network attacks. Both vulnerability and penetration tests are utilized in a scenario in which the external security of AcmeProducts.com, a fictional small e-commerce company, is analyzed. Testing, analysis, and solutions are discussed.

Craig, Susan. "Reflections from a Red Team Leader." *Military Review*. Vol. 82, Iss. 2, (March 2007): 57-60.
Internet: http://usacac.army.mil/CAC/milreview/English/MarApr07/Craig.pdf
Abstract: The author attended the first red team leaders course given in 2006 by the Army's University of Foreign Military and Cultural Studies (UFMCS), Fort Leavenworth, Kansas. This short essay—utilizing a bullet paragraph approach—discusses and reflects upon what she learned in the course concerning critical and creative thinking, cultural awareness, and the promotion of effective red team leader skills.

Culpepper, Anna M. *Effectiveness of Using Red-Teams to Identify Maritime Security Vulnerabilities to Terrorist Attack*. Monterey, CA: Naval Post Graduate School, September 2004.
Call Number: U 310 .C96 2004
Notes: Also available on the Internet at http://www.au.af.mil/au/awc/awcgate/nps/culpepper.pdf
Abstract: The thesis is divided into introductory, red team concept, challenges of terrorism, homeland security vulnerability identification, case study, benefits of case study, and concluding sections. The analysis works within the context of the *National Strategy for Combating Terrorism* and focuses on using Red Teams to determine the terrorist potentials against the port cities of Seattle, San Francisco, and San Diego.

This bibliography is a representative selection of materials either owned or available at the FBI Academy Library. Inclusion of an item does not represent an endorsement by the FBI of the material or its author.

Defense Science Board Task Force. *The Role and Status of DoD Red Teaming Activities*. Washington, DC: Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, September 2003. 48 pp.
Internet: http://www.acq.osd.mil/dsb/reports/redteam.pdf
Abstract: Different forms of red teams and red teaming activities taking place within the Department of Defense are discussed. Conclusions and recommendations to make red teaming more effective are provided. The report itself is only 18 pages long with the rest of the document devoted to appendices. Appendix 4., focusing on historical examples of successful and unsuccessful red teams, is particularly insightful.

Dunlap, Jr., Charles J. "Joint Vision 2010: A Red Team Assessment." *Joint Forces Quarterly.* (Autumn/Winter 1997-1998): 47-49.
Internet: http://www.dtic.mil/doctrine/jel/jfq_pubs/1017pgs.pdf
Abstract: Provides a Red Team analysis of JV 2010 based on an OPFOR (Opposing Force) composed of members drawn from warrior societies distinct from the West. Red Team strategies focus on producing casualties among civilians accompanying military forces, getting large numbers of their own people killed off for media exploitation, creating moral dilemmas for US troops, and utilizing high tech COTS (Commercial-Off-The-Shelf) systems which are equal to or more advanced than fielded US military systems.

Fontenot, Gregory. "Seeing Red: Creating a Red-Team Capability for the Blue Force." *Military Review*. Vol. 85, Iss. 5, (September 2005): 4-8.
Abstract: Provides an introduction to the red-team leaders pilot program course at the University of Foreign Military and Cultural Studies (UFMCS), Fort Leavenworth, Kansas. Extremely informative article on why red teaming is required in today's complex operational environment, the history of red-team efforts, red team lessons learned (best practices and failures), the UFMCS program, and anticipated results for the Army that the leaders program will provide.

Headquarters, Department of the Army. *Opposing Force (OPFOR) Program*. AR-350-2. Washington, DC: 9 April 2004.
Internet: www.fas.org/irp/doddir/army/ar350-2.pdf
Abstract: The Army regulation for policies and procedures concerning integration of the OPFOR Program into Army-wide training and other developmental activities including training development. The document is divided into introductory, planning and management, and appendices sections. Lists the FM 100-7 Opposing Force series of field manuals.

Hoglund, Greg and Gary McGraw. *Exploiting Online Games: Cheating Massively Distributed Systems.* Upper Saddle River, NJ: Addison-Wesley, 2007.
Call Number: TK 5105.52 .H64 2007
Abstract: Written by two computer experts, the work provides an insider's view into finding security loopholes in online games that rely upon central server clusters and distributed programming architecture. Viewed as a harbinger of security issues to come on the Internet, the work provides both text and coding examples of software cheats based on the use of bots, time and state issues, hacking, reverse engineering, and other black hat tools.

Lynch, Michael D. "Developing a Scenario-Based Training Program." *FBI Law Enforcement Bulletin.* Vol. 74, No. 10 (October 2005): 1-8.
Internet: http://www.fbi.gov/publications/leb/2005/oct05leb.pdf
Abstract: Written by a law enforcement officer, the article promotes scenario-based training—an amalgamation of knowledge and skills-based training—that utilizes psychomotor coordination and reinforces a survival mindset in the officer being trained. It promotes the establishment of training objectives and utilizes role players to simulate various scenarios used in officer training to provide real-life situations in a controlled environment.

