



Adaptive Red Teaming: Protecting Across the Spectrum

RED TEAMING is an approach to understanding threats and adversaries. Initially developed to gain insight into physical vulnerabilities (that is, penetration testing of specific target venues), it has been expanded to include a range of techniques and methodologies for understanding adversaries, capabilities, intentions, and potential attack vectors, including tactics, techniques, and procedures (TTPs). Red teaming is one approach to combat what Thomas Schelling called the “poverty of expectations” where “the danger is not that we shall read the signals and indicators with too little skill; the danger is in a poverty of expectations—a routine obsession with a few dangers that may be familiar rather than likely.”¹

Adaptive red teaming involves an iterative range of analytical and physical approaches to understanding an adversary. These approaches are valuable tools for counterterrorism, counterinsurgency, and counter-violence approaches and are used by military, police, and critical infrastructure protection professionals. This essay reviews the concept of adaptive red teaming and discusses some of the analytical red teaming tools available for intelligence assessments and operational planning.

Analytic red teaming is essentially an approach to getting inside the mindset of the terrorist or opposing force (OPFOR) group. Ideally, the result would be “enhanced understanding of the group’s particular driving factors—strategic goals, leadership and decision—making dynamics and processes, operational capabilities and rationales, organizational dynamics and behaviors, adaptive capacities, etc.—and their corollary and derivative operations.”² According to Demarce and Sullivan, “Overall, the key to such a red teaming approach is to identify and understand the prevailing and driving factors and dynamics animating the particular group and its operations.”³ Analytical red teaming will develop a “Group Strategic Threat and Modus Operandi Profile Analytical Framework” that contributes to

A deeper understanding of each group’s unique ‘mindset’ (ideology, strategic agenda, leadership) and operational behaviors (operational capabilities, modus operandi, targeting preferences) can enable a more precise and advantageous assessment of not simply what the group is capable of attacking, but what the group wants/intends to attack, as well as how the group is likely to conduct operations.⁴

A Wider Threat Spectrum

Islamist terrorism occupies a lot of attention in military, intelligence, and law enforcement circles. This is understandable due to its highly destructive and fanatical nature. However, there is a wider threat

by **John P. Sullivan**
and **Adam Elkus**

John P. Sullivan is a senior research fellow at the Center for Advanced Studies on Terrorism (CAST) and a lieutenant with the Los Angeles Sheriff’s Dept.

Adam Elkus is a widely published analyst specializing in foreign policy and security. He is currently associate editor at RED TEAM JOURNAL.

spectrum. A generation ago, terrorist groups were generally left inspired, and the idea that religious terrorism would be the paramount threat to public order would be ridiculed. Today, there are many other physical attack threats to public order than simply Islamist terrorism. A variety of groups have grievances that can translate into violence against both public and private entities. In America, for example, animal rights groups have targeted science labs. In Europe, deepening economic crises have provoked violence against financial targets.

Public and private entities manage risk through a combination of assessment, protective measures, and strategic shifts in policy. Good doctrine, security policy, and simple prudence can be useful in dealing with both a “black bloc” violent anarchist threat in a dignitary protection mission and the threat of al-Qaeda attack on a high-value target. Adaptive red teaming, however, is a crucial element of any protective plan. Red teaming tests and challenges existing security paradigms, and analytical red teaming can discover vulnerabilities in the way we conceptualize the security problem and point out new possibilities.⁵

Our purpose is to introduce or reintroduce concepts that can be employed in an analytic red teaming process: the “kill chain,” order of battle analysis, and the emerging Army military methodology known as “Design.” This is not an article detailing standard red team methodology, which is well covered elsewhere in the red team literature. Rather, we look at some new or old elements from other sources that can be incorporated into established structured red teaming processes in both government and private sector settings.

Our purpose is to introduce or reintroduce concepts that can be employed in an analytic red teaming process

Kill Chains

The first concept we look at is the “kill chain.” Experience has shown that a variety of opposing force groups and organization types exist. We have looked at this concept in the context of the Mumbai attack in our piece on police operational art.⁶ The kind of loose, emergent structure demonstrated in the Seattle “netwar” is a part of the problem, as is the more traditional one-off “cell” type group of urban radicals, the “lone wolf,” as well as multiple individuals and groups linked together in space and time.

A major debate is currently underway in terrorism and conflict studies about command and control (C²) concepts in decentralized groups. The dispute between Marc Sageman’s “Leaderless Jihad” thesis and the more traditional centralized concept of Bruce Hoffman’s thesis is one example of this, as is Dima Adamsky’s more recent study on the possibility of *jihadi* operational art.⁷ Further, research has recently been published in the scientific journal *Nature* proposing a mathematical theory of decentralized insurgency and terrorism.⁸

As an analytical device, the kill chain can be generalized across the spectrum. As noted previously, the basic kill chain model is the process of assembling weapons and personnel in place, conducting reconnaissance and dry runs, and then carrying out the act itself. It can be likened to the slow building of a weapon and its eventual employment. The vulnerability envelope of the OPFOR increases as it grows closer to the assembling of the weapon and its employment on the field. This is a basic factor common to all adversary types and concepts of operation (CONOP). The kill chain is an analog of a decision tree and contains branches and sequels for each of its tasks and subtasks. Each of these contains transactions and signatures that can be anticipated, with the resulting patterns of data—essentially trends and potentials—contributing to the formulation of hypotheses for testing OPFOR capabilities and intentions. To illustrate, we can take a sample scenario of a black bloc CONOP.

