Post Mission, Red Teaming the Details of the Devil.

Carter Matherly

Available at: https://works.bepress.com/matherly/5/
Post Mission,

Red Teaming the Details of the Devil.

Carter Matherly

“Adaptable, non-traditional adversaries seek new means to destroy, disrupt, or outwit us”

-Ministry of Defense
Modern terrorism has irrevocably changed the face of war forever. No longer are wars fought solely on a single linear battle field between well defined countries. Al Qaeda, its various satellites, Iranian Quds Forces, and other extremist factions have actively sought to disrupt and/or kill Americans and American interests on a global scale whenever is logistically possible. This threat will not fade with time. The Department of Defense (DoD) recognizes that there are things that can be done to combat this threat and has been hard at work employing the entirety of the INTS (abbreviation referring to a variety of intelligence capabilities) capabilities at hand, military forces, and paramilitary agencies to lessen the threat posed by terrorists on both global and domestic fronts. A terrorist attack, be it domestic or foreign, is a victory for those that sponsored it. This holds true even if that attack was thwarted, just as long as the public at large believes that they are no longer safe.

These terrorist organizations plot and train every day to discover new ways to embed a fear of violence into the daily lives of their victims. Terrorists will continue to find new and innovative ways to attack their enemies and there will always be persons willing to sponsor the violence to further their own agendas. Red Teaming is an analytical process that will reduce threat by identifying previously unobserved or unrecognized threats through visualization of the battlefield from the enemy’s point of view, via synthesis of the enemies’ decision making processes while removing relatively common analytical bias and perceptions. Despite the invaluable data these teams are able to produce there is little guidance available to assist Red teams in exploiting their gained knowledge of threats. This has ultimately led to these teams being under employed as simple OPFOR (opposing forces) with little thought to post mission analysis or applications. Could a post mission analytical review process benefit not only
Red Team knowledge and employment, but Blue forces as well in reliably identifying and understanding threats that may have gone un-noticed by current post mission intelligence processing methodologies? Post exercise evaluations present the largest opportunities to learn from decisions made leading up to and during exercise execution, yet this information is often overlooked or handled in a manner inconsistent with detailed analytical findings consistent to the Red Teaming processes.

**Perspectives of Red Teaming**

Red teaming is not a new concept nor are its principals, but there have been a lot of eyes recently focused on the concept in both the civilian business and military domains. Because of this there has been a lot of research and discussion on the topic. A handful of papers are available on the subject and all offer some insight to its recommended application. An interesting point is that one Red Team will differ drastically from another depending on the organization that it is employed in. This variation of function is not a product of application or results desired; it is a product of the organization's doctoral view of Red Teaming capabilities as they apply to that organization’s greater mission.

In 2003 the DoD’s Defense Science Board (DSB) released a report that studied the internal usage, or lack thereof, of Red Teams throughout the many DoD components. The report spends seven pages defining and explaining the what, when, why, and how’s of Red Teaming (DoD. 2003). Allotting such a large amount of space towards a definition is a unique approach that is only shared in documents whose entirety is dedicated to defining or explaining Red Teaming. This prelude to the report itself foreshadows the lack of experience the DoD
actually had with Red Teaming prior to 2003. Following the long introduction the report articulates the entirety of the DoD’s Red Teaming efforts in just shy of six pages. At the time of the report there was no DoD wide policy or standardization for such teams. The result was several very different teams with very different operations and goals. Of these the Navy had the most robust program in the 1970s and 80s that utilized Navy Seals to test the storage and safety of nuclear arms under naval control (DoD. 2003). The Air Force on the other hand utilized a Red Team to only assess technology and concepts and how they may be utilized by a potential adversary (DoD. 2003).

The Report concludes with two recommendations:

1. Take steps to inculcate effective Red Team use through the department.
2. Establish a few Red Teams in critical areas”. (DoD. 2003)

These recommendations are backed up by two further points of justification:

1. To deepen understanding of the adversaries the US now faces in the war on terrorism and in particular the capabilities and potential responses to US initiatives.
2. To guard against complacency.” (DoD. 2003)

Despite the above strong recommendations that refer to implementation of Red Teams for operational usage, and the corresponding justifications, the report gives no suggestions or ways ahead to accomplish either of them and no insight on how to use data from a Red Team.

