NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ADAPTIVE RED TEAMING ON DEVELOPMENTAL TECHNOLOGIES

by

John P. Klopfenstein

September 2015

Thesis Advisor:	Gary Langford
Second Reader:	Brigette Kwinn

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704–0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2015	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE ADAPTIVE RED-TEAMING ON DEVELOPMENTAL TECHNOLOGIES	**5. FUNDING NUMBERS**
6. AUTHOR(S) Klopfenstein, John P.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This thesis defines a methodology that can be used to support a comprehensive red-teaming process to assess the technology used during developmental technology. The goal is for the U.S. Army to benefit from a repeatable, adaptable method to acquire defense systems that are both useful and desirable by operational commands. A stakeholder analysis focused on red-team requirements indicated the need to increase threat emulation capabilities, provide a quantitative snapshot of technology, and increase collaboration between government and industry.

Based on the methodology recommended by this research, a new, repeatable process was initiated by the Adaptive Red Team. This new process offers an improved evaluation of developmental technology, which provides a baseline logistics, technological and user factors score for each technology, and a better understanding of the risk of acceptance for a tested technology. Additional process improvements include emulation of formidable threats through equipment; improved tactics, techniques, and procedures; and increased collaboration between government and industry through the use of data standards, new knowledge of adaptive red-team missions, and technology introductions.

Initial results of applying the recommendations of this thesis have uncovered vulnerabilities never seen and when mitigated, have shown to increase operational capabilities for DOD.

14. SUBJECT TERMS Red-teaming, technology development, Adaptive Red Team, and developmental technology	**15. NUMBER OF PAGES** 79
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ADAPTIVE RED-TEAMING ON DEVELOPMENTAL TECHNOLOGIES

John P. Klopfenstein
Civilian, Communications-Electronic Research, Development and Engineering Center,
United States Army
B.S., DeVry Institute of Technology, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2015

Approved by: Gary Langford, Ph.D.
Thesis Advisor

Brigitte Kwinn
Second Reader

Ron Giachetti, Ph.D.
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis defines a methodology that can be used to support a comprehensive red-teaming process to assess the technology used during developmental technology. The goal is for the U.S. Army to benefit from a repeatable, adaptable method to acquire defense systems that are both useful and desirable by operational commands. A stakeholder analysis focused on red-team requirements indicated the need to increase threat emulation capabilities, provide a quantitative snapshot of technology, and increase collaboration between government and industry.

Based on the methodology recommended by this research, a new, repeatable process was initiated by the Adaptive Red Team. This new process offers an improved evaluation of developmental technology, which provides a baseline logistics, technological and user factors score for each technology, and a better understanding of the risk of acceptance for a tested technology. Additional process improvements include emulation of formidable threats through equipment; improved tactics, techniques, and procedures; and increased collaboration between government and industry through the use of data standards, new knowledge of adaptive red-team missions, and technology introductions.

Initial results of applying the recommendations of this thesis have uncovered vulnerabilities never seen and when mitigated, have shown to increase operational capabilities for DOD.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION..1
A. PURPOSE..1
B. BENEFITS OF THIS THESIS..2
C. RESEARCH QUESTIONS..2
D. METHODOLOGY..3
E. ASSUMPTIONS..3
F. THESIS ORGANIZATION..4

II. BACKGROUND..5
A. RED TEAMS..5
B. ADAPTIVE RED TEAM..6

III. ADAPTIVE RED TEAM..9

IV. ADAPTIVE RED TEAM OVERVIEW OF OLD PROCESS..11
A. ORGANIZATION..11
1. White Cell..11
2. Blue Cell..12
3. Red Cell..13
B. ASSESSMENTS..13
1. Discovery Assessment..13
2. Operational Assessment..14
C. ADAPTIVE RED TEAM ASSESSMENTS VENUE LOCATION.....15
D. SCENARIOS..16
E. OLD PROCESS OVERVIEW..17
1. Adaptive Red Team Planning..18
2. Adaptive Red Team Execution..20

V. SYSTEM THINKING APPROACH..23
A. REPEATABLE PROCESS PROVIDING A QUANTITATIVE SNAPSHOT OF TECHNOLOGY..23
B. INCREASE THREAT EMULATION CAPABILITIES..27
C. INCREASE COLLABORATION BETWEEN GOVERNMENT AND INDUSTRY..30
1. Barriers to Collaboration..30
2. Methods to Increase Collaboration..31

VI. NEW ADAPTIVE RED TEAM PROCESS BASED ON SYSTEMS THINKING....35
A. PLANNING....35
B. EXECUTION....36

VII. NEW ADAPTIVE RED TEAM PROCESS INITIAL RESULTS....39
A. TRADESPACE METHODOLOGY INITIAL RESULTS....39
1. Flex Fuel Generator....41
B. ELECTRONIC WARFARE AND COMPUTER NETWORK SECURITY....43
1. Frontier II Low Visibility Friendly Force Tracker Overview....43
2. EW & CNS Assessment of the LVFFT....44
3. EW & CNS Assessment Summary....45
C. COLLABORATION AND INTEGRATION....46
1. Flex Fuel Generator Collaboration....47
2. Frontier II LVFTT....48

VIII. CONCLUSION....51

LIST OF REFERENCES....55

INITIAL DISTRIBUTION LIST....57

LIST OF FIGURES

Figure 1. Camp Roberts National Guard Base—Replica Combat Outpost 16

Figure 2. Old Adaptive Red Team process (from Gilkes and Klopfenstein 2014, 3–5) 19

Figure 3. Old Adaptive Red Team Execution (from Gilkes and Klopfenstein 2014, 3–5) 22

Figure 4. Tradespace Methodology Decomposition (from Klopfenstein and Tober 2014, 107–122)..24

Figure 5. Sample CoT Schema (Kristan 2009, 2–1) 32

Figure 6. Modified Planning Process based on Systems Thinking (from Gilkes and Klopfenstein 2014, 3–5)...35

Figure 7. New Adaptive Red Team Execution and Cell Interaction (from Gilkes and Klopfenstein 2014, 3–5) 37

Figure 8. Adaptive Red Team event 14–2 Most Likely (ML) average per tradespace (from Klopfenstein and Tober 2014, 107–122) 40

Figure 9. 1 kW Flex Fuel Generator...42

Figure 10. Individual Tradespace Methodology subfactor assessment and uncertainty score (from Klopfenstein and Tober 2014, 107–122)............42

Figure 11. Frontier II LVFFT Device (from Klopfenstein and Tober 2014, 107–122) 44

Figure 12. Frontier II LVFFT Control Station Software (from Klopfenstein and Tober 2014, 107–122)..49

Figure 13. COP Software Displaying New Integrated Frontier TTL Devices Circled in Red (from Klopfenstein and Tober 2014, 107–122)................50

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Goals and Objectives to Increase Threat Emulation Capabilities.............27

Table 2. Common Threat Equipment Used and Purpose..29

Table 3. Summary of Actions Traced to Stakeholder Requirements.......................33

Table 4. Enumeration Results for 192.168.112.28 45

Table 5. Flex Fuel Generator Collaborations Results from Adaptive Red Team Assessment...47

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAR	after action review
AES 256	advanced encryption standard 256
ART	Adaptive Red Team
ASA(ALT)	Assistant Secretary of the Army for Acquisitions, Logistics and Technology
ASD(R&E)	Assistant Secretary of Defense for Research and Engineering
CERDEC	Communications-Electronics Research, Development Engineering Center
CNS	computer network security
COP	common operational picture
CoT	cursor-on-target
DFP TFT	Deployable Force Protection Technology Focus Team
DNS	domain name service
DOD	Department of Defense
DoS	denial of service
DTF	Distributed Tactical Fires
ECP	entry control point
ERPS	Expedition Recon Patrol Squad Pak
EW	electronic warfare
FAS	fencepost acoustic system
FFT	friendly force tracker
FFG	flex fuel generator
GUI	graphical user interface
HARVS	Human Activity Recognition in Video Streams
HFT	hostile force tracker
IP	Internet protocol
IRAD	internal research and development
L1FB	level 1 fusion in a box
LVFFT	low visibility friendly force tracker
LWAEC	Lightweight App-enabled Computer
MAC	media access control
MPS	Mortar Protection System
OPFOR	opposition forces
OSD	Office of Secretary of Defense
Pana ND Cam	Panoramic Night/Day Camera

RASE	Reconnaissance Advanced Sensor and Exploitation
RF	radio frequency
RFI	request for information
RGPs	rocket propelled grenades
RO Iridiu	RO Iridium Radio
SOCOM	Special Operations Command
SOF	Special Operations Forces
Stalker XE	stalker extended endurance unmanned aerial system
TRADOC	Training and Doctrine Command
TTL	tracking, tagging and locating
TTP	tactics, techniques and procedures
UFMCS	University of Foreign Military and Cultural Studies
UID	unique identification
USMC	United States Marine Corp
WEP	wired equivalent privacy
WPA2	Wi-Fi protected access 2

EXECUTIVE SUMMARY

Red-teaming is a process that is performed on equipment and procedures to include forums such as contact proposals, briefings, and operational battle plans. Red-teaming is typically carried out using critical thinking, alternative analysis, and cultural empathy to provide an understanding of the opposing or enemy’s viewpoint as it relates to the particular forum under consideration. This opposing viewpoint is used in the commercial world to understand the opposition in order to improve the contract proposal or briefing by incorporating the red team’s outputs. A similar process is used by the Department of Defense (DOD) to codify the opposing viewpoint from the perspective of the adversary. This adversarial perspective is traditionally used to develop operational battle plans, in effect to counter the red strategy. The DOD red teamers are taught to use critical thinking skills to analyze complex issues from a systems perspective and use techniques focused on cultural empathy to understand cultural traditions and customs.

In 2009, the Army created an Adaptive Red Team (ART) as part of the Deployable Force Protection Technology Focus Team (DFP TFT). ART was responsible for assessing vulnerabilities and limitations in developmental technology that will support and protect U.S. military when deployed through the perspective of an adaptable and complex enemy. Developmental technology is defined by Langford (2012) as “the scientific, mechanical, electronic, or chemical means of improving people’s performances or by providing or enhancing their indigenous functions. These improvements provide for (1) making better decisions, (2) doing more work faster, and (3) doing work that could not be accomplished before by any one individual.” As such, Langford continues, -”engineering is an enabler to bring technology to people. And, systems engineering facilitates life cycle thinking to not only make improvements, but also to achieve improvements taking into account life cycle issues, reducing impacts on stakeholders (including the environment), and mitigating unintended consequences due to the building, operations, or disposal of a product or service” (Langford 119).

A vulnerability is a weakness in a technology that has the potential to be exploited by the enemy and possibly render that technology ineffective for its designed purpose.

Vulnerabilities could be as simple as using a cell phone camera to detect an infrared light used in night vision equipment, or a more complex electronic attack exploiting a weakness in a wireless network. Technological limitations can be discovered by red teams when a developer lacks a complete understanding of the operational picture. One example of a technology limitation that was discovered by the Adaptive Red Team is of a laser technology that is used to detect certain chemical substances in gaseous form at an entry point for a combat outpost. The effective range of the laser was only half that required for the safe standoff distance to protect against commonly used explosive devices. The range limitation meant that the commonly used explosive devices in that combat area could have injured the laser operator and destroyed the expensive laser detection technology and possibly resulted in further deaths and destruction.

Adaptive Red Team was designed to be different from the traditional red-teaming. The challenge for Adaptive Red Team was how to utilize and adapt red-teaming techniques that were developed for assessing operation battle plans to the problems with developmental technology. The utilization and adaptation presented a significant challenge for the implementers of Adaptive Red Team. This thesis explores how systems thinking is used to improve upon an existing red-teaming function that deals with developmental technology. The author shows and provides supporting data that incorporates systems engineering and systems thinking to address the vulnerability analysis and system improvement.

Adaptive Red Team utilized a process based on field experimentation with existing military equipment. Further, the limited red team knowledge about the developmental technologies and their general unfamiliarity with the actual equipment compounded the need for a repeatable, quantitative methodology to support red-teaming. The first attempt at an adapted red-teaming process was marginally effective, lacking both the adaptability and flexibility of a truly complex adversary and a repeatable, measurable process.

Adaptive Red Team utilized systems thinking to create a new adaptable but repeatable process to address the stakeholder requirements.

- Create a repeatable process providing a quantitative snapshot of technology.

- Increase threat emulation capabilities in order to uncover additional vulnerabilities and system limitations.
- Increase collaboration between government and Industry.

These requirements were analyzed, and specific objectives were identified. Those objectives tied to specific actions as shown in Table 1.

