Red teaming

A short introduction (1.0)

June 2009

available at http://redteamjournal.com/resources/

Dr. Mark Mateski

Red teaming

Making good decisions

- A wide range of factors—individual, organizational, cultural, situational, and adversarial—contribute to poor decisions.
- Over the years, psychologists, intelligence analysts, and consultants have proposed a variety of methods and approaches to counter the effects of these factors.
- Most of these methods and approaches aim to broaden the analyst or decision maker's "mindset" by considering more options and assessing them more objectively—Handel's charge on the next two slides is typical.

Red teaming

Avoiding rigidity

> Clearly, the majority of failures to anticipate strategic surprise can be correlated with conceptual rigidity and a high incidence of perceptual continuity. Therefore analysts (and to a lesser extent, political and military leaders) should be encouraged to consider alternative interpretations of data and new evidence, and continuously to reevaluate their concept while avoiding dogmatic adherence to given concepts."

Handel, p. 270.

Red teaming

Countering surprise

> The search for ways to promote more open-minded attitudes is basic to almost all proposals for the improvement of intelligence work; to this end, analysts must be encouraged to present their views openly, to be critical, to fight for their opinions if necessary, and to resist group and political pressures. This is perhaps the most rudimentary condition necessary for the upgrading of intelligence work—yet it is also an ideal demand that can never be fully attained within a human environment."

Handel, p. 270.

Red teaming

Alternative analysis and red teaming

- *Alternative analysis* represents a family of methods designed to help analysts and decision makers avoid the pitfalls of poor decision making.
- *Red teaming* is one method of alternative analysis.
- As I note in subsequent slides, calls for more or better alternative analysis tend to follow perceived intelligence failures.

Red teaming

Alternative analysis defined

> … alternative analysis seeks to help analysts and policy-makers stretch their thinking through structured techniques that challenge underlying assumptions and broaden the range of possible outcomes considered.

Fishbein and Treverton.

Red teaming

Alternative analysis defined

Alternative analysis (AA) seeks to impose an explicit self-review by using specific techniques to reveal unconscious analytical assumptions or to challenge weak evidence or logic and to consider alternative hypotheses or outcomes even in the absence of convincing evidence. Simply put, intelligence analysts are now obliged to question explicitly and rigorously the assumptions that underlie their conclusions and guard against conventional wisdom masking a fundamental change in the dynamics of an issue."

George, p. 318.

Red teaming

Alternative analysis defined

[According to George, the] most powerful [alternative analysis] techniques include:

- Key Assumptions Checks
- Devil's Advocacy
- Team A/Team B
- Red Cell exercises
- Contingency 'What If' Analysis
- High-Impact/Low-Probability Analysis
- Scenario Development."

George, p. 318.

Red teaming

Alternative analysis applied

> Properly applied, [alternative analysis] serves as a hedge against the natural tendencies of analysts—like all human beings—to perceive information selectively through the lens of preconceptions, to search too narrowly for facts that would confirm rather than discredit existing hypotheses, and to be unduly influenced by premature consensus within analytic groups close at hand.

Fishbein and Treverton.

Red teaming

Alternative analysis in the real world

“To ensure against error in established analytic judgments, the CIA is vigorously promoting Alternative Analysis formats, including forms of challenge analysis (e.g., Devil’s Advocacy) and structured analysis (e.g., Analysis of Competing Hypotheses). In a complementary effort, the CIA is promoting more rigorous analysis of alternatives in first reaching judgments on complex and fluid issues—that is, the systematic generation and critical review of alternative hypotheses ...”

Davis, p. 157.

Red teaming

Expert commissions

In the last decade or so, a number of expert panels charged with assessing intelligence failure have pointed—directly or indirectly—to alternative analysis as one means of improving the processes of intelligence analysis and decision making. These commissions include

- the Jeremiah panel (1998),
- the Rumsfeld Commission (1998),
- the 9/11 Commission (2004), and
- the WMD Commission (2005).

Red teaming

The Jeremiah panel

[Following the surprise tests of nuclear weapons by both India and Pakistan in 1998] Director of Central Intelligence (DCI) George Tenet asked retired Admiral David Jeremiah to review the record to see what had led to this failure to warn the administration. While the report remains classified, Admiral Jeremiah noted at his June 1998 press conference that his 'bottom line is that both the intelligence and the policy communities had an underlying mindset going into these tests that the BJP [Bharatiya Janata Party—the newly governing Indian party] would behave as we behave.'"

George, p. 317.

