Red Teams; the Misunderstood Key to Defeating the Asymmetrical Warfighter

Carter Matherly
“Red Teams; the Misunderstood Key to Defeating the Asymmetrical Warfighter”

Carter Matherly

2011

INTRODUCTION
The concept of Red Teaming is not new; it is a training aid as old as the very first war game. The first formal military trained Red Team unit was founded in 1968 by the Navy Fighter Weapons School, TOPGUN. The school utilized an A-4 Skyhawk to simulate a MiG-17 (Parsons Nelson, 1993). Today’s military trains with operational Red Teams every time they support exercises such as Red Flag, Emerald Warrior, TOPGUN, operation BLACKJACK, and CSAREX, just to name a few. These teams are traditionally known as Aggressors or OPFOR during an exercise and their jobs are to be the best enemy possible in the training environment. An Aggressor trains to mimic the tactics and employment methods an adversary would use in a real world conflict. In theory a fight with an Aggressor would be not too dissimilar to an actual conflict with the true adversary, less any real munitions or lethality of course. Their job is to know, teach, and replicate potential threats that make them indistinguishable from the enemy (Factsheet, 2007).

The US Military spends millions of dollars every year pretending to be its enemies just to ensure that the first operational introduction to that enemy is not during real conflict. If these professional forces did not train this way and their first time meeting the enemy was on the battle field then the learning curve would be extremely steep, costing an enormous amount of resources and lives. Training, in general, is designed to prepare someone for something. The military trains to meet the next threat, foreseen or probable. As is shown above, the Military operationally trains using OPFOR in exercises to enhance job performance. During these exercises units put themselves mentally and physically in the fight with an enemy numerous times, in numerous different scenarios, and in areas designed to look exactly like the environment that is to be expected when deployed for a fight (Marcinko Weisman, 1998).
The US Armed Forces are very well trained and prepared to take a fight to the shores of its enemies. A prime example of this preparedness occurred on 18 March 2011 when President Obama called troops into action to protect Libyan civilians against a tyrannical dictator. Within hours B-2 bombers were on their way to bomb Kaddafi’s Air Force and cripple his air power without a single American casualty (CBSNews, 2011). However, on November 5, 2009 Major Nidal Malik Hasan shot and killed thirteen US Service members and wounded 30 others before being shot and arrested by base police on Ft Hood, TX (McCloskey, 2009). This sadly is not an isolated incident of violence against US military forces where they are supposed to be safest – at home.

American forces train hard with OPFOR to better prepare for that ‘far of fight’. Yet where is the OPFOR for training against a domestic threat? There was once a special team of Navy SEALs formed under the command of Commander Richard Marcinko. These SEALs joined together as the Navy’s first Red Team. Their task was to identify and exploit weakness within the Navy’s defense of its critical assets; nuclear subs, munitions, launch codes, etc. (Marcinko, 2000). The team was later disbanded under accusations of misappropriations and assault (SO.com, 2000). Unfortunately this disbandment left US forces woefully unprepared for asymmetrical threats within the US. A quick Google search of the team immediately brings up numerous conspiracy theories, most of which are aimed at base commanders who were embarrassed when the Red Team penetrated their base’s defenses so easily. Regardless of the reasons the SEAL Red Team was disbanded, there was and has been no attempt to recapture the Red Team concept within the US Military. Worse yet the loss of this concept and the unique type of training it provided has left the US Military woefully unprepared to face any domestic threat. The bigger question is why? Why in an era of military cut backs and fiscal constraints has this
capability been allowed to die a quick unceremonious death? Perhaps it’s the same reason the US Navy spent $60 million on a failed court-martial against then Commander Marcinko, in his own words he “made the bean counters and paper-pushers who run the Navy look bad” (Tennant, 1998).