Table 1. Summary of Adaptive Red Team Actions with traceability

Stakeholder Requirements	Objective	Action
Repeatable process providing a quantitative snapshot of technology	Implement Quantitative Process	Tradespace methodology using logistics, tech factors and usability as technology acceptance tradespace
Increase threat emulation capabilities in order to uncover additional vulnerabilities and system limitations	Improve Red Cell	Permanent Red Cell Lead
		Increase Red Cell Training
		Increase Red Cell Threat Equipment
		Increase Red Cell Uniforms and Weapons
	Improve Red Cell Electronic Attack	Increase expertise in threat computer network security
		Increase expertise in threat electronic warfare
Increase collaboration between Government and Industry	Increase Collaboration with Industry	Institute bi-weekly teleconferences to increase information flow and understating of ART
		Provide two-minute technology introductions at beginning of execution week.
	Increase Collaboration between Government	Institute bi-weekly teleconferences to increase information flow and understating of ART
		Provide two-minute technology introductions at beginning of execution week.
		Utilize data format standards for integration into government owned COPs

The actions indicated in Table 1 were implemented in the new Adaptive Red Team process and initial results proved to be positive. Specifically, tradespace implementation allowed Adaptive Red Team to provide a quantitative snapshot of developmental technology. This quantitative snapshot provided a measurable and repeatable method to measure the technologies logistics, technological, and user factors. These measurements allow the sponsor to understand the risk and value of technology acceptance by soldiers. Threat emulation capabilities were increased by personnel who are experts in electronic/computer threat emulation. In addition, Adaptive Red Team increased collaboration between government and industry by incorporating a data standard. This data standard allowed for all technology with a networked output to be displayed on one computer running situational awareness software. This data standard allowed for a common operation picture.

Finally, initial results associated with tradespace methodology, electronic attack personnel and common data standards have shown to be favorable. The new Adaptive Red Team process with systems thinking is producing initial results that are favorable. Those favorable results are on track to be the adaptable, flexible process the Army needs to Red Team developmental technology.

The primary benefit of this thesis to the U.S. Army is to provide a comprehensive red-teaming process that is a repeatable, adaptable method for acquiring defense systems that are both useful and desirable by U.S. forces.

List of References

Langford, Gary O. 2012. *Engineering Systems Integration*. Boca Raton, FL: CRC Press.

ACKNOWLEDGMENTS

First, I would like to thank my thesis advisor, Dr. Gary Langford. His efforts and guidance have been instrumental in my thesis, and I could not have done it without his help. His experience and perspective as a red teamer was very useful, not to mention his enthusiastic approach and willingness to help.

I have been fortunate to have worked with some great role models, mentors and friends throughout my career. My mentor and friend Mr. Erik Syvrud has offered guidance, support, and motivation, which has been extremely valuable in my pursing higher education. Without his direction, leadership, and friendship I would not be where I am today.

In addition to Mr. Syvrud, I would also like to thank a very professional and caring person who, by his actions, made me a better person and leader. Dr. Dave Netzer is one of those special people you do not meet very often. He is an inspirational leader who taught me through his actions that leaders are not afraid to take on anything or do anything for the mission, no matter how menial the task.

I would also like to thank my co-workers who sometimes operated a man-down while I attended school or suffered in others ways because of my studies. Thanks for your patience and for picking up the slack.

Finally, I would like to thank my wife and two boys for their patience and understanding while I was pursuing my degree. I have missed many school activities and weekend events while striving to obtain my master’s degree. I love you all very much and missing activities or time with my family hurts. For that, I am truly sorry, but know that I love you all very much, and in the end, it is my family who drives me to succeed in an attempt to better our lives.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE

The Assistant Secretary of the Army for Research and Technology uses the Adaptive Red Team (ART) to improve developing technologies, uncover system vulnerabilities, and identify mitigations paths in order to increase system effectiveness and mission capability (Goerger 2012, 13). These limitation and vulnerabilities are discovered through a quarterly field experiment in which commercial and government equipment is operated by soldiers during military operations, called scenarios, against an enemy. These scenarios allow the equipment to be exposed to enemy tactics, techniques and procedures (TTPs). Enemy responses allow the technology developer to understand what the enemy may do. The enemy responses provide the developer of equipment with a potential path forward for further development. The technology developer is a person or group of people inside an organization, both government and industry, who are responsible to the stakeholder for the advancement and maturation of a particular technology. Each Adaptive Red Team assessment includes 25 technology developers selected to be part of an upcoming assessment. The developmental technology that is the focus for the scenarios within the assessment is utilized in an operational and realistic manner by soldiers executing missions against an enemy that is allowed to be adaptable as the situation changes. This primary Adaptive Red Team process provides the developer a documented list of vulnerabilities and limitations that they can use as path to understanding and mitigation.

This thesis explores how systems thinking is used to improve an existing red-teaming function that deals with developmental technology. The author provides supporting data that incorporates systems engineering and systems thinking to address the vulnerability analysis and system improvement. This thesis introduces a refined Adaptive Red Team process.

From an historical perspective, after the attack on Combat Outpost Keating, it was determined by the Army that the sophisticated enemy was able to take advantage of rapidly developed technology that was neither fully integrated into proven Army operational use nor fully tested. This technology was rushed to the battlefield in an attempt to save lives without fully understanding the vulnerabilities that may have existed for an enemy to exploit. Adaptive Red Team was initiated to provide a method to identify technology weaknesses though an enemy perspective so that the technology developer is made aware and can mitigate the vulnerabilities, in an attempt to prevent another combat outpost from being overrun.

B. BENEFITS OF THIS THESIS

By defining a comprehensive red-teaming process, the goal is for the Army to benefit from a repeatable, adaptable method to acquire defense systems that is both useful and desirable by U.S. forces. Defining a repeatable and adaptable process is the scope for this thesis. Furthermore, this thesis applies this new process to identify vulnerabilities in 25 developmental technologies at the rate of one assessment per quarter. Scalability of this repeatable and adaptable process (and specifically how it could be applied to a larger number of technologies per assessment) is not addressed, but noted to be a desirable next step.

Scalability of the Adaptive Red Team process and methodologies is a topic for future research once the basic Adaptive Red Team process and methodologies are proven. Scalability is important to the Amy because of the hierarchical organizational structure that builds capability from unit level to brigade level through integration of forces and processes. This thesis will focus on a small unit (4-16 soldiers) operational scenario based on the units assigned to Combat Outpost Keating.

C. RESEARCH QUESTIONS

1. What are the impacts of the Adaptive Red-teaming methods on the developmental technology?

2. What value does the Adaptive Red Team process provide for developing defense technologies?

3. How does implementing the Adaptive Red-teaming process help DOD acquire defense system more efficiently?

D. METHODOLOGY

This thesis seeks to define a comprehensive, quantitative red-teaming process that can be used to improve technology development by exposing technology to enemy TTPs to help focus corrections to exploitable methods and equipment. The methodology proposed for red-teaming is not utilized in formal tests with objectives and thresholds, as those are designed around each individual technology. Rather a methodology or process that can be used to expose vulnerabilities in all participating technologies is sought.

The original Adaptive Red Team process that was initiated by DOD and the Army in 2009 was part of a legacy program used from previous field experiment experience, but that legacy program did not fulfill the desired requirements of the sponsor. The following requirements were identified as being unfulfilled.

1. Create a repeatable process providing a quantitative snapshot of technology.
2. Increase threat emulation capabilities in order to uncover additional vulnerabilities and system limitations.
3. Increase collaboration between government and industry (Goerger 2012, 13).

The process used in the original Adaptive Red Team is discussed in Chapter II. Implementation of a new process was needed and a systems thinking approach was adopted. This new approach led to changes and improvements starting with stakeholder guidance on requirements that were not being addressed fully. These system requirements provided the basis for this research and from which improvements could be made to the existing Adaptive Red Team. These improvements are incorporated into the new methods for Adaptive Red Team and initial results are discussed in this thesis.

E. ASSUMPTIONS

When a technology is incorporated into (i.e., “attends”) an Adaptive Red Team assessment and a list of potential vulnerabilities for the equipment being tested is generated, system limitations are discovered. The purpose for Adaptive Red Team is to assure that the development system under assessment will mitigate those vulnerabilities and provide for a less vulnerable and more capable technology that can be deployed to operational units. At the outset, it is assumed that the new procedures incorporated into Adaptive Red Team will be more effective than the old system of red-teaming. That assumption is tested through notional feedback through the assessment results, informal discussions with the participants, and a general perception of the efficiency of assessment planning and execution.

Further, it is assumed that if collaboration is increased, the government will ultimately use better products. Those better products may include more feature sets in a particular technology or enhancing current feature sets with better algorithms or other analysis tools from a different vendor. There are no plans to test this premise as part of either this thesis or as a recommendation. Consider this premise to be a baseline principle from which the red-teaming work is built and enacted.

F. THESIS ORGANIZATION

This thesis describes a process used by the Adaptive Red Team to identify vulnerabilities in developmental technologies. This process was modified though stakeholder interactions and identification of deficiencies in the outcome. Systems engineering principles were used to decompose those deficiencies and modify the process starting in Chapters V and VI. That modified process provided initial results discussed in Chapter VII, followed by a discussion of research questions in the conclusion.

II. BACKGROUND

A. RED TEAMS

According to Defense Science Board, “red teams and red-teaming processes are tools and techniques that have long been used by Government and Industry in order to reduce risk and increase opportunities,” (Defense Science Board 2003, 2). Commercial enterprises use red-teaming as a way to prepare for a client presentation, play the side of the government for a contract proposal, or to capture what the competitor or “other side” may be thinking. Once the presenter or proposal team has an understanding of what the other side is potentially thinking, they may modify their strategy, their tactics, their documents, or their product offerings to accommodate the insight and additional knowledge. This approach to thinking about the opposition is fundamental to systems engineering and systems thinking and has been in widespread general use for the past 40 years. Red-teaming has a long history of use by the Army (University of Foreign Military and Cultural Studies 2012) and has spread to the Operational Communities, Joint Agencies, as well as Interagency Organizations. However, after years of ad hoc methods that were bound to heuristics (Langford 2012, 19), the first *Red-teaming Handbook* was published by the University of Foreign Military and Cultural Studies (UFMCS) in 2006. Since 2006, the *Red-teaming Handbook* has been revised many times to include new insights and maturing concepts (University of Foreign Military and Cultural Studies 2012).

As the Handbook states, “UFMCS red teams are taught strategies and techniques to avoid common problems such as avoiding group think, mirror imaging, cultural ignorance, and tunnel vision” (1).

After more than 40 years of use, red-teaming is accepted and practiced as an effective method to analyze operational plans from a military organization. Red teams are also effective in analyzing corporate briefing or large contract proposals. The key tenet of red-teaming is consistent across all domains—look at the battle plan from the perspective of the enemy or its equivalent for a proposal from the perspective of the receiving agency. Organizations use the red team's output to make a more effective product. However, the techniques taught at UFMCS are not intended to be used to red team developmental technology. To broaden the use of red-teaming taught at UFMCS, this thesis discusses the revisions, methods, and general results for developmental technology.

B. ADAPTIVE RED TEAM

October 3, 2009, the Battle of Kamdesh took place in Afghanistan on Combat Outpost Keating. This battle was one of the deadliest battles on a small outpost in U.S. history. Eight Americans were killed and 27 wounded during that fight while up to 350 Taliban fighters partially overran the combat outpost (Seavey 2015, 1). This small combat outpost was in a remote part of Afghanistan and surrounded by difficult to defend terrain. These Taliban fighters were extremely diligent in their preparation and attention to detail when planning the attack and exploited many gaps in U.S. defenses and took advantage of some vulnerabilities to create this devastating blow to Combat Outpost Keating.

The overrun of Combat Outpost Keating overrun in Afghanistan led the Office of the Secretary of Defense (OSD) and Army to develop a technology focused Red Team. In 2009, a red team was stood up by the Assistant Secretary of Defense for Research and Engineering (ASD (R&E)) with support from Assistant Secretary of the Army for Research and Technology as part of the Deployable Force Protection Technology Focus Team (DFP TFT). OSD was responsible for initiating this effort but funding and program execution was provided by Assistant Secretary of the Army for Acquisitions, Logistics and Technology (ASA(ALT))

DFP TFT was a larger program focused on small base challenges and technology development to support those challenges in a rapid manner. Added was a separate red-teaming component to help mature specific technologies that had been put into operational use based on a threat perspective. This red team was called the Adaptive Red Team (ART).