Malone, Timothy G. and Reagan E. Schaupp, "The 'Red Team': Forging a Well-Conceived Contingency Plan." *Aerospace Power Journal* Vol. 16, No. 2 (Summer 2002): 22-33.
Internet: http://www.airpower.au.af.mil/airchronicles/apj/apj02/sum02/malone.html
Abstract: The authors argue that using red teams to review the crisis-action planning process both during the planning itself and mission rehearsal will result in far more robust war plans. The failure of the air war in Serbia in 1998-1999 is used to highlight this need and how a war plan can go bad when the actions of the opposing force are not considered. The work itself provides a discussion of red teaming history, team composition and preparation, rules of engagement, timing of events, mission rehearsal, and concluding statements.

Marcinko, Richard. *Red Cell: The True Story*. Brentwood, CA: L.O.T.I. Group Productions, 1994. VHS, Color, 55 Minutes.
Call Number: VG 87 .R33 2002
Abstract: Chronicles the exploits of Red Cell, a US Navy counter-terrorist Red Team, conceptually based on the successful Red Flag pilot training program. Red Cell was stood up in the mid-1980s, initially as a classified military unit and drawn from SEAL Team Six members. It was used to penetrate US naval bases worldwide with the operations being videotaped for training purposes. The unit was dismantled in 1992 though bureaucratic and political issues had caused Red Cell operations to be severely curtailed some time earlier.

McRaven, William H. *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice.* Novato, CA: Presidio Press, 1995.
Call Number: U 262 .M37 1996
Abstract: This important work explains how "a small group of specially trained soldiers can accomplish their mission despite a numerically superior enemy." Characteristics of special operations and the six principals of special operations (simplicity, security, repetition, speed, surprise, and purpose) are introduced and developed and applied to historical case studies that validate this theory of special options. A key concept developed in the work is that of 'relative superiority' and how small forces must gain and retain it in their operations. Work has utility for the successful Red Teaming of terrorist operations.

Meehan, Capt. Michael K. "Red Teaming for Law Enforcement." *The Police Chief*. Vol. 74, No. 2, (February 2007).
Internet:http://policechiefmagazine.org/magazine/index.cfm?fuseaction=print_display&article_id=1111&issue_id=22007

Abstract: Written by a Seattle Police Department Captain with TOPOFF exercise experience, this article looks at the utility of red teaming for counterterrorism purposes. This article provides a basic introduction and a short treatment of analytical and physical red teaming. In addition, it briefly looks at the benefits, impediments, methodology, scenarios, safety, and limitations encompassing the use of red teams.

Mitnick, Kevin D. and William L. Simon. *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, IN: Wiley, 2002.
Call Number: QA76.9.A25 M58 2002
Abstract: The book focuses on the technique of 'social engineering' which relies upon the use of influence and persuasion to deceive people into providing information to someone they should not be sharing it with. This technique is commonly utilized by criminals, hackers, and even terrorists to obtain sensitive information. Sections of the book focus on information security vulnerabilities, attacker methodology using technical and non-technical means, attack examples, and information security training to mitigate social engineering attacks.

Mitnick, Kevin D. and William L. Simon. *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Detectives*. Indianapolis, IN: Wiley Publishing, Inc., 2005.
Call Number: QA76.9.A25 M587 2005
Abstract: A follow-on to *The Art of Deception* focusing on multiple incidents in which cyber-security penetrations for criminal, terrorist, and testing (red-teaming) purposes took place. Each incident is detailed and analyzed, and then suggested countermeasures are provided. The work has minimal endnotes and a detailed index.

Moore, Judy, John Whitely, and Rick Craft. *Red Gaming in Support of the War on Terrorism: Sandia Red Game Report*. Albuquerque, NM: Sandia National Laboratories, February 2004. 45 pp.
Call Number: U 310 .M66 2004
Notes: Also available on the Internet at http://www.prod.sandia.gov/cgi-bin/techlib/access-control.pl/2004/040438.pdf
Abstract: A terrorism red teaming table-top exercise was held in New Mexico that simulated two terrorist cells attacking the Washington DC subway system with an RDD (radiological device) and a biological weapon. The intent of this exercise was to help intelligence analysts (grouped in black teams) determine what piece or pieces of information would be important vis-à-vis the operational plans used in the hypothetical terrorists scenarios and seeded into a prototype compute engine. The report methodology, results, and lessons learned are provided along with detailed instruction and questions pertaining to game play.