Years later the Bipartisan Policy Center issued a report that took a domestic and global perspective on the US’s susceptibility to terrorist attacks (Bergen Hoffman, 2010). The study focused on a time period of Jan 2009-Aug 2010. During the specified time frame ten serious attacks were reported. Two of them were successfully carried out with lethal consequences, including the afore mentioned shooting at Ft. Hood. The report closes noting that since 9/11 terrorists at home and abroad have not rested. They are quickly adapting and planning their next attack to defeat America’s sense of security and its means of livelihood (Bergen Hoffman, 2010). Could a Red Team provide realistic training and analysis opportunities that would contribute positively to the overall, readiness, safety, vigilance, and security of both US Military personnel and its critical areas of operation? Yes, but what of the biases and prejudices that haunt base security and Red Team employment?

Identifying current biases and prejudices directed towards base security will provide a unique opportunity to critically analyze the effectiveness of current security measures, challenge these and future measures allowing security planners to critically analyze unscripted reaction to threats, this will fill a current void in threat anticipation that will in turn foster a culture of threat vigilance, preparedness, and appropriate reactions to threats all of which will be operated under an increasing demand for fiscal responsibility.
There is a marked lack of training when one compares how the military trains for fights at home and abroad. Above is barely a glimpse into the summation of the Military’s operational training. Current training for a domestic threat is dominated by computer based tests (CBTs) that mix hypothetical situations and DoD doctrine with humor. The goal is to train a soldier quickly, cheaply, and easily while using humor to make the CBTs less painful. When compared to the large force exercises described at the beginning of this paper there is a very large discrepancy in realism and preparedness when comparing the two. Even though terrorists have shown that they can and will attack the US on its own soil, priorities in training have not significantly changed to meet this threat head on. The threat is not going to go away; it is only going to get worse (Bergen Hoffman, 2010).

THE PROBLEM

Throughout all of the official literature published by the United States Government any mention to Red Team, Aggressor, or OPFOR relates directly to either large scale operations or exercises where operational tasks and scenarios are paramount. The use of a Red Team to test en-garrison security, attitudes, and responses is virtually unmentioned or considered.

In Air Force Instruction (AFI) 31-210 (USAF, 1997) the terms ‘Red Team’ are not mentioned once. The entire AFI is directed to the base commander level where it recommends that they rely on AF Office of Special Investigations (AFOSI) to provide an update of threats to the base and its workers. The major downfall to AFI 31-210 is it revolves around bases located outside the continental US. Shortly after the attacks on the Twin Towers and Pentagon on the 11th of September 2010, the AFI was rescinded.
Since these attacks the military has established a position within each unit that is intended to counteract any terrorist threats. The Anti-Terrorism Officer (ATO) is supposed to be the one-stop shop for assessing, responding to, and preventing a terrorist attack against a military base or unit. However, the directives governing this office provide the ATO only the tools needed to react to an attack. Without compromising operational security, these tools equate to basically hunkering down and waiting. The ATO program does not outline or direct any provisions for actually testing security or assessing shortfalls in current policy though any means other than brainstorming and operational exercises. These exercises are commonly referred to as an Operational Readiness Exercise (ORE). An ORE is a large-scale war game where a unit or units deploy to a hypothetical base and support a war against a hypothetical enemy. These ORES rarely occur at the unit’s home base and are designed to simulate being deployed to a base located outside of the US. Thus training is, by design, directed towards defending against a foreign military threat, normally a conventional standing military.

With consideration to this project, there is no practical way to determine if the current approach to garrison operational security is due to the escapades of Commander Marchinko’s team or not. However, in light of recent attacks against military bases and personnel, one thing is clear – more needs to be done. This attitude was reflected in a recent study conducted for this research paper.

To help better identify current perceptions of security on military bases, a voluntary 10-question survey was made available to 100 people for five days. After the five days, a total of 59 persons responded to the survey. The vast majority of the respondents, 91 percent, have been or currently are employed on a military base, and only nine percent have never worked on a military base. For the purposes of this study, having been on a military base in any capacity at least once
before is a qualifying factor for providing an accurate perception of security on military installations. Subjects were not made aware of this qualifier and all of the subjects reported that they have been on a military installation at least once before. Considering this and after careful review of responses and remarks it was determined that all of the 59 subjects and their responses were reliable and none were thrown out.