> The mission of the Adaptive Red Team is to support the Assistant Secretary of the Army for Acquisition, Logistics & Technology efforts to enable the soldier by identification of potential vulnerabilities in developmental technologies including performance degradation in contested environments, interoperability, adaptability and training/ease of use through live experiment venues designed to improve soldier maneuver, survivability, and lethality. (Goerger 2012, 3)

THIS PAGE INTENTIONALLY LEFT BLANK

III. ADAPTIVE RED TEAM

The Adaptive Red Team execution team was originally made up of four personnel. The team included the team manager, event coordinator, operations lead, and data collection lead. The manager was responsible for developing and executing the plan to conduct four quarterly Adaptive Red Team events know as vulnerability assessments. This plan includes sponsor interactions, budget plan and execution, contractual interactions, and program briefings. The event coordinator was responsible for executing the manager's plan as it pertains to the details of orchestrating all activities necessary to conduct a vulnerability assessment. These activities included coordination of military base range operations, radio frequency spectrum clearance, maintaining quarterly task schedules, and coordination of planning meetings. A full-time active duty Army National Guardsman served as the operations lead and is responsible for maintaining soldier support for each event—planning out the roles and responsibilities for personnel conducting the scenario, developing the scenarios, and running the U.S. Forces operations center. The final member of the original execution team was the data collection lead. This person had the responsibility of establishing a base line list of questions for each technology, assigning additional data collectors for each technology, and managing the report process. Each member of the original Adaptive Red Team had a unique responsibility on the execution team and all team members pulled together to assist each other when necessary.

The Adaptive Red Team's execution team was asked to perform the Adaptive Red Team mission based on their previous field experiments for Special Operations Command (SOCOM). This fieldwork was desired by the sponsor in order to begin with an experienced team that understood field experimentation. The field experimentation experience provided the execution team an understanding of how to invite industry to participate legally, organize a group of technology developers for a common goal, and how to incorporate soldiers into field experimentation.

However, this field experience provided only part of the needs for success as an Adaptive Red Team. Since the execution team did not have any knowledge or experience in red-teaming, they needed an understanding of general red-teaming methods before they could execute an Adaptive Red Team effectively for the sponsor.

The need for general knowledge of red-teaming was addressed in 2010 by attending a course from the Army Combined Arms Center called *Critical Thinking for Red Team Practitioner*. This two-week course familiarized the execution team with critical thinking skills, cultural empathy, and groupthink mitigation strategies to help challenge assumptions and consider alternative perspectives in support of better decision making (University of Foreign Military and Cultural Studies 2012).

The training provided a general background and understanding of red-teaming as it is applied to staff who implement red team military operational plans. The skills and strategies taught in this critical thinking course were considered to be good skills to have when participating in an operational organization that develops battle plans for a unit’s execution. This thesis research reinforces that assumption.

The Adaptive Red Team was created to assess vulnerabilities and system limitations in developmental technologies. However, the Adaptive Red Team was not concerned about operational plans (as were emphasized in the mobile course). For example, traditional red teamers, as taught, will care that a military organization destroyed a bridge in a battle after they crossed but that may not be a culturally acceptable tactic. Knowing the ultimate use of the course materials, the attendees from the Adaptive Red Team translated their needs through the perspective of the course materials to improve relevance and understanding of the course.

To date, the training and experience has allowed the team to conduct vulnerability assessments using soldiers emulating enemy tactics, techniques, and procedures. The Adaptive Red Team challenge has been to weave together red-teaming concepts that were designed for operational plans and use so they can be used on technology development.

IV. ADAPTIVE RED TEAM OVERVIEW OF OLD PROCESS

A. ORGANIZATION

The organization of the Adaptive Red Team is based on semi-autonomous cells performing individual functions. Within each cell, each member or teams of members perform a particular subfunction. In this manner, the top-level functions that must be carried out are divided cells, in a fashion similar to functional decomposition used in systems engineering to that leads to a work breakdown structure. Commensurate with the systems engineering functional decomposition, the associated processes and activities are carried out by members of the cells.

The three cells used for the execution of an Adaptive Red Team are the white, blue, and red cells. The white cell has the function of data collection. The blue cell has the function of equipment training and planning/executing the operational scenarios that represent U.S. forces. Lastly, the red cell has the function of threat emulation. During the execution of an assessment, each cell is provided additional support personnel through the actions of execution team. The execution team utilizes their leadership positions and networks to provide support from other government research facilities and operational units.

1. White Cell

The data collection effort is performed by the white cell and the lead data collector from the execution team becomes the white cell lead for the execution of this function. Each data collection team from white cell is comprised of two team members: an engineer/scientist and a soldier performing this subfunction. The data collection teams are each assigned three technologies and are responsible for collecting performance data to support their assigned technologies throughout the assessment week.

The engineer/scientist data collectors include representatives from many governmental organizations. Soldiers from various branches of the military are also included as part of the two-person white cell data collection team. This combination of technical experts with operational users allows the engineering/science to be understood, communicated, and assessed in the context of operational uses.

Assessments are categorized as discovery or operational.

- **Discovery assessments:** Each technology is assessed as a standalone capability to understand the technologies capabilities/limitations/vulnerabilities as presented.

- **Operational Assessments:** Technologies are assessed during operational scenarios that are conducted by soldiers assigned to blue and red cells discussed below. These scenarios are designed to stretch the operational limitations of the technology and uncover how well the technology performs against enemy actions. Scenarios are conducted several times each day and are based on real world missions that the Army conducts.

2. Blue Cell

Blue cell is responsible for the development and execution of all operational scenarios and operational feedback. The lead for operations on the execution team leads the blue cell. Blue cell is augmented by additional soldiers from support units that have been placed on orders to participate by the execution team. The Blue cell lead is a senior, non-commissioned officer (NCO) with many Special Operations Forces (SOF) deployments to Iraq, Afghanistan, Africa, and many other counties working on combat outposts and other smaller remotes bases. Blue cell leadership organizes the supporting soldiers by the units and experience. Soldiers are organized into squads, each with a squad leader and approximately five soldiers. The rank of each squad member ranges from E-2 through E-6. This variety of rank allows a different perspective to be incorporated into the assessments of the scenarios.

Blue cell squad members are trained on a specific technology that they will use when executing the scenarios. Technology developers provide this training. The training function is discussed in Section B2. Blue cell squad members execute the missions in the scenarios, then provide feedback in the after-action reviews.

Operational scenarios are a method for each technology participant (if desired) to have a soldier train on the equipment and use it during a tactical mission(s) called a scenario. This set of activities is enacted with the expectation that the majority of the vulnerabilities will be discovered.

3. Red Cell

Red cell provides the threat emulation and acts as the enemy force for each scenario. Red cell members perform roles such as farmers or shop keepers. These roles each have a unique set of actions that are performed based on the scenarios being executed. Farmers could be used to place or carry explosives and shopkeepers could be selling stolen merchandise from blue cell or watching base activity for pattern of life.

This cell is led by a government civilian that supports Adaptive Red Team, but this lead is not part of the execution team. The red cell lead has over thirty years' experience in SOF and related small unit missions both from a planning and execution perspective. Red cell is augmented by soldiers from various organizations. Typically, this cell has eight to 15 people on the team, depending on the physical terrain and operational area planned in the scenario.

Red cell is organized to accommodate various scenarios. Sometimes red cell is structured like a village with a very specific key leader. Other times the red cell is organized into two person teams or single individuals acting as sheepherders, farm workers, or shop workers. These different organizational structures allows red cell to expose the technology to different enemy TTPs.

The rank of each red cell member varies slightly, but typically the higher ranking, more experience soldiers are assigned to red cell. All assigned red cell members receive training form the red cell lead on how to execute enemy TTPs effectively.

B. ASSESSMENTS

1. Discovery Assessment

The discovery function is performed by the two-person data collection team from white cell. This team has a generic list of questions that are the general starting point for a technology discussion carried out by the white cell teams. These assessments provide a baseline of each technology and its performance characteristics in the context of different scenarios. The list of questions is the starting point in the discussions with the technology developers. The questions are geared to provide an understating of the following areas: technology, form factor, connectivity, reliability, user interface, training, and sustainability. Sample discovery assessment questions used:

1. What is field of view and resolution of this option?
2. Is it a cooled imager? If so, can the enemy detect the cooler noise?
3. How is the system transported? Any material handling equipment requirements?
4. How can the system be setup and operated at night?

2. Operational Assessment

Technology performance in the operational scenarios conducted by blue cell and red cell is called the operational assessment. This operational assessment is performed by the white cell data collectors assigned to each technology. White cell teams perform this function by a combination of techniques from watching performance in the operations center, blue cell interviews, red cell interviews, and participation in the after action reviews. Typical questions asked by white cell members include:

1. Through the use of the technology, did blue cell notice red cell activities that were meant to be clandestine?
2. Did red cell interpret blue bell activities?
3. Did red cell breach the outer perimeter?
4. Were red cell communications detected?

Operational assessments are a method for each technology developer to have a soldier train on the equipment and use it during a tactical mission(s) called a scenario. This technique results in the discovery of the majority of the vulnerabilities. The training function only happens if the participant wishes to pursue inclusion in the scenarios. Training time is limited and varies for each technology. This limitation is a realistic constraint based on soldier feedback from previous participation. When soldiers are deployed, time is a very precious resource, and when a personnel rotation is underway, everything becomes more difficult, including training on systems that the incoming unit has never seen before. The departing soldier must train his/her replacement in a limited amount of time while still performing the daily duties and getting ready for departure. This change is called rotation of personnel/transfer of authority (RIP/TOA). Adaptive Red team simulates RIP/TOA by limiting the time a participant has to train soldiers, which allows the participant to understand the complexities associated with RIP/TOA. Understanding this issue allows the participant to address with quick start guides, videos, and segmented software (easy/advanced), color-coding cables, or some other issue learned during the training and scenario debriefings.

Once fully trained on the equipment, the soldier now has control of the technology and begins to prepare for movement. This experience allows the soldier to pack the equipment in his/her rucksack and prepare for the mission. The load out of equipment also proves to be a valuable lesson for developers, as many do not understand what other essential mission items go into a rucksack with space at a premium.

Operational scenario participation exposes technology weaknesses and vulnerabilities that would not normally be discovered in a laboratory environment because soldiers do stress the technological limits and sometimes use the technology in unintended ways. Systems engineers describe this behavior as emergence.

C. ADAPTIVE RED TEAM ASSESSMENTS VENUE LOCATION

The origin of the DFP TFT and creation of the Adaptive Red Team was based on Combat Outpost Keating being overrun. Deployable force protection TFT focus was on enhancing technology that could be used to protect small bases less than 300 personnel.

Afghanistan has 652,230 square kilometers (CIA , 1) and is slightly smaller than Texas. This landlocked country has the Hindu Kush mountain range that runs northeast to southwest dividing the country. This mountain range creates a terrain that can be difficult to protect but also provides long flat open terrain in specific areas. War strategy dictates the locations of outposts and not one outpost is identical to another.

Adaptive Red Team execution team use information from the operations lead and stakeholders to guide selection of the assessment venue and organize accordingly. Adaptive Red Team prefers venues that have already built structures such as exterior walls and entry control points as a way of mimicking the terrain of Afghanistan.

Camp Roberts National Guard Base in California has an existing outpost that the military regularly uses as they prepare for deployment. This outpost is located among rolling hills, open plains, and distant mountains. The weather can be similarly hot and dry. The Camp Roberts site was chosen as the primary assessment venue location because of its terrain and existing outpost structure, such as guard towers, walls, entry control points, and wooden buildings.

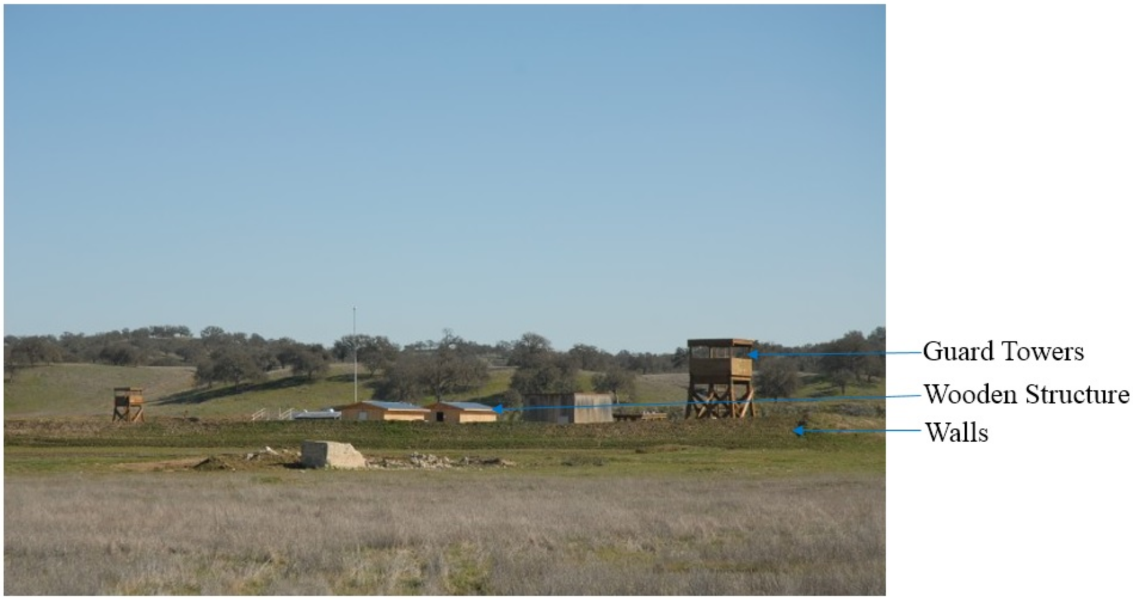


Figure 1. Camp Roberts National Guard Base—Replica Combat Outpost

D. SCENARIOS

Scenarios are conducted during daylight hours and are where the red cell and blue cell come together to provide a feedback to the data collection team on system performance and how the technology performed against the enemy. Scenarios are the setting for the operational assessments that white cell undertake. Adaptive Red Team establishes a sequence of operational activities prior to execution, which provide a logical, realistic progression of scenarios in a hostile area. Blue cell executes the scenarios and utilizes realistic mission statements providing the commander's intent.