As an analytical device, the “kill chain” can be generalized across the spectrum

Black bloc (anarchist) groups—per their philosophy, their loose organizational links, and their general lack of patrons and resources—tend to operate in an emergent manner. While all human organizations are interactively complex systems, some groups tend to be more interactively complex than others.⁹ They cooperate, trading on the charisma of a leader or an amorphous common aim, however, to accomplish set tactical tasks. Their disorganization may impede the creation of a common strategy, but it can be helpful in frustrating a linear defense. This was famously seen in the “Battle of Seattle” in 1999.

For example, in a plot to inflict mass property damage and even some injuries and deaths during a trade convention, a kill chain could still be modeled as the assemblage of personnel and weapons through the buildup of critical mass in the period preceding the convention. Indications and warnings could be culled through a combination of both open- and closed-source data. Open-source research and investigations could be employed to constantly probe at signs of communication and open-source collaboration to effect an attack.

Incorporated into the overall red team process, knowledge of the kill chain can also be used to test assumptions beyond the indicators of a forming attack. It also can be used to explore vulnerabilities in defenses with different kinds of adversary C² combinations. Utilizing different models of centralized, decentralized, and “mixed” network groups, the kill chain concept can explore possibilities for OPFOR strike.

The Order of Battle

This brings us to our next concept: order of battle (ORBAT or OOB) analysis. In conventional military affairs, an ORBAT displays the enemy’s organization and disposition. Anyone familiar with military history or professional or recreational wargaming may recall the sets of boxes, checks, and arrows denoting different types of units, equipment, and axes of advance. Using ORBATs, military intelligence specialists create analytical pictures of OPFOR units (cells or nodes) and use the picture to try to predict the behavior of these units. In a civil or homeland security context, utilizing ORBATs derived from historical, open-source, and covert intelligence data can help an analyst or decision maker mentally visualize the enemy and the enemy’s attack concepts. In 2005, in *Networks, Terrorism and Global Insurgency*, Lisa J. Campbell adapted such a methodology for doing so.¹⁰

In red teaming, ORBAT analysis can be used to give teeth to analysis of the kill chain. In much the same way that a military intelligence officer would look at the ORBAT of a Soviet army, ORBAT analysis by either government or commercial analytical teams can help model adversary attributes and behavior. This can aid in analyzing raw intelligence data, creating future operations studies, or conducting a red team threat and/or vulnerability analysis of a given tactical scenario.

One way an ORBAT can be visualized in real-team red teaming is through free-play tactical decisionmaking games (TDGs). Many wargame scenarios are overly structured and do not provide a realistic training environment. TDGs, pioneered and advocated by former Army major Donald Vandergriff, are tactical scenarios that test adaptation in difficult situations. In the spirit of equality, there is no one “right” decision to solve a tactical problem. Rather, each participant evaluates and critiques (in a respectful manner) the others’ approaches, and the coordinator culls larger lessons from the exercises.

Additionally, free-play games employing a mirror-image OPFOR have been a staple of the Army’s National Training Center (NTC), where countless units have gone up against the fictional “Krasnovians”—highly

In red teaming, ORBAT analysis can be used to give teeth to analysis of the kill chain.

skilled maneuver specialists playing Soviet bloc and Third World opponents. Mirror-image training is already a part of standard red teaming, but free-play games with teams devoted to playing terrorists can also be used to test readiness and play out adversary tactical concepts. ORBATs can flesh out these exercises by providing concrete scenarios for TDGs as well as composite, well-structured opponents for red teamers to play in competitive gaming. This, unlike the standard penetration exercise, is an interactive game that provides greater opportunities for learning.

Design

Lastly, the emerging Army methodology of “Design” provides some food for thought. Design is a method pioneered by the School of Advanced Military Studies (SAMS) to frame a problem creatively prior to solving it. The Army concept of Design notes that a good deal of mistakes have been made by a failure to come to a “good enough” conceptual frame of an operational problem prior to beginning more reductive planning and assessment.¹¹

A Design methodology consists of framing the operational environment (the context in which the design is applied), framing the problem (that is, the situation that the use of power will solve), and an operational approach to push the problem toward a satisfactory solution. The process is simultaneously separate conceptually from planning but also continuous within it, similar to the concepts of the operational idea, the commander’s estimate of the situation, and the running estimate of the situation.¹² While controversial, the Design methodology may have some utility to the civil/homeland security context of red teaming.