Participants were asked to rate how secure they perceive a military installation to be on a descending scale form; Unbeatable, Secure, Adequate, Sub-Par, to A Joke at the bottom of the rating chain. An evenly combined ninety percent stated that security on a military base is Secure or Adequate. Only seven percent of responses felt security was less than Adequate.

Another question asked survey takers to state which should be more secure, a military base or an Airport. Eighty five percent responded a military base should be more secure and fifteen percent responded an airport. Survey takers were allowed to type in reasoning for their answer and nine took advantage of this option providing a typed response in addition to their selection. The majority of the typed responses agreed that a military base should be more secure than an Airport. These responses referenced the fact that a military base will house weapons of war and provide for the defense of the nation and its infrastructure. Two of the written statements remarked that the types of additional security at airports; scans, searches, etc., would not be cost effective or ‘worthwhile’ to further secure a military base. The main concern was security versus gaining accesses to base in a timely manner. The wait for security screening at an airport can exceed 45 minutes, this would not be practical to employ at a security gate entering a military base.

The third question in the survey asked subjects if they feel more secure in their own neighborhood versus on base. Seventy one percent stated they would feel more secure on a
military base while twenty eight percent feel more secure in their own neighborhood. Previously in the survey thirty seven people stated they have lived on base while only five have never lived on or near a base. These five did however state that they have worked on a military base in some capacity.

Survey takers were also asked if they felt that a military base would be secure against a terrorist attack and if the US military could defend against such an attack. The subject’s perceptions showed that the US military could defend against a terrorist threat from within the US (sixty eight percent), but could not secure themselves against such a threat (fifty eight percent).

**PERCEPTIONS**

Perceptions of security on military bases vary strongly. All of the respondents identified themselves as being exposed to military security as least once before, they went on to say that they feel that security is at least adequate. Adequate is defined by Merriam Webster as ‘lawful and sufficient’ or ‘sufficient for a specific requirement’ (Webster, 2011). For the purposes of this study securing a military base from un-warranted incursions or threats would be considered adequate. The survey also concluded that a military installation should be more secure than an airport and that people feel safer living on a base rather than off of one.

Of the total 623 different quantifiable responses collected by the survey 196 were informational in nature. The remaining 427 can be categorized as either conveying a positive perception of base security or a negative one. Considering each response and categorizing them as positive or negative perceptions study shows that 268 responses are positive in nature and 159
are negative. For easy comparison these figures are shown in a histogram in Figure 1.1 along with other figures covered below.

Base security was addressed as five different levels of security from *un-beatable* to *a joke*. Fifty five responses were positive in nature, identifying base security as at or above *adequate*. Only four responses categorized security below that mark. Furthermore fifty responses stated that a military base should be more secure than an airport. This is very similar in quantity to those who feel a military base is already secure.

The overview of responses and perceptions attached to the responses show that overall it is highly perceived that a military base provides sufficient security to keep its personnel and assets secure from an enemy. Security is intended to prevent unwanted people from gaining access to particular assets, persons, facilities, etc. This is one of the reasons the Terrorist Screening Center is in existence (FBI, 2011). It helps prevent known persons from gaining access to methods that can cause the US harm.

**REALITY**

Perceptions can cloud judgments and make people believe things that are not true. Most people are prone to anchoring bias when judging areas of uncertainty. This can be easily identified in a discussion with the terms ‘I believe’, ‘it is unlikely that’, or ‘chances are’ (Tversky, 2007). These are all keys that anchoring bias is playing a large role in ones opinions and thus decisions. Anchoring bias is a major key in identifying misconceptions surrounding base security. When prompted to identify how secure a military base is 93 percent of survey takers identified the base as at least adequately secure. When the same survey takers were asked if a military base is secure from a terrorist attack only 42 percent responded positively, the
remaining 58 percent responded that it was not secure from such attacks. This discrepancy can be seen in Figure 1.1 below.