The operational missions that are provided in the mission statements are chosen based on the technology selected for each assessment. An example of a realistic mission that blue cell performs in enemy territory on the outpost is entry control point (ECP) operations. Entry-control point operations are where blue cell members operate an entry control point of the combat outpost using a variety of specific technology selections. This entry area serves as the primary entrance for all personnel on the outpost and allows for realistic flow of personnel when performing the scenario. Red cell members are intermingled into the flow of personnel entering. This intermingling allows the blue cell soldier who is operating the equipment a realistic approach used by the enemy. Red cell members sometimes hide suspicious packages or other devices in some manner based on enemy TTPs. This entry-control point activity becomes progressively more difficult to detect based on decreasing the size and location of the suspicious package, number of red cell member's incoming, and stacking of red personnel with unsuspecting personnel to mask the suspicious device during entry.

E. OLD PROCESS OVERVIEW

The initial process for the execution team was the same process used in the previous field experiments for Special Operations Command (SOCOM). Based on guidance provided by the sponsor, Adaptive Red Team assessments were scheduled to take place quarterly. This quarterly schedule allowed the execution team to properly plan and execute each weeklong assessment.

Industry and government submit the proper documents for attendance. Industry submits to a request for information (RFI). That RFI is the Adaptive Red Team's legal mechanics to invite Industry to a government-funded assessment. This RFI is published on Federal Business Opportunities (FEDBIZOPPS) website with instructions for how to submit, submission deadlines, and where to submit are provided. Technology developed by the government must be accompanied by a quad chart for each technology that is solicited through a “call for data.” This data call is sent in a quarterly email from ASA(ALT) to the research and development commands leadership. Those commands are responsible for research and development of future Army technology and when applicable to Adaptive Red Team scope they will respond to that email by submitting a quad chart to the execution team to be considered for selection in the upcoming Adaptive Red Team assessment.

The outcome for each Adaptive Red Team assessment is to identify technological limitations and vulnerabilities in those technologies selected to participate with the intent that the technology developers from both government and Industry will invest resources to mitigate those vulnerabilities. Adaptive Red Team neither provides any funding to the participating developers (government or industry) that are selected to attend nor does Adaptive Red Team provide funding for vulnerability mitigation. This funding is outside scope of Adaptive Red Team mission.

1. Adaptive Red Team Planning

Two planning meetings are conducted each quarter and led by the execution team, as show in the Figure 2. The first is the initial planning meeting to select the technologies that have been submitted, select operational mission that are to be incorporated into the scenarios, initial threat TTPs, and any modifications to the generic data collection questions that will be used by white cell members. The second, final planning meeting addresses technology withdraws after selection, any scenario modifications, and threats/TTPs to be used.

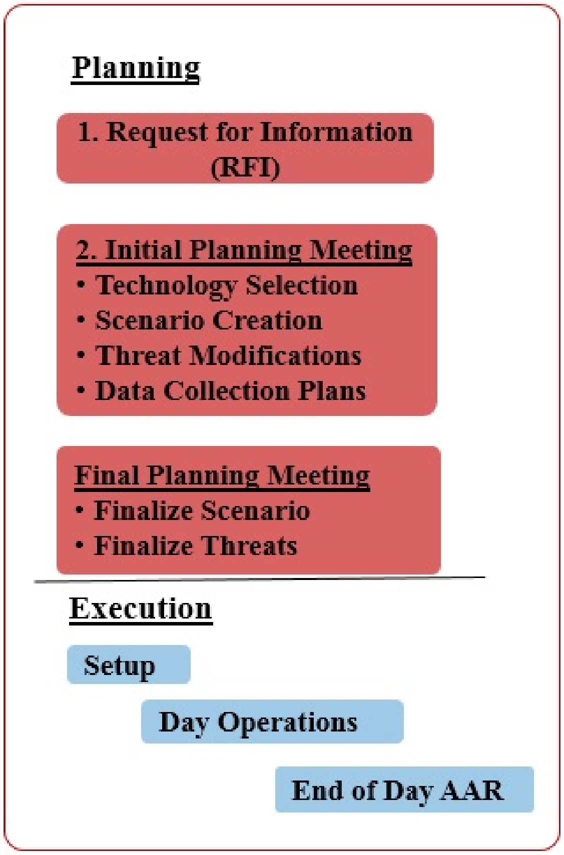


Figure 2. Old Adaptive Red Team process (from Gilkes and Klopfenstein 2014, 3–5)

The outputs of the initial planning meeting are a list of 25 technologies selected for the upcoming Adaptive Red Team assessment, initial data collection questions for white cell, and initial list of scenarios and enemy TTPs that will be used by blue and red cells. The outputs of the final planning meeting are the final list of technology quad charts, final list of scenarios to be executed and enemy TTPs that will be incorporated into the scenarios.

All technologies selected are informed of their acceptance and those not selected are also notified. Representatives associated with the selected technologies are asked to participate in bi-weekly teleconferences to gain a better understating of the Adaptive Red Team process and approach to technology assessments. Schedules, maps, and an initial technology layout showing developers initial setup locations are briefed on the teleconferences.

2. Adaptive Red Team Execution

The middle of Figure 2 outlines the steps that occur during execution week as setup, day operations, and end of day after action reviews. Setup begins on Saturday prior to the execution week in order to ready the combat outpost for the developers who arrive on Monday.

During setup, a tent is utilized as the blue cell tactical operations center. This operations center serves as the command post for all blue activities. When applicable to the technology, its information is transmitted over a wired and wireless network back to the operations center for utilization in the scenarios for tactical decisions.

The following Monday is the first meeting with all technology developers present. A range safety briefing is given to all in attendance, and an Adaptive Red Team overview and a picture briefing of what it is like to live on a small combat outpost by a recently deployed soldier is provided. This picture briefing helps developers understand the limitations and challenges of living in a remote outpost. For example, developers sometimes think a soldier has ready access to all tools required for assembly of their technology or that if a fastener is dropped when putting something together, the soldier can just go get another one. This picture briefing is an effort to raise awareness of those challenges in order to motivate developers to incorporate innovative solutions that address the challenges. After the Monday meetings, all developers gather equipment and begin initial setup. This initial setup begins the data collection discovery assessments, which are performed by white cell members.

At the end of every day, an after action review (AAR) is conducted to discuss the day’s events. The AAR agenda includes administrative comments by execution team followed by the blue cell, red cell, white cell, and then each technology. White cell lead makes sure all technologies have met their data collection team, while blue and red cells discuss the scenarios that were executed that day. Each soldier speaks about the technology on which they were trained, and how well it performed during the specific missions. As the blue cell soldiers provide feedback, red cell members describe the TTPs they used and how effective they were from a red perspective, if known. Blue cell soldiers fill in the gaps on the red TTPs effectiveness. All of this information is captured by the appropriate white cell data collection team and, if addition clarification is required, a separate interview with blue and/or red cell is conducted. After the AAR, technology developers have an opportunity to share any significant accomplishments of the day. Figure 3 below represents the old Adaptive Red Team execution process and how all the cells interacted. Discovery assessments are executed by the white cell data collection teams on each assigned technology. When each data collection team successfully answers the list of questions in the data collection plan, the technology is allowed to proceed to the scenarios. The technology is provided by the developer to the blue cell for operation in the scenario. Blue cell soldiers operate the technology in the scenario to understand the operational effectiveness against the red cell. Subsequent scenarios for each particular technology will become progressively more complex. This complexity allows the red cell members to become more aggressive and adaptive using evasion techniques to resist detection or cover and concealment to slip past a sensor all utilizing enemy TTPs.

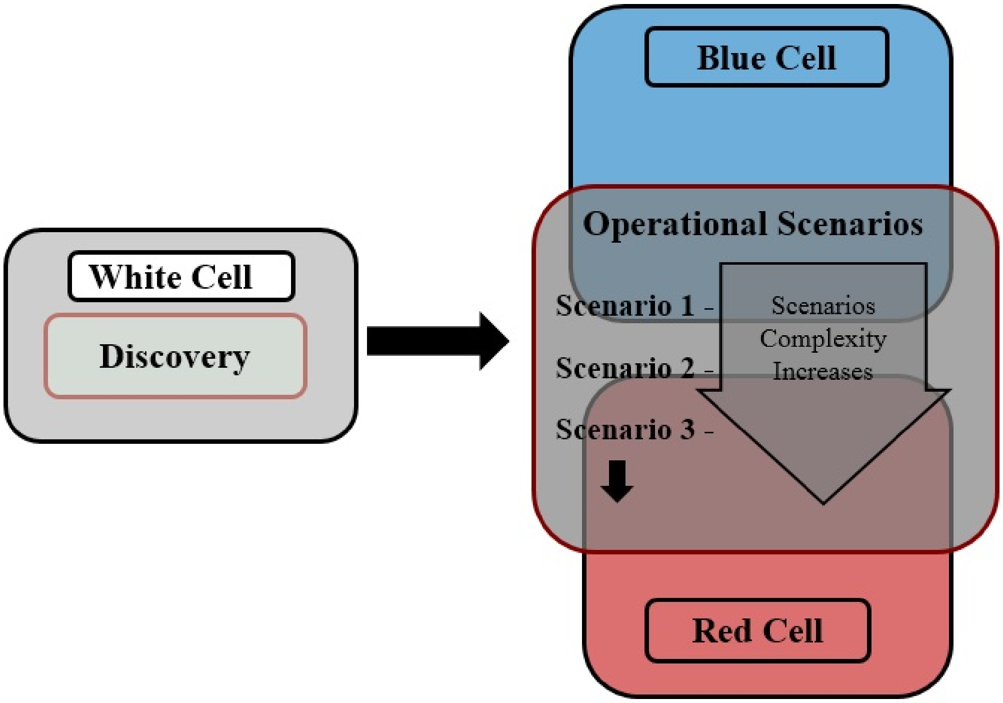


Figure 3. Old Adaptive Red Team Execution (from Gilkes and Klopfenstein 2014, 3–5)

The execution team leveraged a previous process, combined with some red-teaming concepts learned during a two-week red-teaming course, to develop and implement the process outlined above. This process was ineffective and did not meet the sponsors' requirements to provide an adaptable, repeatable process used to assess technology limitations and vulnerabilities through the perspective of an adaptive and complex enemy. A new process was needed to meet this requirement.

V. SYSTEM THINKING APPROACH

In order to execute fully an Adaptive Red Team mission per the stakeholders' guidance, a new process had to be established based on systems engineering principles. This new process needed to take into account the following stakeholder requirements:

- Create a repeatable process that provides a quantitative snapshot of technology.
- Increase threat emulation capabilities in order to uncover additional vulnerabilities and system limitations.
- Increase collaboration between government and industry.

The requirements are addressed individually to provide an actionable path forward that can be executed.

A. REPEATABLE PROCESS PROVIDING A QUANTITATIVE SNAPSHOT OF TECHNOLOGY

When engineers begin a project, many design approaches, methods and materials are traditionally considered. Those approaches are called tradeoffs. Some tradeoffs may include material choice, selection of components, others may include button layout and titles in a graphical user interface (GUI) and, finally, some tradeoffs may include types of encryption or methods of data exfiltration. The boundaries of those tradeoffs delineate and are considered the tradespace.

The Adaptive Red Team execution team created a process called the tradespace methodology to assess a technology's current development state and level of alignment with soldier expectations that influence successful fielding and acceptance. The tradespace methodology employs science and engineering expertise, coupled with hands on soldier training, system use, and operational observations during scenarios, to estimate the potential value return and potential risk of technology based on the scoring of specific factors.