Almost a year after these recommendations were presented to the DoD leadership, including the Sectary of Defense, Lt Commander Anna Culpepper undertook a post graduate thesis in which she concentrated on assessing vulnerabilities (threats) to maritime security by utilizing Red Teams. Culpepper’s intent was to build on the recommendations of the DSB’s 2003 report to complement Homeland Security counter terrorism efforts (Culpepper. 2004).
Unlike the DoD’s report which took seven pages to explain Red Teaming, Culpepper utilized only one and a half pages surmising that the definition given by the DSB, despite many other definitions available, would be the one used for the thesis (Culpepper. 2004).

Culpepper conducted a combined field and seminar exercise that relied on three Red Team cells to act as a surrogate enemy, while several critical decisions were also made by soliciting votes from fellow students not working in a cell. In the end the research showed that Red Teams could help improve a system’s effectiveness (Culpepper. 2004). The paper made a few very promising structural and operational recommendations for universal application Red Teams, building on the DSB report as promised. However, there is little presented in the way of using a team’s data for intelligence planning and prevention.

Five years later the DSB released another report that echoed the same heavy recommendations for Red Team usage. This time the report concentrated on addressing potential Surprise Capability of an adversary be it through technology, industry, or an unforeseen event. When one considers strategic planning and national security any unforecasted capability or intelligence surprise carries with it a high probability of threat. Of the five recommendations the report asserts, the number two recommendation states “Red Teaming as the norm instead of the exception.” (DoD. 2009). Six years and a very comprehensive application study of Red Teaming in maritime environments after the DSB originally recommended wide spread Red Team usage and it is identified that the DoD still uses Red Teams by exception only; hardly what the DSB was hoping to find.
The DSB goes on to state that Red Teams are often seen as a threat themselves (DoD. 2009). In a culture that rewards winners and looks down on losers a team that is designed to beat the home team will most likely have trouble finding any favor with the organization it just defeated. The DSB states that this problem is leadership’s burden to bear and likewise to make work (DoD. 2009). The concept was sold under a premise that if leaders embraced Red Teams it would be very simple to learn from them (DoD. 2009). Embracing something foreign is difficult to do whether mandated or not, and the individual buy-in is vital. The report fails to identify any key elements for leader and follower buy-in; the ‘whys’ are missing.

Across the pond and one year later the UK Chief of Staff promulgated an official Guide to Red Teaming (MD. 2010). This document is an all-inclusive guide to Red Teaming that, unlike other research available on the subject, offers guidance for commanders and team members themselves, as well as trouble shooting tips for both. The only thing this document is missing is a checklist, as addressed in the prologue, where it states that the guide is not intended to be doctrine but rather serve as more of a guide to identify where Red Teams would be beneficial (MD. 2010).

The Ministry of Defense’s A Guide to Red Teaming would be a great tool for domestic use of Red Teams with a little adaptation work. It is written for the military of the UK and thus relies heavily on their planning doctrine and governmental structure. For anyone wanting to know more about the ins and outs of employing a Red Team this guide has just about everything a general planner could ask for: ample information and suggestions for all parts of the planning and employment cycles. This guide falls short in one area - post exercise analyses.
Even though there is a significant span of time between the various publications they all build upon one another and increase the amount of knowledge available. Red Teaming has been identified as a very serious and important piece to any training or planning cycle. One major piece of knowledge still lacking is what to do with the information gleaned at the end of the event. There have been no insights or suggestions for effective methods of translating the knowledge gained from a Red Team into broad mission supporting data.

‘ENDEX’ is just another word for ‘STARTEX’

‘Know yourself and you will win all battles’ - Sun Tzu.

As the literature shows there are numerous gaps in Red Teaming, especially when the DoD is considered. The extreme interest shown in Red Teaming around and after 2003 has waned, leaving the intelligence and assessment industry relatively unchanged.

The ‘whys’ mentioned previously that would make red teaming easier to embrace is the intelligence gained from the team's employment, not only about the enemy but also concerning Blue Forces (friendlies). This intelligence is potentially more valuable than what can be learned during a war game or by building an additional fence to protect a high value objective. Refining Red Team findings is the precise focal point of improving military forces for future battles, identifying not only external threat but internal as well. This post exercise analytical phase is most commonly referred to as debriefing and is the capstone of any exercise or event (Markulis et al. 2003).