Red teaming

The Jeremiah panel

Going further, Admiral Jeremiah proposed that CIA analysts be more aggressive in thinking through how the other side might behave: ‘you could argue that you need to have a contrarian view that might be part of our warning process, ought to include some divergent thinkers who look at the same evidence and come to a different conclusion and then you test that different set of conclusions against other evidence to see if it could be valid.’”

George, p. 317.

Red teaming

The Rumsfeld Commission

> Almost simultaneously [with the Jeremiah panel], the 1998 Commission to Assess the Ballistic Missile Threat to the United States [headed by Donald Rumsfeld] issued a similar assessment. It found 'analysts unwilling to make estimates that extend beyond the hard evidence they had in hand, which effectively precluded developing and testing alternative hypotheses about actual foreign programs taking place.'"

George, p. 317.

Red teaming

The 9/11 Commission

> [Writing to Donald Rumsfeld and referring to a plot to crash] an explosives-laden plan into CIA headquarters," [Wolfowitz] "wondered why so little thought had been devoted to the danger of suicide pilots, seeing a 'failure of imagination' and a mind-set that dismissed possibilities."

9/11 Commission Report, p.336.

Red teaming

The 9/11 Commission

“

It is therefore crucial to find a way of routinizing, even bureaucratizing, the exercise of imagination. Doing so requires more than finding an expert who can imagine finding an expert who can imagine that aircraft could be used as weapons.”

9/11 Commission Report, p.344

Red teaming

The WMD Commission

The widely recognized need for alternative analysis drives many to propose organizational solutions, such as ‘red teams’ and other formal mechanisms…. Any such organs, the creation of which we encourage, must do more than just ‘alternative analysis,’ though. The Community should institute a formal system for competitive—and even explicitly *contrarian*—analysis.

WMD Commission Report, p.170.

Red teaming

The WMD Commission

Perhaps most important, however, is the view that the Intelligence Community should not rely upon specialized ‘red team offices,’ or even individual ‘red team exercises’ to ensure there is sufficient independent analysis. Rather, such independent analysis must become a habitual analytic practice for *all* analysts.

WMD Commission Report, p.170.

Red teaming

Red teaming in legislation

The reports emerging from expert panels have informed Congress and led to legislation directing the government to undertake red teaming. Two examples include

- the Intelligence Reform and Terrorism Prevention Act of 2004 and
- the FY2006 Homeland Security Authorization Act.

Red teaming

2004 Intelligence Reform Act

Sec. 1017. ALTERNATIVE ANALYSIS OF INTELLIGENCE BY THE INTELLIGENCE COMMUNITY

a) IN GENERAL—Not later than 180 days after the effective date of this Act, the Director of National Intelligence shall establish a process and assign an individual or entity the responsibility for ensuring that, as appropriate, elements of the intelligence community conduct alternative analysis (commonly referred to as 'red-team analysis') of the information and conclusions in intelligence products."

Intelligence Reform and Terrorism Prevention Act.

Red teaming

Homeland Security Authorization Act

“The Act requires DHS to apply red team analysis to terrorist use of nuclear weapons and biological agents. As terrorists seek to exploit new vulnerabilities, it is imperative that appropriate tools be applied to meet those threats. The Act will broaden the intelligence process, thereby strengthening preemptive capabilities.”

FY2006 Homeland Security Authorization Act, Sec. 214 [p. 9].

Red teaming

A variety of definitions

For every *red team* that exists, a slightly different definition of *red teaming* also exists. That said, most definitions emphasize a common set of principles. I review nine representative definitions and then identify the principles.

Red teaming

Definition A

> [A red team is] a group of subject-matter experts (SME), with various, appropriate air and space disciplinary backgrounds, that provides an independent peer review of products and processes, acts as a devil's advocate, and knowledgeably role-plays the enemy and outside agencies, using an iterative, interactive process during operations planning."

Malone and Schaupp.

Red teaming

Definition B

The red team is a group of subject matter experts (SMEs) of various appropriate disciplinary backgrounds who provide an independent peer review of plans and processes; act as the adversary's advocate; and knowledgeably role-play the adversary, using a controlled, realistic, interactive process during operations planning, training, and exercising."

Homeland Security Exercise and Evaluation Program

Red teaming

Definition C

[Red teaming is an] authorized, adversary-based assessment for defensive purposes…. Adversary-based means accounting for the motivation, goals, knowledge, skills, tools, and means of one or more adversaries”

Sandia Labs’ Information Design Assurance Red Team (IDART)

Red teaming

Definition D

> [Red teaming] can mean role-playing the adversary, conducting a vulnerability assessment, or using analytical techniques to improve intelligence estimates. While these definitions seem unrelated, they have in common the goal of improving decision making.