The analytical process by which Design sorts through “wicked” or “ill-structured” problems (interactively complex problems with no stopping rule, no one “right” answer or definition, and other such attributes) through commander-led dialogue and collaboration (sometimes with outside experts) is similar to concepts of analytical red teaming. While it may not be of use in immediate tactical situations, it can be of use in challenging conceptual assumptions in a more long-term issue such as risk analysis and risk management. (We have recommended the use of the modified intelligence preparation of the battlespace variant intelligence preparation for operations [IPO]¹³ course of action analysis function.) Design’s emphasis on problems with “no stopping rule” is particularly pertinent to terrorism issues.

The German Red Army faction, while organizationally decrepit by the end of the 1970s, still carried out killings and hits for a long time afterwards. The Irish Republican Army (IRA)’s decline was only a prelude to the even more violent Provisional Irish Republican Army (PIRA). A view gaining consensus within the terrorism studies community is that al-Qaeda’s end is likely to be far more messy and inconclusive than a decisive victory.¹⁴ Since terrorism is a problem that requires risk management, the employment of Design may enhance not only structured red teaming and wargames but also support planning for defensive measures by public and private groups.

Conclusion

Red teaming extends beyond physical vulnerability analysis by red cell penetration. By employing both old and new red teaming methodologies in a structured yet creative process, public and private entities can help diagnose threats, vulnerability and risk, and point the way toward a better means of providing security and addressing emerging threats. Adaptive and analytical red teaming are valuable components of the toolbox that enable the ability to identify not only vulnerabilities but also patterns of

While controversial, the Design methodology may have some utility to the civil/homeland security context of red teaming

behavior that could culminate in a terrorist attack. These can potentially be leveraged in order to refine support to prevention and deterrence activities. Integrating the tools discussed in this paper into red teaming efforts and counterterrorism intelligence is one way of enhancing our understanding of emerging terrorist threats, anticipating threats to provide indications and warning, and ensuring an effective operational planning process that enables nimble and adaptive response to the threat envelope that contains the range of potential threats that may be encountered.

Notes

¹ Thomas Schelling, quoted in Mary McCarthy, "The National Warning System: Striving for an Elusive Goal," *Defense Intelligence Journal*, vol. 3, no. 1 (Spring 1994): 13.

² Andre Demarce and John P. Sullivan, "Developing a Group Strategic Threat and Modus Operandi Profile Analytical Framework," paper presented to Panel on Intelligence and Operational Issues for Counterterrorism and Counterinsurgency, International Studies Association, 2006 ISA Annual Conference, San Diego, CA, 24 March 2006.

³ *ibid.*

⁴ *ibid.*

⁵ For an introduction to the concept of red teaming, see Col. Timothy G. Malone and Maj. Reagan E. Schaupp, "The Red Team: Forging a Well-Received Contingency Plan," *Aerospace Power Journal*, Summer 2002.

⁶ See John P. Sullivan and Adam Elkus, "Preventing Another Mumbai: Building a Police Operational Art," *West Point Combating Terrorism Center Sentinel*, June 2009, pp. 4–7.

⁷ Marc Sageman and Bruce Hoffman, "Does Osama Still Call the Shots? Debating Containment of al Qaeda's Leadership," *Foreign Affairs*, July/August 2008, pp. 163–166 and Dima Adamsky, "Jihadi Operational Art: The Coming Wave of Jihadi Strategic Studies," *Studies in Conflict & Terrorism*, Vol. 33, no. 1, 2010 pp. 1–19.

⁸ See Juan Camilo Bohorquez, Sean Gourley, Alexander R. Dixon, Michael Spagat, and Neil F. Johnson, "Common Ecology Quantifies Human Insurgency," *Nature*, 462, 911–914 (17 December 2009), doi:10.1038/nature08631.

⁹ For an application of this to policy practice, see Jeremiah S. Pam, "The Paradox of Complexity: Embracing Its Contribution to Situational Understanding, Resisting Its Temptation in Strategy and Operational Plans," in Christopher M. Schnaubelt (ed.), *Complex Operations: NATO at War and On the Margins of War*, Rome: NATO Defense College Forum, forthcoming, 2010, p. 3.

¹⁰ See Lisa J. Campbell, "Applying Order of Battle Analysis to al-Qaeda Operations," in Robert Bunker (ed.), *Networks, Terrorism, and Global Insurgency*, London: Routledge, 2005, pp. 129–146.

¹¹ Department of the Army, *Field Manual 5-0 The Operations Process*, 2010, p. 3-1.

¹² *FM 5-0*, p. 3-7.

¹³ See John P. Sullivan, Hal Kempfer, and Jamison Jo Medby, "Understanding Consequences in Urban Operations: Intelligence Preparation for Operations," *INTSUM Magazine*, Marine Corps Intelligence Association, Vol XV, Issue 5, Summer 2005, pp. 11–19 for an in depth discussion of IPO.

¹⁴ See Audrey Kurth Cronin, *How Terrorism Ends: Understanding the Decline and Demise of Terrorism Campaigns*, Princeton: Princeton University, 2009.

About RED TEAM JOURNAL

The RED TEAM JOURNAL Web site (www.redteamjournal.com) was launched in 1997 to further the practice of red teaming and alternative analysis. The current iteration of the site is designed to help analysts and decision makers improve their ability to generate effective national security and business strategies.