The factors, shown in Figure 4, are examined when the tradespace methodology is used to assess technologies:

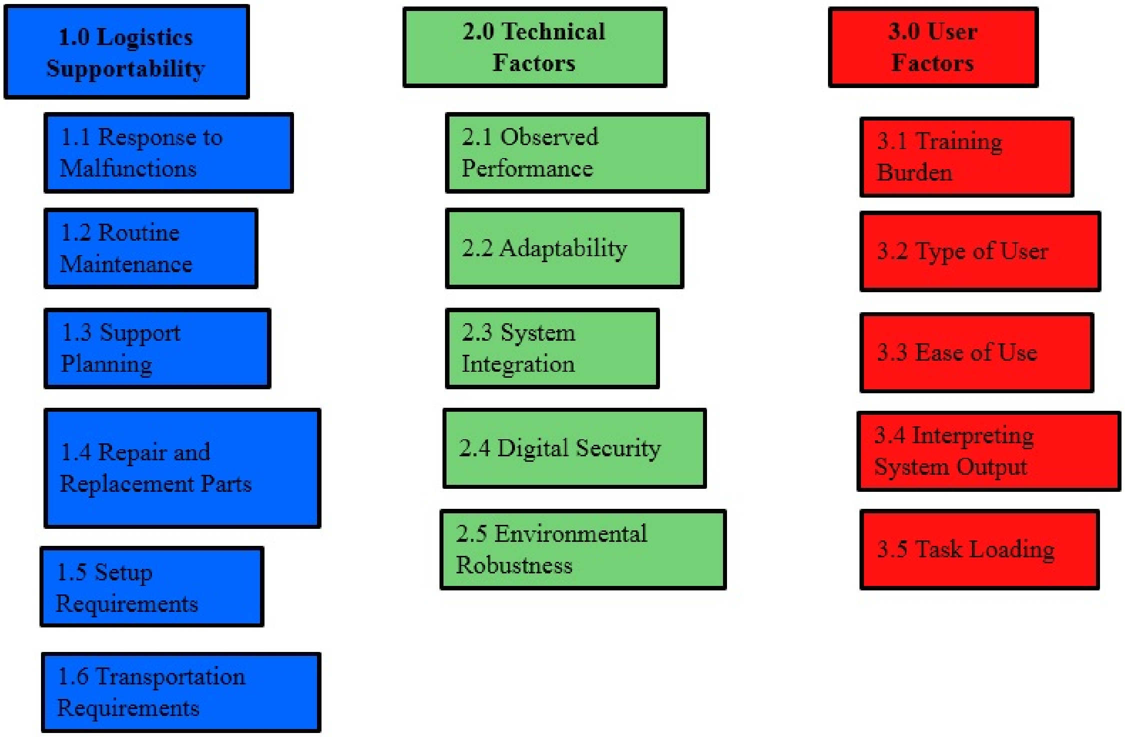


Figure 4. Tradespace Methodology Decomposition
(from Klopfenstein and Tober 2014, 107–122)

After many discussion with soldiers, feedback from recently deployed soldiers, and discussion among the Adaptive Red Team execution team, the top-level factors and subfunctions were defined for technology acceptance by soldiers.

The logistics supportability factor is designed to assess a technologies operation readiness and the components, procedures, and transportation required to remain operational. The subfactors associated with logistics supportability include response to malfunctions (Log Factor 1), routine maintenance (Log Factor 2), support planning (Log Factor 3), repair and replacement parts (Log Factor 4), setup (Log Factor 5), and transportation requirements (Log Factor 6).

As an example, Log Factor 1: response to malfunctions is further broken down to the bulleted list below with a specific list of answers for each. Answers are selected based on white cell data collection teams' interaction with technology developers, blue cell who used the technology in scenarios, and red cell who opposed it.

- Log Factor 1—response to malfunctions
  - required location for troubleshooting/repair
  - tools required to troubleshoot/repair
  - skills required to troubleshoot/repair
  - added risk to soldier by performing troubleshooting/repair

Discussions about the above factors determine the score to Log Factor 1—response to malfunctions.

Technological factors are designed to capture the actual performance as observed based on developer's stated capabilities, and how adaptable, secure, and robust.

The subfactors associated with technological include observed performance (Tech Factor 1), adaptability (Tech Factor 2), integration into common operational picture (Tech Factor 3), digital security (Tech Factor 4), and environmental robustness (Tech Factor 5).

Tech Factor 1: observed performance is further broken down into the bulleted list below, with a specific list of discussions for each. Answers are selected based on the white cell data collection teams' interaction with technology developers, blue cell who used the technology in scenarios, and red cell who opposed it.

- Tech Factor 1—observed performance
  - comparison to stated capability from developers submitted paperwork

Ten answers are available for the stated capability allowing a direct correlation to a number score of one to ten for Tech Factor 1.

The user factor is designed to assess a technologies ease of use and understanding of the output. The subfactors associated with user factor include training burden (User Factor 1), required type of user (User Factor 2), ease of use (User Factor 3), and interpreting the output (User Factor 4).

User Factor 1: training burden is further broken down to the bulleted list below with a specific list of answers for each. Answers are selected based on white cell data collection teams' interaction with technology developers, blue cell who used the technology in scenarios, and red cell who opposed it.

- User Factor 1—training burden
    - type of trainer required
    - geographic location of required training
    - required time to train

Answers to the above will determine the score to User Factor 1, training burden.

Each log factor, technical factor and user factor have a set of information to be collected; above are just examples of one factor per area.

The information for each factor is translated into numerical values, or factor scores, as each white cell data collector first assigns a most likely (ML) score to communicate their estimate of the current system state on a particular factor after analyzing all available information. Recognizing both the limited interaction time and the developmental nature of many of the technologies participating at Adaptive Red Team, each data collector assigns estimated low (EL) and estimated high (EH) scores that bracket each factor ML score. These numerical scores are used to capture the level of individual uncertainty associated with a reported factors ML score.

All of the subfactors scores are averaged into one numerical value for each factor. For example, all six subfactors scores for factor logistics supportability are averaged to formulate a single ML score per data collector for logistics supportability. This averaging process is applied to the ML, EL and EH values and provides a three separate scores for logistics, technological, and user factors.

All technologies at an Adaptive Red Team event are combined into one spider chart. The spider chart segregates the average ML scores for each factor (technical, logistic, and user) to expose potential strengths along with possible risks requiring mitigation. All tradespace factors are converted to a percentage; for example, a score of 6.1 will become 61% in the spider chart. The higher the percentage per factor, it is assumed each technology is less vulnerable.

The second output of the tradespace methodology is a whisker plot that represents the range of uncertainty from best case high score (EH) to worst case low score (EL) per technology across all data collectors scores. The EH score is used at the top end for the range of uncertainty and the EL is used to define the end point on the range of uncertainty. The EH and EL scores are used to represent the range of uncertainty for each subfactor’s ML score.

B. INCREASE THREAT EMULATION CAPABILITIES

The primary stakeholder determined that the ART process lacked desired threat emulation capabilities. This lack of capabilities was not allowing Adaptive Red Team to adequately emulate the threat and meant technologies were not exposed fully to adaptive and complex threats.

Adaptive Red Team addresses this stakeholder requirement by several methods, including additional red cell training, hiring additional experts, and increasing threat equipment. Table 1 below outlines the objectives needed to accomplish the goal of increase threat emulation capabilities.

Table 1. Goals and Objectives to Increase Threat Emulation Capabilities

Requirement	Objective
Increase Threat Emulation Capabilities	Assign Permanent Red Cell Lead
	Obtain Ethical Hackers
	Obtain Electronic Warfare (EW) Experts
	Design/Purchase Threat Equipment
	Utilize Threat Uniforms/Weapons

Training to become a red cell lead is provided by Training and Doctrine Command (TRADOC) Operational Force (OPFOR) academy, which leads to certification as a red cell expert. This training provides a process for specific threat systems and this process helps set the stage for all Adaptive Red Team red cell activities. The process is flexible to allow red cell adjustments in the complexity of red cell activity for the scenarios, which adds adaptability and complexity to the scenarios and Adaptive Red Team process.

Subject matter experts can be added to the team to provide specific expertise as required. For example, support for understanding the ethical hacker and electronic warfare expertise may be outside the domain expertise of red team members. The ethical hackers are considered computer network security experts (CNS) that are specifically geared to understand and utilize enemy software, hardware, and TTPs. The open source software and commercial hardware from many foreign countries are the tools that many hackers across the world use every day to discover system exploits, passwords, or other vulnerabilities.

For example, a CNS team has the ability to assess vulnerabilities in the enterprise network, webservers, satellite communications, unmanned vehicle command and control, encryption (AES 256/WEP. WPA2), smart phones/tablets, and social media networks.

These vulnerabilities can be identified by such things as denial of service, man in the middle attacks, rootkits, and Trojans.

A denial of service (DoS) attack is when a hacker prevents users from accessing specific services. This threat is accomplished by attacking your computer and network or the computer and network from the service you are trying to obtain by effectively overloading the communications media making legitimate traffic difficult to reach the intended destination.

Man in the middle attacks are when a hacker gets between a legitimate user and the regular flow of information. This hacker is now in the middle of the communication stream and has the ability to “see” all traffic flow. This information may contain passwords, location of friendly troops, sensors positons, or other sensitive information.

A rootkit is a collection of software that when installed as a regular user enables administrator level access. This technique upgrades administrator access to allow a hacker to gain additional access to different computers, servers or other networks only assessable my administrators.

Trojans are designed to appear as useful software but will cause damage when installed on a computer. Trojans vary in damage and some may delete files or others will rearrange your desktop. This vulnerability leaves computers and the networks they access open to complete take over and control leaving all data compromised.

Electronic warfare experts in threat technologies can be obtained to address vulnerabilities in radio frequency (RF) based technologies. These experts look for vulnerabilities in the RF spectrum by techniques such as low power jamming, high power jamming (when applicable), off center frequency jamming, and waveform manipulation.

Jamming is accomplished on technology that communicates through the RF spectrum. This communication is done by creating a waveform on or close to the center frequency on a signal generator and broadcasting that signal back to the technology being assessed. Low power jamming is accomplished by little to no signal amplification and high power uses amplification. Off-center jamming occurs by creating a waveform that is a specific frequency offset from the center and then broadcast back to the technology being assessed.

Waveform manipulation is a technique where RF data is recorded from the target device. This recoded waveform can then be manipulated using software to adjust specific parameters of the waveform in an effort to trigger the technology being assessed or possibly mask a trigger.

Technologies respond to different techniques in different manners as some are compromised, while others are not, depending on the level or hardening, shielding, and electrical design.

To address threat equipment and weapons, the execution team with additional input from previously deployed soldiers, formulates a list of the most likely equipment used against a combat outpost.

Table 2. Common Threat Equipment Used and Purpose

Threat Equipment/Weapons	Purpose
GPS Jammers	Disrupt GPS Signals
Mobile Phone Jammers	Disrupt Mobile Phones
AK-47	Realistic Targets
Rocket Propelled Grenades (RPGs)	Realistic Targets

Low powered GPS jammers and mobile phone jammers would be designed and built by the adversary's EW experts. These threat technologies will be utilized by red cell in scenarios in order to discover vulnerabilities of assessed blue cell technologies previously not being accessed.

Threat weapons can be purchased from a vendor specifically selling accurate, non-operational replicas of threat weapons. These weapons have the same look, feel, weight, and other properties of originals, but they are just not fully functional. These targets will be used by red cell in the scenarios and assist specific technologies in weapon detection and identification. The realistic nature will allow red cell to be creative in its deception techniques using the red force (enemy) TTPs.

The threat equipment and realistic weapons will add a layer of realism and adaptability not previously part of the Adaptive Red Team process. These additions allow the Adaptive Red Team to increase complexity of scenarios and uncover additional vulnerabilities and satisfy the remaining part of the requirement to increase threat emulation capabilities.

C. INCREASE COLLABORATION BETWEEN GOVERNMENT AND INDUSTRY

Adaptive Red Team execution team looks for ways to both increase collaboration and decrease barriers to collaboration with industry and government developers. Collaboration is an approach that describes two or more technology developers working together to increase each developers capabilities. If collaboration is increased, the government should be able to get better products by including more feature sets in a particular technology, or enhancing current feature sets with better algorithms, or using other analysis tools from a different company other than those that are participating in Adaptive Red Team.

1. Barriers to Collaboration

One barrier to collaboration in the old Adaptive Red Team process for technology developers was what the next steps were carried out after they had participated in an event. Adaptive Red Team is a government-funded program that is an information provider on developing technologies' limitations and vulnerabilities. Adaptive Red Team does not provide funding for developer's participation or vulnerability mitigation. However, Adaptive Red Team is an information provider in the form of executive summaries, quick look reports, and a final report to Adaptive Red Team sponsors and others within government. This information is now provided to government and industry developers, in bi-weekly teleconferences. Communicating this previously unknown information should increase collaboration, as developers are not vying for additional funding sources.