Longbine, abstract.

Red teaming

Definition E

Defined loosely, red teaming is the practice of viewing a problem from an adversary or competitor's perspective. The goal of most red teams is to enhance decision making, either by specifying the adversary's preferences and strategies or by simply acting as a devil's advocate."

Red Team Journal

Red teaming

Definition F

> Our usage of the term red team includes not only ‘playing’ adversaries or competitors, but also serving as devil's advocates, offering alternative interpretations (team B) and otherwise challenging established thinking within an enterprise.”

DSB Red Teaming Task Force Final Report, p. 1.

Red teaming

Definition G

“

The term red teaming is commonly used to depict processes designed to bring a devil’s advocate perspective by exposing flaws and gaps in our ideas, strategies, concepts, and other new proposals.”

Sandoz, p.1

Red teaming

Definition H

> ‘Red-teaming’ is seeking to get inside the heads of adversaries, not asking what we would do if we were them but creatively trying to ask what they might do given their own goals, culture, organization, and the like.”

Treverton, p.17n.

Red teaming

Definition I

“The term red team comes from American military war gaming, where the blue team was traditionally the United States and, during the Cold War, the red team was the Soviet Union. In this context, red teaming is defined as teams of executives ‘playing’ the ‘enemy’ to understand what the competitive context (and competitor moves) will be in some potential future.”

Beck, p. 21.

Red teaming

Common definitional elements

- Arguably the most common principle emphasized in these definitions is that red teams view problems from an adversary's perspective or a contrarian point of view.
- A second principle worth noting is that red teams assist decision makers. They typically do not act apart from a client or decision maker's specific need, whether this need is to "optimize systems" or "[improve] decision making."

Red teaming

Applications of red teaming

Businesses, civilian government agencies, and the military use red teaming to test concepts, hypotheses, and operational plans in a controlled manner using understood tactics, techniques, and procedures (TTPs) or situations. For example, businesses use red teams to simulate the competition; government organizations use red teams as 'hackers' to test the security of information stored on computers or transmitted through networks; the military uses red teams to address and anticipate enemy courses of action."

Ambrose and Ahern, p. 136.

Red teaming

Applications of red teaming

“Red teaming is a term that describes a variety of exercise activities. The most basic level of red teaming is to conduct peer review of plans and policies to detect vulnerabilities or perhaps to simply offer alternative views of scenarios. Another definition [or application] of red teaming is an interactive process conducted during crisis action planning to assess planning decisions, assumptions, processes, and products from the perspective of friendly, enemy, and outside organizations.”

Meehan.

Red teaming

Applications of red teaming

> … ‘red teams’ can be used to help ensure that information systems will meet security challenges. ‘Red team’ activities can range from threat or attack exercises to critical reviews of security procedures.”

Anderson, et al, p. 72.

Red teaming

Applications of red teaming

The value of red teaming is twofold. First, it is arguably the best tool for raising security awareness in an organization. Most red teams discover known security holes for which known fixes, configurations, or patches have not been applied or where compensating security procedures are not in effect or not being enforced…. Second, red teaming is useful for ensuring that correct security configurations are maintained for the system."

National Research Council, p. 72.

Red teaming

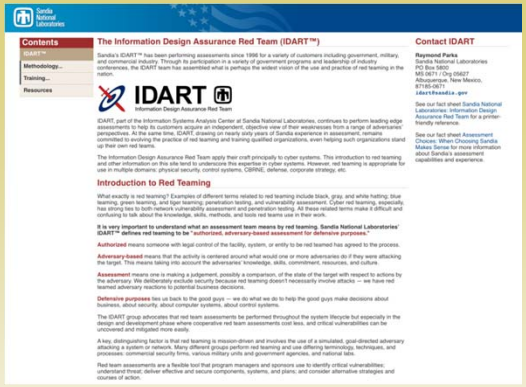
Applications of red teaming

- At least in principle, red teaming can support decision making in almost any context: security, short- or long-term strategy, engineering design, and even personal decisions.
- As suggested by the definitions, red teams may engage in planning, audits, exercises, or studies and analysis.
- Different organizations tend to define the scope of red teaming differently depending on the nature of the organization's mission.

Red teaming

Sandia's IDART

Ex



- Sandia's Information Design Assurance Red Team (IDART) "provides independent assessments of critical information systems that are performed from an adversary point-of-view …"
- Sandia's red team has hosted a variety of conferences and training courses in the past few years.

Sandia Labs' Information Design Assurance Red Team (IDART)

Red teaming

U.S. Army's UFMCS

Ex

U.S. Army Training and Doctrine Command
Office of the Chief of Public Affairs

Victory Starts Here!