Naylor, Sean D. "War games rigged? General says Millennium Challenge 02 'was almost entirely scripted.'" *Army Times*. August 16, 2002.
Internet: http://www.armytimes.com/legacy/new/0-292925-1060102.php
Abstract: Synopsis of the Department of Defense's Millennium Challenge 02 war game and how the Opposing Force (OPFOR) was so successful against US forces under Gen. Paul van Riper, USMC (Ret.) that many elements of the conduct of the war game including restarts, OPFOR directions not being carried out, and the eventual stepping down of van Riper in protest to game play took place.

Perla, Peter P. *The Art of Wargaming: A Guide for Professionals and Hobbyists.* Annapolis, MD: Naval Institute Press, 1990.
Call Number: U310 .P45 1990
Abstract: A classic but now dated work that looks at both the wargame (the tool) and wargaming (the process) from a historical, theoretical, and current-futures perspective. The interrelationship between military (professional) and hobby (amateur) wargaming is also discussed. Well documented with a good bibliography for further reading.

Red Team Journal. Online. 1997, Current.
Internet: Redteamjournal.com.
Abstract: This digital journal was founded in 1997 by Dr. Mark Mateski, went offline for a time, and resumed publication in August 2008. It covers all forms of red teaming and alternative analysis and has expanded to include non-military national security concerns. Besides current article postings and archives, the journal provides links to related red team sites such as Sandia's Information Design Assurance Red Team (IDART).

Sandoz, John F. *Red Teaming: A Means to Military Transformation*. Alexandria, VA: Institute of Defense Analysis, Joint Advanced Warfighting Program, January 2001. 28 pp.
Call Number: U 310 .S26 2001
Notes: Also available on the Internet at: http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA388176&Location=U2&doc=GetTRDoc.pdf
Abstract: The wargame "Attack Operations Against Critical Mobile Targets," set in the 2015 time frame, is discussed. Mobile theater ballistic missiles (TBMs) are the focus of this game that utilized an adaptive red team that countered blue force attack operations. Findings suggest that red teams are valuable not only for concept development and experimentation for new joint warfighting concepts but also have great value for providing strategic and operational insights.

Sandoz, John F. *Red Teaming: Shaping the Transformation Process, Annotated Briefing.* Alexandria, VA: Institute of Defense Analysis, Joint Advanced Warfighting Program, June 2001. 42 pp.
Call Number: U 310 .S266 2001
Notes: Also available on the Internet at: http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA398285&Location=U2&doc=GetTRDoc.pdf
Abstract: This work builds upon the preceding work undertaken by the same author in regards to the joint wargame that took place. It is conducted in annotated briefing format where the top part of each page contains a briefing slide and the bottom part of each page contains briefing notes. The briefing is divided into sections on types of red teams and what they do, challenges and attributes of a "world class" red team, issues and alternatives for establishing a red team, and the proposed establishment of a prototype red team.

Schmitt, John F. *A Practical Guide for Writing and Developing Military Concepts.* Defense Adaptive Red Team (DART) Working Paper #02-04. McLean, VA: Hicks & Associates, December 2002. 29 pp.
Call Number: U 153 .S35 2002
Internet: http://www.au.af.mil/au/awc/awcgate/dod/dart_guide.pdf

Abstract: This outstanding working paper was written by the author of a number of keystone Marine Corps doctrinal manuals and was vetted by some of the best military operational minds in existence today. The publication supports the mission of DART by providing a framework for military concepts (Part I.) and explaining how to assess future operating concepts (Part II.) It also contains an annotated glossary.

Second public hearing of the National Commission on Terrorist Attacks Upon the United States: Statement of Bogdan Dzakovic to the National Commission on Terrorist Attacks Upon the United States May 22, 2003. Washington, DC: National Commission on Terrorist Attacks Upon the United States.
Internet: http://www.9-11commission.gov/hearings/hearing2/witness_dzakovic.htm
Abstract: Statement to the 9-11 Commission by a former Federal Aviation Administration (FAA) employee who was the long term leader of the FAA Red Team. His statement discusses FAA Red Team activities, FAA response, and information he provided a month after 9-11 when he filed a Whistleblower Disclosure against the FAA for its improprieties in counter-terrorism preparation.

Sloan, Stephen. *Simulating Terrorism*. Norman, OK: University of Oklahoma Press, 1981.
Call No: HV6431 .S56
Abstract: Pioneering and extremely influential work derived from the activities of the Study Group on International Terrorism at the University of Oklahoma. The book focuses on law enforcement and military response exercises and the use of red teaming that simulates ten full-scale terrorist attacks in the United States and abroad. Targets included airports, military installations, and corporate facilities. This work is now somewhat dated due to its age. It focuses on the older traditional view of terrorism as a theatrical performance based on incidents in the late 1960s and 1970s, in which the body count is limited, hostage taking and negotiations is common, and high drama ensues.

Complied by Dr. Robert J. Bunker, FWG, 12/08