Adaptive Red Team makes an attempt to decouple the company from the technology by not allowing banners/plaques or other branding, as the events are not trade shows or technology demonstrations. Adaptive Red Team uses technology names in all technology lists and formal outputs, but not company/organization names. This approach allows for all developing organizations to interact freely and feel like everyone is on the same team supporting the U.S. Army.

2. Methods to Increase Collaboration

Adaptive Red Team selects 25 technologies to participate in the weekly events. Previously, there were no introductions of the 25 technologies to members of the cells. The new Adaptive Red Team process implements a technology developer introduction. This two-minute introduction allows technology developers to understand what other participants are developing. This change provides an understanding of the other participants and there technologies as a first step toward future collaboration.

During the end of day AARs, each technology debrief must include any collaboration attempted or accomplished. This reinforcement of sharing shows all other technology developers that collaboration is acceptable and highly encouraged.

The last method implemented to increase collaboration is geared toward increasing collaboration from the government side. Technology integration was implemented as a way to increase collaboration, reduce stovepipes, and reduce costs spent on common operational platforms (also known as situational awareness displays). Integration addresses the ability to use a common data format for information sharing that can be processed and understood by the common operations pictures (COP). Adaptive Red Team uses one standard in particular, called cursor-on-target (CoT), which was development by the U.S. Air Force. This data standard uses an XML schema to address information such as who, what, where, and when allowing integration into Adaptive Red Team COP.

```
      <?xml version='1.0' standalone='yes'?>
      <event    version="2.0"
             uid="J-01334"
             type="a-h-A-M-F-U-M"
time="2005-04-05T11:43:38.07Z" start="2005-04-05T11:43:38.07Z" stale="2005-
                              04-05T11:45:38.07Z" >
         <detail>
         </detail>
         <point lat="30.0090027" lon="-85.9578735" ce="45.3" hae="-42.6"
                         le="99.5"                              />
      </event>
```

Figure 5. Sample CoT Schema (Kristan 2009, 2–1)

This sample CoT schema shows the layout for a particular type of information (lat/log) formatted to meet CoT standards. Sample CoT schema listed below:

- UID—Unique identification for this information that typically shows up in the COP next to representative icon
- Type—this represents the type of information such as friendly force/vehicle/ tank getting more specific as the sting continues
- Time—when the event was created
- Start—time when event is valid
- Stale—ending time when event is no longer valid
- Point Lat—latitude
- Lon—longitude

- Ce—circular area around the point (if desired)
- Hae—height above point (if desired)

Table 3. Summary of Actions Traced to Stakeholder Requirements

Stakeholder Requirements	**Objective**	**Action**
Repeatable process providing a quantitative snapshot of technology	Implement Quantitative Process	Tradespace methodology using logistics, tech factors and usability as technology acceptance tradespace
Increase threat emulation capabilities in order to uncover additional vulnerabilities and system limitations	Improve Red Cell	Permanent Red Cell Lead
		Increase Red Cell Training
		Increase Red Cell Threat Equipment (Jammers/UAV)
		Increase Red Cell Uniforms and Weapons (state/non-state uniforms/AK-47/RPGs)
	Improve Red Cell Electronic Attack	Increase expertise in threat computer network security
		Increase expertise in threat electronic warfare
Increase collaboration between Government and Industry	Increase Collaboration with Industry	Institute bi-weekly teleconferences to increase information flow and understating of ART
		Provide two-minute technology introductions at beginning of execution week.
	Increase Collaboration between Government	Institute bi-weekly teleconferences to increase information flow and understating of ART
		Provide two-minute technology introductions at beginning of execution week.
		Utilize data format standards for integration into government owned COPs

THIS PAGE INTENTIONALLY LEFT BLANK

VI. NEW ADAPTIVE RED TEAM PROCESS BASED ON SYSTEMS THINKING

A. PLANNING

The new Adaptive Red Team process takes advantage of systems thinking in order to address stakeholder requirements. The modified process is shown in Figure 6 does not change the methods for technology submission and selection or planning meeting structure. The new process does reflect the addition of the tradespace methodology, EW/CNS experts, bi-weekly meetings, and, integration and additional red cell threat equipment.

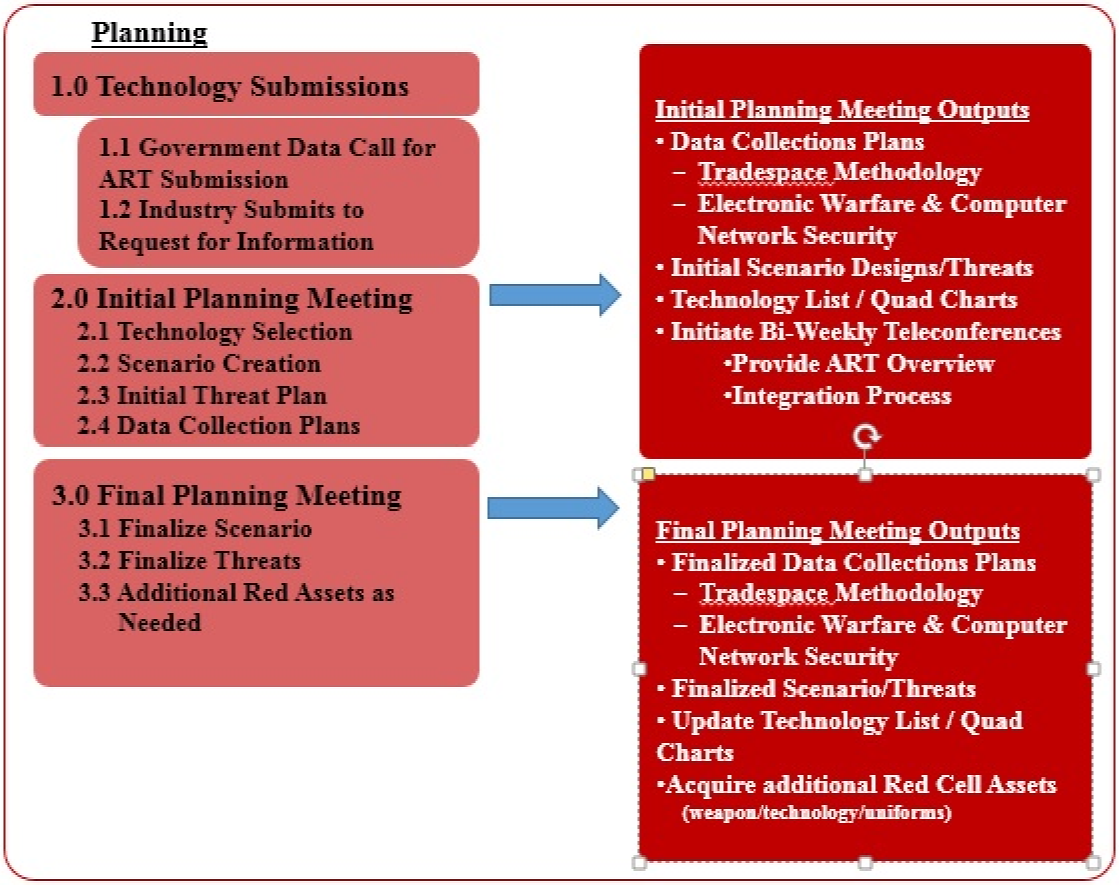

Planning
1.0 Technology Submissions
1.1 Government Data Call for ART Submission
1.2 Industry Submits to Request for Information
2.0 Initial Planning Meeting
2.1 Technology Selection
2.2 Scenario Creation
2.3 Initial Threat Plan
2.4 Data Collection Plans
3.0 Final Planning Meeting
3.1 Finalize Scenario
3.2 Finalize Threats
3.3 Additional Red Assets as Needed
Initial Planning Meeting Outputs
• Data Collections Plans
– Tradespace Methodology
– Electronic Warfare & Computer Network Security
• Initial Scenario Designs/Threats
• Technology List / Quad Charts
• Initiate Bi-Weekly Teleconferences
•Provide ART Overview
•Integration Process
Final Planning Meeting Outputs
• Finalized Data Collections Plans
– Tradespace Methodology
– Electronic Warfare & Computer Network Security
• Finalized Scenario/Threats
• Update Technology List / Quad Charts
•Acquire additional Red Cell Assets
(weapon/technology/uniforms)

Figure 6. Modified Planning Process based on Systems Thinking (from Gilkes and Klopfenstein 2014, 3–5)

Tradespace methodology and EW/CNS data collection plans are started at the initial planning meeting. Tradespace methodology will specifically address the repeatable process providing a quantitative snapshot of technology. The EW & CNS data collection plans are part of the increase threat emulation capabilities.

The stakeholder goal to increase collaboration between government and industry is supported in this new process by adding Adaptive Red Team overview that addresses barriers to collaboration in the bi-weekly teleconferences. Integration process is also now discussed at the bi-weekly meetings with specifics given on CoT data standard, how to get access and assistance with CoT verification.

Final planning meetings are conducted to wrap-up any last minute details on technology drops that lead to data collection plan and scenario modifications. A list of additional red assets are compiled and acquired each quarter to support the increase threat emulation capabilities. This equipment will allow uncovering of additional vulnerabilities and system limitations to meet the stakeholder requirement.

Several items not part of process modification but required to meet stakeholder objectives are administrative in nature. These include the assignment of a permanent red cell lead instead of a rotational basis and annual training to continually to evolve this threat skillset.

B. EXECUTION

The new Adaptive Red Team execution process, as shown in Figure 7, provides an overview of event execution and how each cells function together. This new process begins with the same discovery method from the old Adaptive Red Team process, but combines the new tradespace methodology and EW & CNS data collection. When each data collection team successfully answers the list of questions in discovery, tradespace methodology, and EW &CNS data collection plans, they have cleared the first hurdle to insertion in the scenarios.

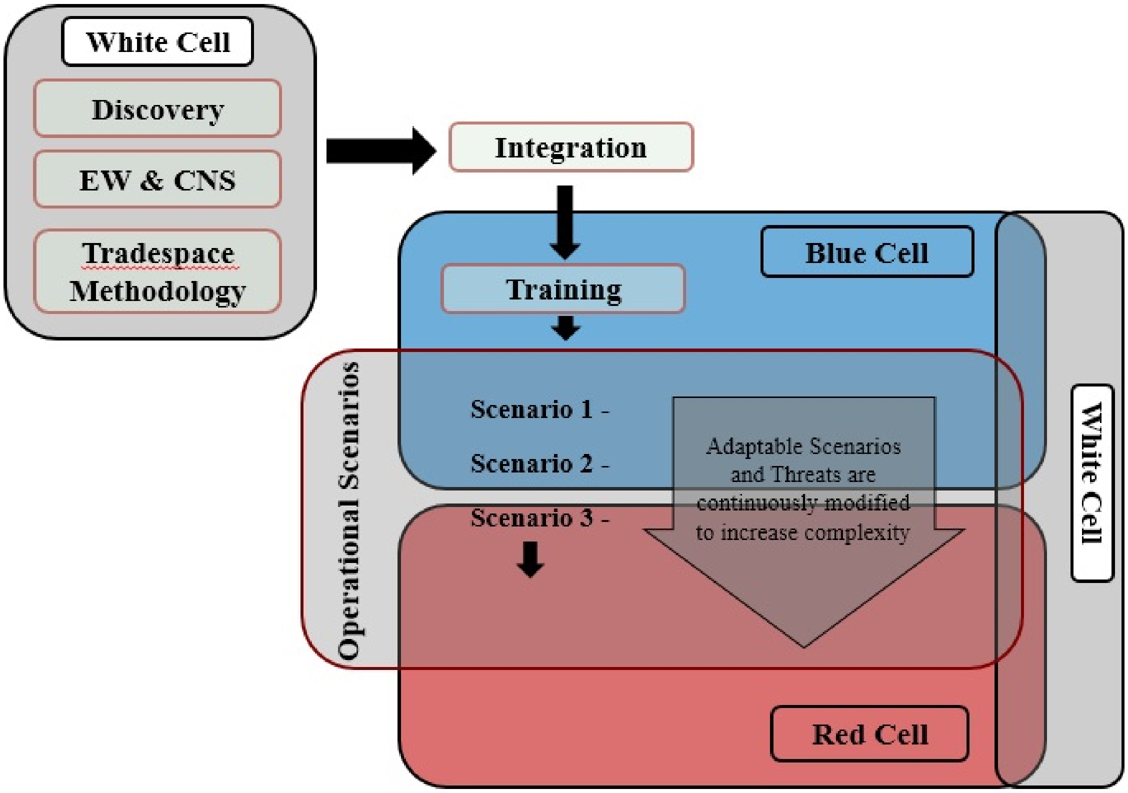


Figure 7. New Adaptive Red Team Execution and Cell Interaction (from Gilkes and Klopfenstein 2014, 3–5)

Integration is a process that begins during the bi-weekly teleconferences when information is provided on the CoT data standard. Developers begin integration at their home stations in an effort to maximize time on the ground, so final integration and verification is done in parallel with the white cell data collection efforts.