Luckily there are numerous volumes already published on identifying threat in its various forms yet these tried and proven methods need to be adapted to effectively analyze the
results of an exercise that involved Red Teams. By concentrating on the process and intent of proven threat analyzing techniques that are often employed post exercise the intent of analytical processes employed by Red Teams can be fully exploited.

The end result will be a product that helps leaders understand and utilize Red Teams to a higher level. Red Team employment does not end at the call of ‘ENDEX’ (a term used to call the end of an exercise) - this is where the majority of learning begins. As shown above the post exercise process has not yet been adapted to fully analyze the information gained from a Red Team's employment. This is the Achilles Heel of both experimental and training exercises (Dutton. 1979).

**The Details: This is Where the Devil Lurks**

“Red Teams can provide a different perspective on the assessment process and should offer alternative views on how adversaries, partners or other actors gauge progress, success and victory.” (MD. 2010)

The devil is in the details holds true in that the secrets of looming threat that need to be unlocked during post exercise analysis must be derived from the myriad of information available to both Blue and Red Teams. Most military debriefing processes rely on tactical decisions or actions made by operators that affected the battle space. These points are almost always spot corrective in nature. This is due to the fact that culture surrounding debriefing is to serve two purposes; firstly to assist in an operator learning from their actions and secondly to reverse the negative effects of an experience (Feaster. 2010).

During exercise preparation a Red Team will undergo several steps to formulate a plan that reflects the enemies’ most likely course of action. There are several diagnostic techniques
that can be utilized, including a Key Assumptions Check, Quality of Information Check, Indicators of Change, Deception Detection, and Competing Hypothesis (MD. 2010). All of these standard analytical processes are undertaken by team members in an indoctrinated state to replicate the thought process of the selected enemy. This entire process is unique to the Red Team undertaking the perspectives of the enemy and not that of friendly forces.

It is this unique thinking that must be preserved during the debrief process. Lederman describes seven key elements to a successful debrief:

1) The debriefer is a guide
2) Active participants
3) The debriefed holds some level of expertise in the field
4) The event had some impact
5) There is a record of events
6) There is a third party reporting of events (alternate viewpoint)
7) The debrief focuses on a specific time frame/event (Lederman. 1992)

Each of these are a vital component to the debriefing process and key to identifying what happened in a given scenario via reflection of that event (Markulis et al. 2003). However, the debriefing that most benefits Red Team involvement is not an analysis of what happened but rather taking an in-depth look at why things happened would be the appropriate vantage point.

An adaptation of Lederman’s base of seven points to facilitate the search for "why" instead of "what" would read similar to:

1) The debriefer is a guide, not involved in the event – This is an unbiased third party (can be a member of the White Team) that facilitates information flow.
2) Participants analyze/think in accordance with their Red/Blue team roles – Issues must be discussed by the same mental processes that created them. This helps to identify prejudices, thought processes, and mental blocks of each team.

3) The Red/Blue team members are the expertise in their field (for the debrief) - Blue Teams should work to understand the Red Team’s thought process while Red should work to explain the how and why of their processes; especially ones that seem irrational to Blue Team members. Neither team will learn more about the other team than either team already knows, but the opposing team may view the same information differently.

4) The event or decision has unresolved questions – This can mean that someone does not understand an event or decision post mission or that there is a key event that holds significance for the exercise.

5) There is a record of events from the Red Team and Blue Team – Each team must be able to reliably recreate what happened during the given event. Either team being oblivious to an action is a valid record (and possibly the root cause of the event).

6) A third party translation of events – This occurs as the debrief is taking place by the debriefer who highlights key points from each team and helps to facilitate translation of actions by differing mindsets.

7) A stated objective – This is the goal, the pursuit of why a team made a specific decision or acted a particular way during the exercise.
With this basis of key elements established a process needs to be identified that allows for critical analysis of Red Team events, thus exposing the underlying threat posed by a real adversary. The debrief process is generally described as a chronological analytical process that rigorously examines a critical event to determine the events that happened and facilitate improved outcomes during the next encounter (Scholtes. 1998) Traditionally this refers to debriefing that occurs in a very regimented descriptive process composed of seven steps in a linear process:

1) Introduction  
2) Fact finding  
3) Impression  
4) Reaction  
5) Cause  
6) Learning (ACA. 2011)