About TRADOC | HQ TRADOC | School Locations | Publications/Forms | Services | Search

TRADOC PAO
TRADOC Home
PAO Home
TRADOC News Service
Media Releases
Photos/Graphics
Professional Development
Fact Sheets
Organization Info.
Chief of Public Affairs
Public Communications
Command Information
Visual Information
Plans and Policy
TRADOC Band
TRADOC Resources
Command Policy Letters
TRADOC BRAC Info
FOIA
Links of Interest
Site Map

Army approves plan to create school for Red Teaming

Story by Marcus Spade/ ***TRADOC News Service***

FORT MONROE, Va. (TRADOC News Service, July 13, 2005) – The Army recently approved the concept plan to establish the University of Foreign Military and Cultural Studies at Fort Leavenworth, Kan., providing the Army a force-wide Red Teaming capability at the unit of action through unit of employment operational levels.

A pilot program – where UFMCS begins teaching courses – starts next year. The pilot will be based on an educational, training and operational-experience curriculum and will educate specially selected students who will serve on the staffs of designated organizations.

The pilot will be similar in structure and intensity to existing programs for other advanced military studies programs for the individual services and Joint community.

UFMCS' pilot courses next year will be:

- Red Team Leader Course (18 weeks) – Intended for leaders of Red Teams organic to a UA, UEx or UEy. Initial course to begin in January 2006.
- Red Team Member Course (six weeks) – Intended for subordinate members of a Red Team that is organic to a UA, UEx or UEy.
- Red Team Practitioner Course (two weeks) – Intended for mentors and subject-matter experts assigned to support operational Red Teams.

The Army defines Red Teaming as a "structured, iterative process executed by trained, educated and practiced team members that provides commanders an independent capability to continuously challenge plans, operations, concepts, organizations and capabilities in the context of the operational environment and from our partners' and adversaries' perspectives."

According to an official from Training and Doctrine Command's Deputy Chief of Staff for Intelligence, findings of the Army's actionable-intelligence focus area – as well as operations during the Global War on Terrorism – confirm that today's Army requires an independent capability that will allow it to adapt quickly to new and unanticipated requirements.

Historically, government and industry have employed some form of Red Teaming, the DCSINT official said. "However, there's no common Red Teaming doctrine, procedures, methodologies or framework for lessons learned," he said. "There is also no formal education or training currently available to institutionalize it. As the first of its kind, UFMCS will set the standard."

A UFMCS-trained Red Team will be educated to look at problems from the perspectives of the adversary and our multinational partners, with the goal of identifyng alternative strategies. The Red Team provides commanders with critical decision-making expertise during planning and operations. The team's responsibilities will be broad – from challenging planning assumptions to conducting independent analysis to

- In 2005 the U.S. Army launched its University of Foreign Military and Cultural Studies (UFMCS).
- The purpose of the initiative is to "[provide] the Army a force-wide Red Teaming capability at the unit of action through unit of employment operational levels" and train Army officers to "look at problems from the perspectives of the adversary …"

U.S. Army Training and Doctrine Command

Red teaming

Categories of red teaming

- In the next two slides, I characterize the purpose and functions of various types of red teaming. I follow these slides with a listing of eight red teaming types developed by Sandia Labs.
- Given the variety of possible applications and settings, it is unlikely that any categorization can capture the full variety of possible red teaming activities. In fact, variety indicates possible innovation, specialization, and adaptation.
- That said, categories and types facilitate discussion and comparison.

Red teaming

Passive

Purpose	Functions	Examples
Understand	• Help BLUE better understand RED, BLUE, and how RED and BLUE view • Clarify BLUE assumptions and expose biases.	• Various intelligence, military, and commercial planning efforts (implicit).
Anticipate	• Anticipate possible RED courses of action. • Avoid surprise. • Better shape BLUE's courses of action.	• Threat, risk, or vulnerability assessments (implicit and explicit). • The military decision making process.

Mateski, "Toward a Red Teaming Taxonomy, 2.0," *Red Team Journal*.

Red teaming

Active

Purpose	Functions	Examples
Test	• Probe or penetrate BLUE systems or security. • Identify and explore vulnerabilities. • Explore and test RED COAs and BLUE countermeasures interactively.	• Penetration testing (physical and IT). • Some military exercises and experiments.
Train	• Teach BLUE how RED thinks and operations. • Prepare BLUE to respond to possible RED courses of action.	• National Training Center opposition force (OPFOR), Top Gun, and so on. • TOPOFF exercises.