Once integration has been verified, technology training begins. This technology training is executed by the technology developers to the blue cell members who will be operating the equipment during the scenarios. When training is complete, soldiers take possession of the technology and begin loading it for the upcoming scenarios.

Each scenario becomes progressively more complex from a red cell perspective, by utilizing enemy TTPs, new threat equipment, or exploiting a vulnerability found by the EW & CNS data collection team. The approach, procedures, and the complexity emulates real world adversaries and the equipment they use. Blue cell members are provided the flexibility to adapt and try new uses for the technology as threat complexity increases. In some cases, technology is raised and placed on a platform at an entry control point out of a potential blast zone of a suicide bomber entering the compound. The now elevated technology is not destroyed and allows for the detection of incoming red cell threats. During the scenarios, white cell members continue to collect valuable information on how the technology did or did not perform, on the adaptability of blue cell members, and the techniques/equipment used by the red cell.

This new Adaptive Red Team process allows the Adaptive Red Team to become truly adaptive and potentially more effective at discovering vulnerabilities.

VII. NEW ADAPTIVE RED TEAM PROCESS INITIAL RESULTS

Three major process improvements to support stakeholder requirements are implementation of tradespace methodology, the addition of electronic warfare and computer network security experts, and the introduction of an integration standard.

A. TRADESPACE METHODOLOGY INITIAL RESULTS

Previous Adaptive Red Team assessment employed a tradespace methodology across all technologies. The spider chart shown in Figure 8 utilizes the averaged Most Likely (ML) scores for each tradespace factor—Logistical, User, and Technical—to expose system strengths along with possible risks requiring mitigation should the system be acquired in its current state of development.

Adaptive Red Team tradespace methodology baselines average ML results by evaluating tradespace factors for each of the twenty-nine (29) technologies on a 100% scale in which higher scores indicate a greater degree of alignment with soldier expectations.

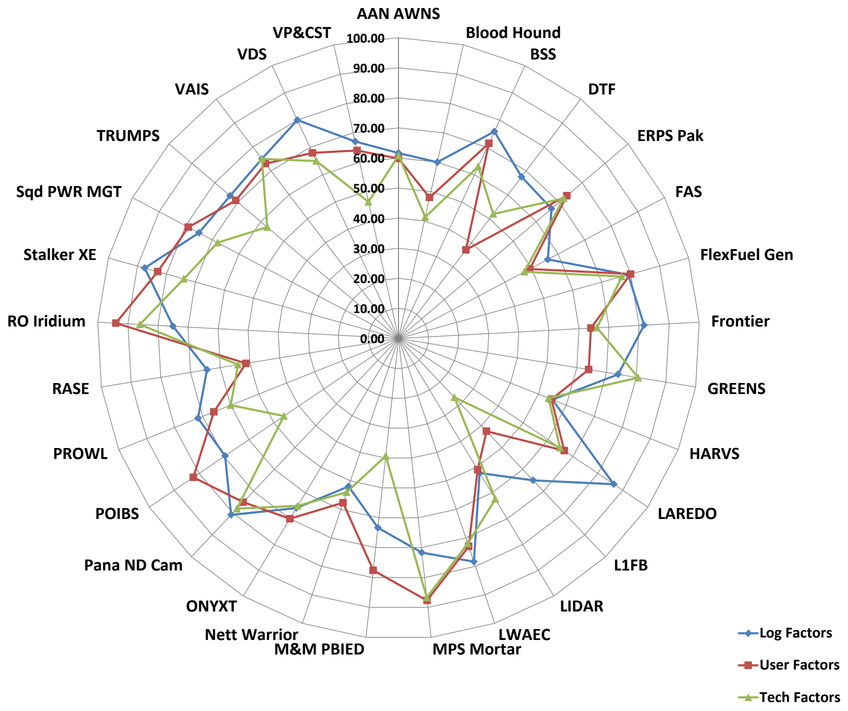


Figure 8. Adaptive Red Team event 14–2 Most Likely (ML) average per tradespace
(from Klopfenstein and Tober 2014, 107–122)

The blue line represents log factors averaged ML scores. They are averaged from the individual ML scores of log factors 1–6. This logistics score is plotted as the blue line on the spider chart for each technology. The same process is repeated for the ML user factor and the ML technology factor. ML user factor is compiled from the averaged individual scores of user factor 1–5 and plotted in red on the spider chart for each technology. The green line represents the technology factor and uses the averaged ML scores from each technology factors 1–5. Based on interpreting the above spider chart the following were assessed to have high likelihood of technology acceptance:

- Expedition Recon Patrol Squad Pak (ERPS Pak)
- Flex Fuel Generator
- Lightweight App-enabled Computer (LWAEC)
- Mobile Protection System Mortar Pit (MPS Mortar)
- Panoramic Night/Day Camera (Pana ND Cam)
- RO Iridium Radio (RO Iridium)

- Stalker XE UAS (Stalker XE)

Conversely, several systems appear to require changes to accommodate technology acceptance:

- Blood Hound
- Distributed Tactical Fires (DTF)
- Fencepost Acoustic System (FAS)
- Human Activity Recognition in Video Streams (HARVS)
- Level 1 Fusion in a Box (L1FB)
- Lidar Based Facial Recognition (LIDAR)
- Nett Warrior
- Reconnaissance Advanced Sensor and Exploitation (RASE)

Additional results are provided for one system that exhibited a high percentage of technology acceptance and one technology with a lower percentage of technology acceptance. Flex fuel generator scored approximately 70% technology acceptance, based on the three factors surveyed. LIDAR based facial recognition, which scored approximately 40% on the averaged ML logistics and user factors, and approximately 60% on technology factors.

1. Flex Fuel Generator

Flex fuel generators (FFG) as seen in Figure 9, is a power generation capability that can utilize a combination of fuels for operation. This multi-fuel power source can be used with compressed and liquid fuels, including light and heavy distillate fuels. The FFGs agnostic fuel architecture allows for the use of a variety of fuels in any combination.

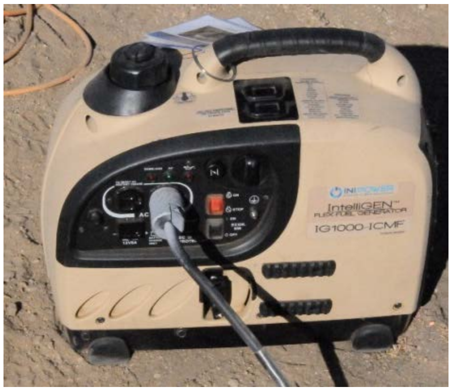
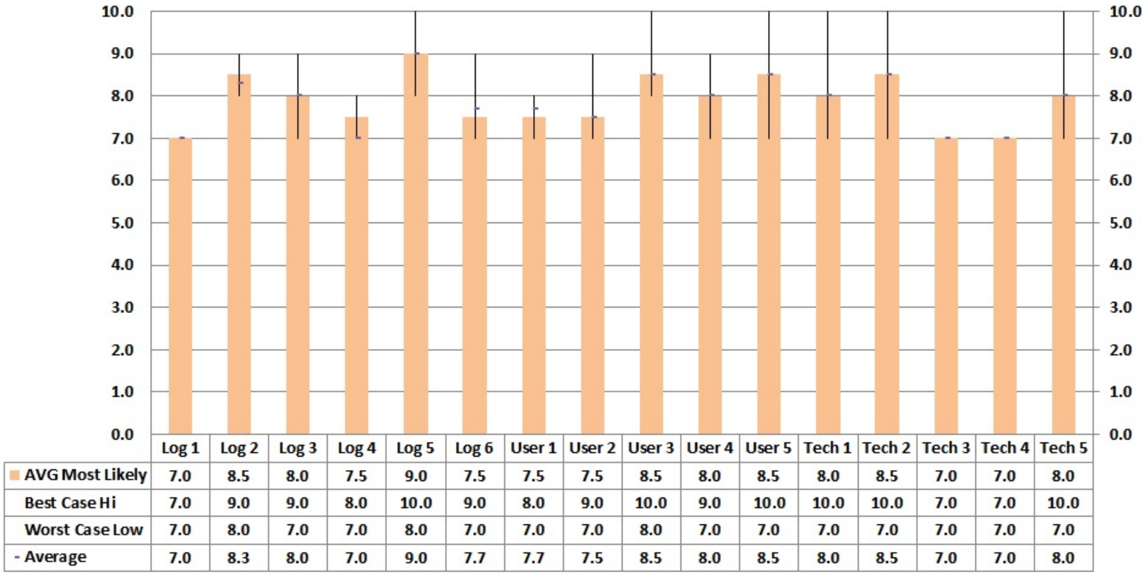


Figure 9. 1 kW Flex Fuel Generator

The spider chart plots the averaged ML score for each factor. This ML score may present some uncertainly that is captured in the estimated high (EH) score and estimated low (EL) score. This uncertainty is presented in Figure 10 and shows two key statistics for each tradespace factor.



	Log 1	Log 2	Log 3	Log 4	Log 5	Log 6	User 1	User 2	User 3	User 4	User 5	Tech 1	Tech 2	Tech 3	Tech 4	Tech 5
▨ AVG Most Likely	7.0	8.5	8.0	7.5	9.0	7.5	7.5	7.5	8.5	8.0	8.5	8.0	8.5	7.0	7.0	8.0
Best Case Hi	7.0	9.0	9.0	8.0	10.0	9.0	8.0	9.0	10.0	9.0	10.0	10.0	10.0	7.0	7.0	10.0
Worst Case Low	7.0	8.0	7.0	7.0	8.0	7.0	7.0	7.0	8.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0
- Average	7.0	8.3	8.0	7.0	9.0	7.7	7.7	7.5	8.5	8.0	8.5	8.0	8.5	7.0	7.0	8.0

Figure 10. Individual Tradespace Methodology subfactor assessment and uncertainty score (from Klopfenstein and Tober 2014, 107–122)

The first of these key statics is simply the average most likely (AVG Most Likely) score for each tradespace factor. A solid bar is used to indicate the level of this measure. The AVG Most likely score is the average of all the data collectors score for that specific category (i.e., Log 1). Higher scores are associated with a greater degree of technology acceptance. The second key static is the whisker plot that represents the range of uncertainty in the AVG Most Likely from best-case high score to worst-case low score. The best-case high (Best Case HI) score is the highest score, not averaged, from all data collectors on a given category. The worst case low (Worst Case Low) is the lowest score, not averaged, from all the data collectors on a given category. The shorter the black line the more certain the white cell is of the assessed most likely value. Log factor one, tech factor three and four represent almost no uncertainty from the averaged most likely score. Tech factor five (Tech 5) averaged most likely score is eight; the range of uncertainty for this category is as high as ten and as low as seven. The lowest score of all the data collectors estimated low (EL) is a seven with the estimated high (EH) being a ten. Overall, this technology has high degree of technology acceptance.

B. ELECTRONIC WARFARE AND COMPUTER NETWORK SECURITY

The EW & CNS team specializing in threat vulnerability analysis are part of the new Adaptive Red Team process to uncover vulnerabilities and system limitations.

Utilizing the tools described above these experts assess all technologies at an Adaptive Red Team assessment that connect to any wireless/wired network, send/receive a radio signal or have incorporated a computer of any type. Vulnerability assessment results are provided for one technology that scored in the middle of the tradespace methodology.

1. Frontier II Low Visibility Friendly Force Tracker Overview

Frontier II, show in Figure 11, low visibility friendly force tracker (LVFFT) is a tagging, tracking, and locating (TTL) device primarily intended for low visibility applications, but can be also used for hostile force tracking (HFT) and other friendly force tracking (FFT) applications. Positional and sensor data are autonomously transmitted from the remote device to the command post or other COP based on configuration.

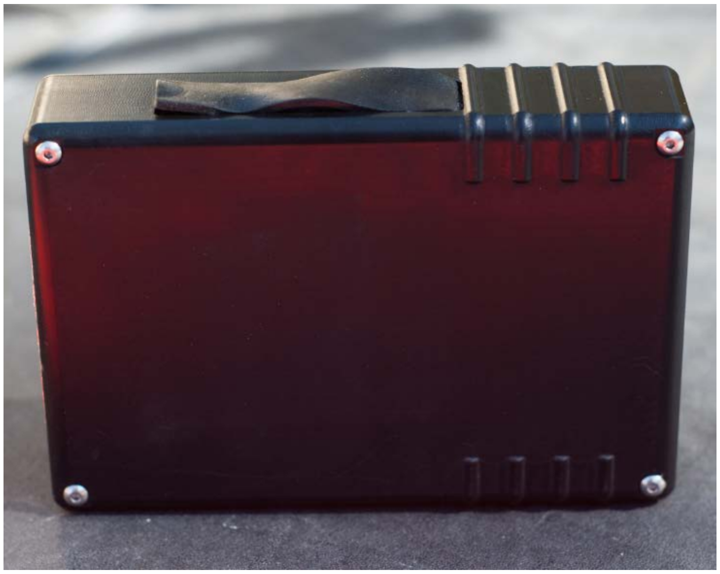


Figure 11. Frontier II LVFFT Device (from Klopfenstein and Tober 2014, 107–122)

2. EW & CNS Assessment of the LVFFT

EW & CNS white cell performed a passive assessment against a single Frontier II LVFFT laptop server running the command post software located in the operations center. The passive assessment included system footprinting, enumeration, and vulnerability scans.