When the broad question of ‘is a base secure’ is compared to the detailed question of ‘...against terrorist attack’ anchoring bias is easily identified. When a question is broad enough respondents will focus on what is on the forefront in their mind by conducting a global evaluation (Kahneman, 2006). When entering a military base the fence, guards, barbed wire and other visual stimulants give the perception of a high level of security. However when prompted to judge against something specific at differences begin to appear in the perception of the person asked. They start to notice discrepancies in security that the threat might exploit; low over hanging branches, gaps in the fence line, unpatrolled sections of base, and the numerous times they have gained access to base without their ID card because they left it at work. This perception flaw is exactly what a Red Team combats by addressing the global evaluation process and identifying potential threats and how they exploit security to their benefit.

CONCLUSION
Biases and false perceptions of reality constantly plague evaluations of military bases’ security. There was once a team specifically dedicated to combating these perceptions and exposing how unsecure bases with critical assets to national defense actually are. The Navy was the only service to ever employ such a Red Team with a mission to exploit naval installation security. The team enjoyed resounding success until they were disbanded under questionable circumstances. As the survey for this report identified there are biases surrounding the actual security of military bases. The base commander is ultimately responsible for securing the base against exploitation and attack from potential enemies. A lapse in security or demonstrated overall failure of security can cost a base commander their job and in most cases their career (UCMJ, 2011).

Any action that would risk a commander’s career is certainly an unwelcome threat. With the Navy’s Red Team reporting findings directly to the Secretary of the Navy and not base commanders its clear why the team commander was arrested under charges of conspiracy brought on by former base commanders. Many of the team’s actions brought to light the biases identified in this study. On several occasions the team kidnapped admirals, family members of commanders, stole nuclear submarines, nuclear devices, and even acquired top secret launch codes for the nuclear devices (Marchinko, 2000). All of this occurred in the mid/late 1980s using tactics not very different from tactics used by terrorist organizations today. In 2003 the DSB released its report surmising Red Team activities within the US military. The report states that even though the enemy has changed, the basics of covert attack have only become more advanced and less dependent on technology (DSB, 2003). The threat to military bases within the US from an asymmetrical threat is real. Biases have clouded the need for a low cost high yield active threat assessment option, a Red Team. One hundred percent of the survey takers felt that
such an option would not negatively affect current security, 83 percent felt it would improve
security. Eight years after the recommendations of the DSB their findings have only seen limited
spotlight and it is still the current stance of the US military to practice security training and
testing only in an exercise environment.

This study was able to capture a small snapshot of current and past biases affecting
military security against asymmetrical threats. The majority of the survey takers for this study
are active duty, rated, Air Force officers, Captain to Lt Col, whom have all deployed to active
war zones in support of current and past US led wars.

Given the limited availability of official unclassified information published on Seal Team
Six Red Team and access to persons involved in their analysis of security, absolutes cannot be
drawn to their reasons for being disbanded. The research contained herein has adhered to the
strict standards and sought opinions of others, on an informal basis, familiar with command and
base security for analysis of the Seal Red Team.

More research is needed to state, as fact, that an actively employed Red Team would
provide enhanced security for US military bases. As intended this report has shown that there are
biases hindering perception of base security. These biases have also translated into policy
surrounding US military bases and training in support of that security. The intent of this study is
to identify these discrepancies’ and promote further dialogue and testing to improve base
security. As one respondent to the study stated “[Base] security is part of maintaining National
security.” This statement could not be more accurate. How can a military secure a nation against
a domestic asymmetrical threat if it is not prepared to defend itself against the same threat?
ACRONYMS

OPFOR; Opposing Force

CSAREX; Combat Search and Rescue Exercise

SEAL; Name for the Navy’s premier special operations team. Plural, SEALs

DoD; Department of Defense

CBT; Computer Based Test

US; United States

AFOSI; Air Force Office of Special Investigations

REFERENCES


McCloskey, Megan, 2009 "Civilian police officer acted quickly to help subdue alleged gunman", Stars and Stripes, November 8, 2009


Peter Bergen and Bruce Hoffman, 2010. “Assessing the Terrorist Threat” Bipartisan Policy Center September 10, 2010


UCMJ, 2011. “UNIFORM CODE OF MILITARY JUSTICE”