Conducting a debrief with a Red Team has a different goal than what Scholtes described. The process or event may be chronologically recreated; however the emphasis should not be placed on the sequence of events. Discovering the key decision or the cause, as described in step five by the ACA, that resulted in the event is not the explicit goal here either. When debriefing a Red Team the goal is identification and synthetization of the decision process that resulted in the cause or key decision. This is in direct conflict with traditional debriefing processes that identify a point and instruct it to correction, regardless of the reasoning behind the cause (Folland. 2009). This creates very black and white process that is not conducive to the deductive reasoning required to synthesize the indoctrinated thinking process utilized by Red
Teams. Keeping with the seven basic steps a simple adaptation will allow their use in conjunction with the seven key elements. A Red Team debriefing would ideally flow in the following manner:

1) **Introductions** – It is vital to understand who is on each team and what each person’s role was.
2) **Framing** – What is the event or decision in question.
3) **Reactions** – Vital to outlining biases and assumptions.
4) **Identifying Facts** - Lay out assumptions first then identify the known facts as relevant to the event or decision.
5) **Guiding Principal** – This is the principal that guided each team’s thought and decision matrix. The Red Team’s input here is critical to the next step.
6) **Synthesis** – Led by the Blue Team to demonstrate the Guiding Principles identified in the previous step.

Conducting a debrief with the above steps will allow the Blue Team understand the mental model of the Red Team and ultimately the enemy. If a successful debrief has occurred the Blue Team will be able to identify several different opportunities or strategies of attack from a given enemy. This process differs from the traditional format for debriefing in several ways. Chiefly this is accomplished by shifting focus from a specific reaction to an event to understanding the underlying reasoning and mechanics of an event from the perspective of the enemy.

There is an entire step devoted to framing the situation. This allows both Red and Blue teams to state their intents, perceptions of the battle space, and what situational awareness they had. The following step, Reactions, can occur simultaneously as each team reacts as new information is presented. During the identification of facts each team will be directed to what
biases were factual and shown areas where information was lacking. Facts that were left out or unknown will be presented to both teams at this point. As the experts on the enemy the Red Team will demonstrate how the stated information and findings were utilized to formulate their decision or the event. Finally, the capstone of the debrief will be led by the Blue Team. Traditionally this is the *Learning* phase that would consist of tailored instruction (ACA. 2011).

The goal of the synthesis phase is not instruction, but demonstration of the knowledge uncovered in the preceding steps. The end result will be identification not of an action or a tactic, but a core concept that can be utilized to prevent and counter the enemy in a reliable manner.

**Impact**

Despite several calls for a significant integration of Red Teams and their capabilities into the DoD’s stockpile of INT capabilities there has been little progress (DoD. 2009). Their ability to identify previously unidentified threat has been unequivocally demonstrated by Culpepper and outlined by numerous DoD research papers as cited herein. But what has been lacking is the ability to apply Red Team findings to a greater identification of threat beyond a single circumstance or event. This has left most leaders questioning the utility of employing such teams and ultimately discarding them immediately after, or worse yet before, and exercise even takes place (DoD.2009).

Post exercise evaluations present the largest opportunities to learn from decisions made leading up to and during exercise execution. This information is often overlooked or handled in a manner inconsistent with detailed analytical findings with respect to Red Teaming processes.
Tackling the debriefing process furthers the applicability of Red Teams and their innate ability to look inside the mind of an enemy.

The above process and principals give planners another tool to employ in the search to identify and mitigate threat. The process is not at all inclusive and is limited in scope on a few fronts. First and foremost it is only as reliable as the Red Team’s expertise on the enemy. Secondly it will not help to mitigate threat, only identify it. Mitigating threat is outside the scope of this paper as there are numerous methods available to mitigate known threat. The greatest obstacle tackled here has been the identification of a previously unknown threat. With an apt Red Team, vested commitment to the post exercise evaluation principals, and steps developed above previously unknown threat will be identified.

There is a long way ahead regarding Red Team research with numerous options to consider. The Ministry of Defense has provided a very comprehensive guide for structure and function of Red Teams. The next step in this line of research would ideally be a comprehensive application of the principals and theories developed in this paper to a Red Team debriefing event. Such an application will provide testing for confirmation and refinement of the proposed process and principals.
REFERENCES


Folland, Rolf. 2009. Holistic Debriefing: A Paradigm Shift in Leadership. Air Command and Staff College, Maxwell AFB, AL.