Mateski, "Toward a Red Teaming Taxonomy, 2.0," *Red Team Journal*.

Red teaming

The IDART/RT4PM types

As part of their RT4PM course, Sandia has identified eight types of red teaming:

- design assurance red teaming,
- red team hypothesis testing,
- red team gaming,
- behavioral red teaming,
- red team benchmarking,
- operational red teaming,
- analytical red teaming, and
- penetration testing.

Sandia Labs' Information Design Assurance Red Team (IDART), RT4PM.

Red teaming

The continuing need for red teaming

> Whether you run a corporation or a country, the stakes are high, and business as usual is no longer good enough. More than ever, you need to know what your competitors and opponents are thinking. You need to overcome your organization's biases and generate creative, resourceful strategies that work. You need to anticipate the next crisis, prevent it if possible, and respond swiftly and effectively if not."

Mateski, "A Call for a Red Teaming Surge," *Red Team Journal*.

Red teaming

Sources

- Ambrose, Fred, and Beth Ahern. “Unconventional Red Teaming.” In *Anticipating Rare Events: Can Acts of Terror, Use of Weapons of Mass Destruction or Other High Profile Acts Be Anticipated?* 2008.
- Anderson, Robert H., et al. *Securing the U.S. Defense Information Infrastructure.* Santa Monica, CA: RAND, 1999.
- Beck, John C. “Responding to Global Crises Using the Change Cycle.” In *Thunderbird on Global Business Strategy*, by Thunderbird, The American Graduate School of International Management, 384. New York: John Wiley & Sons, 2000.
- Davis, Jack. “Why Bad Things Happen to Good Analysts.” In *Analyzing Intelligence: Origins, Obstacles, and Innovations*, by Roger Z. George and James B. Bruce. Washington, DC: Georgetown University Press, 2008.

Red teaming

Sources

- *Final Report.* Defense Science Board Task Force on the Role and Status of DoD Red Teaming Activities, U.S. Dept. of Defense, 2003.
- Fishbein, Warren, and Gregory Trevorton. *Rethinking "Alternative Analysis" to Address Transnational Threats.* Occasional Papers: Volume 3, Number 2, The Sherman Kent Center for Intelligence Analysis, 2004.
- FY2006 Homeland Security Authorization Act, Sec. 214.
- George, Roger Z. "Fixing the Problem of Analytical Mindsets." In *Intelligence and the National Security Strategist*, by Roger Z. George and Robert D. Kline. Lanham, MD: Rowman & Littlefield, 2006.
- Handel, Michael I. *War, Strategy, and Intelligence.* London: Frank Cass, 1989.

Red teaming

Sources

- Intelligence Reform and Terrorism Prevention Act of 2004. *Public Law 108--458.* December 2004.
- Longbine, David F. *Red Teaming: Past and Present.* Monograph., Fort Leavenworth, KS: School of Advanced Military Studies, United States Army Command and General Staff College, 2008.
- Malone, Timothy G., and Reagan E. Schaupp. "The 'Red Team': Forging a Well-Conceived Contingency Plan." *Aerospace Power Journal*, June 2002.
- Mateski, Mark. *Red Team Journal.* November 11, 2008. http://redteamjournal.com/2008/11/a-call-for-a-red-teaming-surge/ (accessed June 2009).
- —. *Red Team Journal.* September 2004. http://redteamjournal.com/2008/09/toward-a-red-teaming-taxonomy-20/ (accessed June 2009).

Red teaming

Sources

- Meehan, Michael K. “Red Teaming for Law Enforcement.” *The Police Chief*, February 2007.
- National Research Council. *Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities.* Washington, DC: The National Academies Press, 2000.
- *Sandia Labs’ Information Design Assurance Red Team (IDART).* 2009. http://idart.sandia.gov/ (accessed June 2009).
- —. 2009. http://idart.sandia.gov/methodology/RT4PM.html (accessed June 2009).
- Sandoz, John. *Red Teaming: A Means to Military Transformation.* IDA Paper, Alexandria, VA: Institute for Defense Analyses, 2001.

Red teaming

Sources

- *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States.* New York: W.W. Norton & Co., 2004.
- The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction: Report to the President of the United States. *Final Report.* U.S. Government, 2005.
- Treverton, Gregory F. *The Next Steps in Reshaping Intelligence.* RAND Occasional Paper, Santa Monica, CA: RAND Corporation, 2005.
- *U.S. Army, Training and Doctrine Command.* 2005. http://www.tradoc.army.mil/pao/tnsarchives/July05/070205.htm (accessed June 2009).