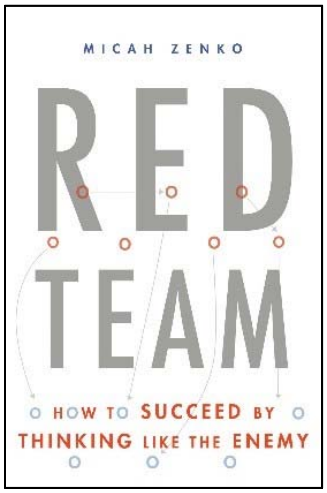
COUNCIL *on*
FOREIGN
RELATIONS

58 East 68th Street, New York, New York 10065
tel 212.434.9400 fax 212.434.9800 www.cfr.org



Teaching Notes
Red Team: How to Succeed by Thinking Like the Enemy

By **Micah Zenko**
Senior Fellow, Council on Foreign Relations

Basic Books
November 2015
$26.99 paperback
ISBN: 978-0-4650-4894-6

Red Team: How to Succeed by Thinking Like the Enemy reveals how red teams comprised of professional skeptics and saboteurs can help organizations identify vulnerabilities, challenge assumptions, and anticipate threats. Author Micah Zenko reveals how disasters like the 2014 cyber theft of over twenty million U.S. government personnel records—one of the largest data breaches in history—could have been avoided through the use of red teams.

Red Team is the first book to examine the work of these modern-day devil's advocates across a broad range of fields, including the military, security, intelligence, and business sectors. Drawing on seventeen little-known case studies, Zenko delves into the history of red teams and lays out their six best practices. He explains how organizations have benefitted from or misused red teaming, and what happens when their findings are ignored. In a final section, Zenko provides recommendations for the practice of red teaming in government that can also be tailored to private sector needs.

- The book's case studies include: the Federal Aviation Administration (FAA) red team that covertly tested airport security before 9/11 and warned about vulnerabilities that could easily be exploited by terrorists, but whose troubling findings were ignored by FAA leadership;
- benevolent "white hat" hackers who revealed that Verizon femtocells (essentially miniature cell towers used to improve reception in buildings) could easily be used to clone or steal data from phones without the knowledge of users;

- the Central Intelligence Agency (CIA) Red Cell that then director George Tenet formed days after 9/11, and which continues to conduct alternative analysis today, to "tell me things that others don't, and make seniors [officials] feel uncomfortable";
- the multiple independent analyses conducted to estimate the probability that Osama bin Laden was living in a compound in Pakistan, and the simulations that prepared the Navy SEALs for a range of contingencies prior to their successful 2011 raid; and
- red teamers who run business war games in advance of major decisions in order to analyze competitors' strategies and break rigid thought structures of their own executives.

This book is suitable for the following types of undergraduate and graduate courses:

- U.S. Foreign Policy
- Security Studies/Homeland Security
- Business Strategy

Discussion Questions

Courses on U.S. Foreign Policy (focus reading on chapters 1-3, 6):

1. What are some common weaknesses in policymaking, both in decisions and implementation?
2. Given the current global environment, what are three foreign policy issues, threats, or strategies that would benefit from red teaming?
3. What lessons can be drawn from failures to use or misapplications of red teams, such as the FAA covert airport testing before 9/11, the Millennium Challenge 2002 war game, or the bombing of the Al Shifa pharmaceutical factory?
4. What lessons can be drawn from successful red teaming, such as the CIA Red Cell's alternative analyses before the bin Laden raid or the NYPD tabletop exercise after the Mumbai terrorist attacks?
5. What are some organizational constraints that would make it difficult to use red teaming or implement a red team's findings?
6. What are the best practices of red teaming?

Courses on Security Studies/Homeland Security (focus reading on chapters 1, 6 and either 2 (military), 3 (intelligence), or 4 (homeland security)):

1. What lessons can be drawn from the use of red teaming in the case of the:
   a. FAA cover airport testing before 9/11? (homeland security)
   b. hack of Verizon's femtocell? (cybersecurity)
   c. CIA Red Cell's alternative analysis ahead of the raid of bin Laden's compound? (national security)
   d. Millennium Challenge 2002 war game? (military studies)
2. For hierarchical institutions, what are organizational constraints that might make it difficult to meaningfully apply red teaming or implement a red team's findings?
3. What are the best practices of red teaming?

Courses on Business Strategy (focus reading on chapters 1, 5-6):

1. What are some constraints of corporate culture that make it difficult to meaningfully apply red teaming or implement a red team's findings?
2. Which business practices or decisions not covered in the book could benefit from red teaming?
3. What are the best practices of red teaming?
4. What lessons can be drawn from business war gamers Ken Sawka, Benjamin Gilad, and Mark Chussil?

Essay Questions

Courses on U.S. Foreign Policy:
What do you consider the most costly or highly consequential foreign policy decision that policymakers are grappling with? If you were a government official tasked with red teaming the decision, what liberating structure would you apply and why?

If the U.S. military were planning a war game to anticipate adversaries and the threats they will pose ten years from now, which two red teaming best practices should receive the most attention from the blue and red teams and why?

Which red team best practice do you think is the most difficult for either the U.S. Department of State, U.S. Department of Defense, or Central Intelligence Agency to uphold and why? What recommendations would you give to leadership and red teamers to address this difficulty?

Courses on Security Studies/Homeland Security:
What do you consider the most high risk national security threat that policymakers are grappling with? If you were a government official tasked with red teaming the threat, what red teaming technique would you apply and why?

Which of the three types of red teaming—simulations, vulnerability probes, and alternative analyses—do you think should be applied to the threat of homegrown violent extremism?

Courses on Business Strategy:
If you are a CEO of a company tasked with deciding whether or not to launch a new product, what liberating structure would you apply to anticipate challenges and why?

Describe a scenario in which you would conduct a business war game and, as a red teamer, the steps you would take to ensure that best practices are met.

What are some of the common challenges faced by penetration testers in improving cyber or physical security?

Further Projects

Liberating Structure:
Apply one of the liberating structures listed below to a costly or highly consequential decision or policy formulation that you think the U.S. Department of State, U.S. Department of Defense, an intelligence agency, or a large corporate company could face in the next twelve months. The goal is to identify potential challenges. Descriptions of the liberating structures may be found in: University of Foreign Military and Cultural Studies, *The Applied Critical Thinking Handbook*, version 7.0, January 2015.

1. Four Ways of Seeing (p. 77)
2. Five Will Get You Twenty-Five (p. 79)
3. Alternative Futures Analysis (p. 81)

Op-Ed:
Argue why a historical event of your choice—such as a consequential foreign policy decision, national security strategy, corporate decision, or an adversary that proved a significant threat—should have been red teamed in advance.

Red Cell Memo:
Write a one-page alternative analysis memo modeled on a CIA Red Cell memo. Publicly available memos include "Afghanistan: Sustaining West European Support for the NATO-led Mission—Why Counting on Apathy Might Not Be Enough" (March 11, 2010) and "What If Foreigners See the United States as an 'Exporter of Terrorism'?" (February 5, 2010).

Supplementary Materials

Courses on U.S. Foreign Policy:

Central Intelligence Agency, "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis," March 2009, publicly released May 4, 2009.

Dunning, David, *Self-Insight: Roadblocks and Detours on the Path to Knowing Thyself*, New York, NY: Psychology Press, 2005.

Lanau, Martin, "On the Concept of a Self-Correcting Organization," *Public Administration Review*, 33(6), November-December 1973, pp. 533-542.

Murray, Williamson, "Thoughts on Red Teaming," Defense Adaptive Red Team, 2003.

Tolbert, William, *The Power of Balance: Transforming Self, Society, and Scientific Inquiry* (London, UK: Sage Publications, 1991).

Tversky, Amos and Daniel Kahneman, "Judgement under Uncertainty: Heuristics and Biases," *Science*, 185(4157), September 27, 1974, pp. 1124-1131.

University of Foreign Military and Cultural Studies, *The Applied Critical Thinking Handbook*, version 7.0, January 2015.

Courses on Security Studies/Homeland Security:

Central Intelligence Agency, "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis," March 2009, publicly released May 4, 2009.

Detert, James R. and Linda K. Trevino, "Speaking Up to Higher-Ups: How Supervisors and Skip-Level Leaders Influence Employee Voice," *Organization Science*, 21(1), 2008 pp. 249-270.

Dunning, David, *Self-Insight: Roadblocks and Detours on the Path to Knowing Thyself*, New York, NY: Psychology Press, 2005.

Lanau, Martin, "On the Concept of a Self-Correcting Organization," *Public Administration Review*, 33(6), November-December 1973, pp. 533-542.

Murray, Williamson, "Thoughts on Red Teaming," Defense Adaptive Red Team, 2003.

Sloan, Stephen, *Simulating Terrorism*, Oklahoma, OK: University of Oklahoma Press, 1981. For an updated version of this book, see, Sloan and Robert J. Bunker, *Red Teams and Counterterrorism Training*, Oklahoma, OK: University of Oklahoma Press, 2011.

Tolbert, William, *The Power of Balance: Transforming Self, Society, and Scientific Inquiry*,London, UK: Sage Publications, 1991.

Tversky, Amos and Daniel Kahneman, "Judgement under Uncertainty: Heuristics and Biases," *Science*, 185(4157), September 27, 1974, pp. 1124-1131.

University of Foreign Military and Cultural Studies, *The Applied Critical Thinking Handbook*, version 7.0, January 2015.

Courses on Business Strategy:

Detert, James R. and Linda K. Trevino, "Speaking Up to Higher-Ups: How Supervisors and Skip-Level Leaders Influence Employee Voice," *Organization Science*, 21(1), 2008, pp. 249-270.

Dunning, David, *Self-Insight: Roadblocks and Detours on the Path to Knowing Thyself*, New York, NY: Psychology Press, 2005.

Gilad, Benjamin, *Business War Games: How Large, Small, and New Companies Can Vastly Improve Their Strategies and Outmaneuver the Competition*, Pompton Plains, NJ: Career Press, 2008.

Janis, Irving, *Victims of Groupthink: A psychological study of foreign-policy decisions and fiascoes*, Boston, MA: Houghton Mifflin Company, 1972.

Lanau, Martin and Donald Chisholm, "The Arrogance of Optimism: Notes on Failure-Avoidance Management," *Journal of Contingencies and Crisis Management*, 3(2), June 1995, pp. 67-80.

Murray, Williamson, "Thoughts on Red Teaming," Defense Adaptive Red Team, 2003.

Tolbert, William, *The Power of Balance: Transforming Self, Society, and Scientific Inquiry*, London, UK: Sage Publications, 1991.

Tversky, Amos and Daniel Kahneman, "Judgement under Uncertainty: Heuristics and Biases," *Science*, 185(4157), September 27, 1974, pp. 1124-1131.

University of Foreign Military and Cultural Studies, *The Applied Critical Thinking Handbook*, version 7.0, January 2015.

Valukas, Anton R., *Report to Board of Directors of General Motors Company Regarding Ignition Switch Recalls*, Jenner&Block, May 29, 2014.