Footprinting and enumeration network scans were executed using Nmap and Softperfect, both of which are open source network mapping software running on Windows (trademarked by Microsoft Corporation) and Linux. Vulnerability scans using open source scanners named OpenVAS, xProbe2 and Nessus were utilized.

Footprinting and enumerating a target system refers to the adversary's ability to identify their target and gather information for an attack or escalation of an attack. From the Adaptive Red Team network, EW & CNS data collectors were able to locate the Frontier II LVFFT server using xProbe2 and Nmap. Nmap provided a network scan for the 192.168.112.xxx network, identifying the command post server's Internet protocol (IP) address of 192.168.112.28 system. xProbe2 was then used to validate the findings.

Enumeration proved to be difficult as EW & CNS white cell discovered the system had implemented strong security measures, including port filtering. Table 4 displays the information acquired from the port scanners.

Table 4. Enumeration Results for 192.168.112.28

Host Name	Open Ports	MAC Address	System/OS
Mcp803800-pc.tsoa-PTR	1000: Filtered	DE:BE:D9:27:04:72	Dell/Unknown

The limited amount of information provided in Table 4 illustrates the difficulty enumerating the Frontier II LVFFT system, as all of the open ports were filtered and not reporting. EW & CNS white cell were only able to collect readily available network data, such as the domain name system (DNS) host name, the media access control (MAC) address, and the name of the manufacturer derived from the unique MAC address.

Vulnerability validation was accomplished against the .28 system. EW & CNS white cell used Nessus and OpenVAS open source and commercially available vulnerability scanners to identify and validate exploitable vulnerabilities.

Two informational notes and no vulnerabilities were identified. The informational notes further validated the enumeration findings, the DNS host server name, the MAC address, and the computer manufacturer. Due to the security in place, the EW & CNS white cell discontinued their attempt to further enumerate the Frontier II LVFFT command post laptop server.

Using open source software and commercial laptops, the adversary would not be able to successfully enumerate the Frontier II LVFFT system. A denial of service (DoS) attack was not attempted on the Adaptive Red Team network.

3. EW & CNS Assessment Summary

Using multiple enumeration and vulnerability tools, EW & CNS white cell were unsuccessful in identifying exploitable vulnerabilities associated with the targeted system. The .28 server was secured with local security, including port filtering, which prevented thorough and accurate enumeration of the target system. The only findings included the systems DNS host name, MAC address and manufacturer, which provided no actionable data for the adversary.

This vulnerability analysis accomplished by the EW & CNS white cell is similar to the TTP used by our enemy to exploit our technology. Understanding the vulnerabilities in developmental technologies provides the developer an actionable list for mitigation.

C. COLLABORATION AND INTEGRATION

Collaboration and integration are two different components of an Adaptive Red Team event but both try to accomplish the stakeholder goal of increasing collaboration between government and industry. Some technologies have the ability to integrate in to the COP such as an unmanned aerial vehicles, tracking, tagging and location devices, and unattended ground sensors. These examples provide an output that can be consumed, georeferenced, and displayed in the COP.

Collaboration is a method that shows interaction between participating technologies. Power sources such as generators, wind turbines, and solar panels are examples of technology that have high collaboration potential.

Using two of the technologies discussed above, Adaptive Red Team initial results will show one integrated with the COP and the other collaborated with other developers. Integration is important because it allows the information flow to be standardized and shown on one COP. A COP is a computer running situational awareness software that is connected to a large display in the operations center. When all information can be shown on one display, this minimizes the need to look at separate computer screens to understand the battle flow. Potentially, this displayed information allows for quicker decisions and better understating of the battlefield.

Collaboration is a way for products to become more capable by working with another technology developer to share resources. Collaboration occurs in many ways and one example is a generator developer collaborated with a power management company to develop a more effective power generation and management system.

1. Flex Fuel Generator Collaboration

A collaboration table is created based on technology feedback from the end of day hot washes or individual white cell data collectors and consolidated in a single table, shown as Table 5.

Table 5. Flex Fuel Generator Collaborations Results from Adaptive Red Team Assessment

Collaborated with: Generic name (Tech name)	**Achieved/ Attempted**	**Comments**
Sensor Platform (Cerberus)	Achieved	Provided backup (only when battery/solar power was not available) to Cerberus trailer.
Battery Backup Kit (Expedition Pak/Patrol Pak)	Achieved	FFG powered the LIDAR-Based Facial Recognition system overnight. The Expedition Pak was used as the power management system to ensure power throughout the night.
Solar Panels (GREENS)	Achieved	Served as backup power for experiment.
LIDAR-Based Facial Recognition	Achieved	FFG provided prime power at night.
Communications Platform (Nett Warrior)	Achieved	FFG provided prime power.
Secure Communications System	Attempted	Discussed future collaboration.
Power Management Technology (Squad Power Manager)	Achieved	Provided input power to SPM-622 using solar

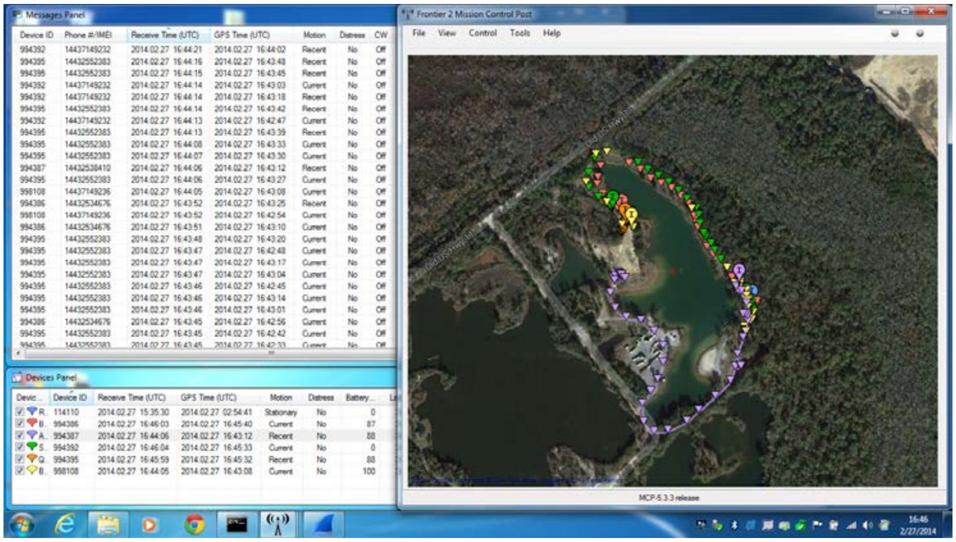
This table represents all of the attempted or achieved collaborations for the flex fuel generator. These generators provided primary power to a facial recognition system and communications platform. Backup power was provided to system sensor platform named Cerberus. This technology collaborated with power management technology that smartly manages its input power that is supplied to a load. Using the power management technology, solar panel technology, and a battery backup kit, the white cell was able to power the facial recognition technology day and night, rain, or shine.

Based on this three-way collaboration described above, it was determined by the white cell that an auto start capability should be incorporated in the FFG. This auto start feature will allow the automatic recharging of batteries based on specific conditions and eliminate an activity that needed to be monitored.

February 2015, INI Power Systems' technology's new auto-start FFG was selected as generator/auto start solution for Unites States Marine Corp (USMC) one-man portable battery charger requirement. This formal acquisition contract is for the purchase of 3,000 units (Markoski 2015, 1).

2. Frontier II LVFTT

When the Frontier technology was first selected to participate in an Adaptive Red Team event the product was deemed a very reliable TTL device as it used either satellite or cellular transmission of its information that is available coverage. The downside was that this device needed to communicate with the command post server. This "back" communication was the only way the TTL device was able to provide an output. This communications link was difficult to use as the blue cell commander was constantly turning around and taking his eyes off the COPs to look at the Frontier II command post software, shown in Figure 12 that displays the physical location of each device. This capability was hindered by the need to constantly look at a different stand-alone display rather than the integrated COP.



Messages Panel

Device ID	Phone #/IMEI	Receive Time (UTC)	GPS Time (UTC)	Motion	Distress	CW
994392	14437149232	2014.02.27 16:44:21	2014.02.27 16:44:02	Recent	No	Off
994395	14432552383	2014.02.27 16:44:16	2014.02.27 16:43:48	Recent	No	Off
994395	14432552383	2014.02.27 16:44:15	2014.02.27 16:43:45	Recent	No	Off
994392	14437149232	2014.02.27 16:44:14	2014.02.27 16:43:03	Current	No	Off
994392	14437149232	2014.02.27 16:44:14	2014.02.27 16:43:18	Recent	No	Off
994395	14432552383	2014.02.27 16:44:14	2014.02.27 16:43:42	Recent	No	Off
994392	14437149232	2014.02.27 16:44:13	2014.02.27 16:42:47	Current	No	Off
994395	14432552383	2014.02.27 16:44:13	2014.02.27 16:43:39	Recent	No	Off
994395	14432552383	2014.02.27 16:44:08	2014.02.27 16:43:33	Current	No	Off
994395	14432552383	2014.02.27 16:44:07	2014.02.27 16:43:30	Current	No	Off
994387	14432538410	2014.02.27 16:44:06	2014.02.27 16:43:12	Recent	No	Off
994395	14432552383	2014.02.27 16:44:06	2014.02.27 16:43:27	Current	No	Off
998108	14437149236	2014.02.27 16:44:05	2014.02.27 16:43:08	Current	No	Off
994386	14432534676	2014.02.27 16:43:52	2014.02.27 16:43:25	Recent	No	Off
998108	14437149236	2014.02.27 16:43:52	2014.02.27 16:42:54	Current	No	Off
994386	14432534676	2014.02.27 16:43:51	2014.02.27 16:43:10	Current	No	Off
994395	14432552383	2014.02.27 16:43:48	2014.02.27 16:43:20	Current	No	Off
994395	14432552383	2014.02.27 16:43:47	2014.02.27 16:42:48	Current	No	Off
994395	14432552383	2014.02.27 16:43:47	2014.02.27 16:43:17	Current	No	Off
994395	14432552383	2014.02.27 16:43:47	2014.02.27 16:43:04	Current	No	Off
994395	14432552383	2014.02.27 16:43:46	2014.02.27 16:42:45	Current	No	Off
994395	14432552383	2014.02.27 16:43:46	2014.02.27 16:43:14	Current	No	Off
994395	14432552383	2014.02.27 16:43:46	2014.02.27 16:43:01	Current	No	Off
994386	14432534676	2014.02.27 16:43:45	2014.02.27 16:42:56	Current	No	Off
994395	14432552383	2014.02.27 16:43:45	2014.02.27 16:42:42	Current	No	Off
994395	14432552383	2014.02.27 16:43:45	2014.02.27 16:42:33	Current	No	Off

Devices Panel

Devic...	Device ID	Receive Time (UTC)	GPS Time (UTC)	Motion	Distress	Battery...
☑ R..	114110	2014.02.27 15:35:30	2014.02.27 02:54:41	Stationary	No	0
☑ B..	994386	2014.02.27 16:46:03	2014.02.27 16:45:40	Current	No	87
☑ A..	994387	2014.02.27 16:44:06	2014.02.27 16:43:12	Recent	No	88
☑ S..	994392	2014.02.27 16:46:04	2014.02.27 16:45:33	Current	No	0
☑ Q..	994395	2014.02.27 16:45:59	2014.02.27 16:45:32	Recent	No	88
☑ B..	998108	2014.02.27 16:44:05	2014.02.27 16:43:08	Current	No	100

Figure 12. Frontier II LVFFT Control Station Software
(from Klopfenstein and Tober 2014, 107–122)

Finally, the technology developer was able to reformat the message using cursor on target. This new message format and command post server modifications allowed the message traffic to be shared on the Adaptive Red Team network.

The COP picture in Figure 13 is one of the first screen captures of a Frontier TTL device providing CoT formatted messages to the COP. The red circles are the Frontier devices. Notice no name next to the icon, as they have not fully implemented the UID field in CoT XML schema.

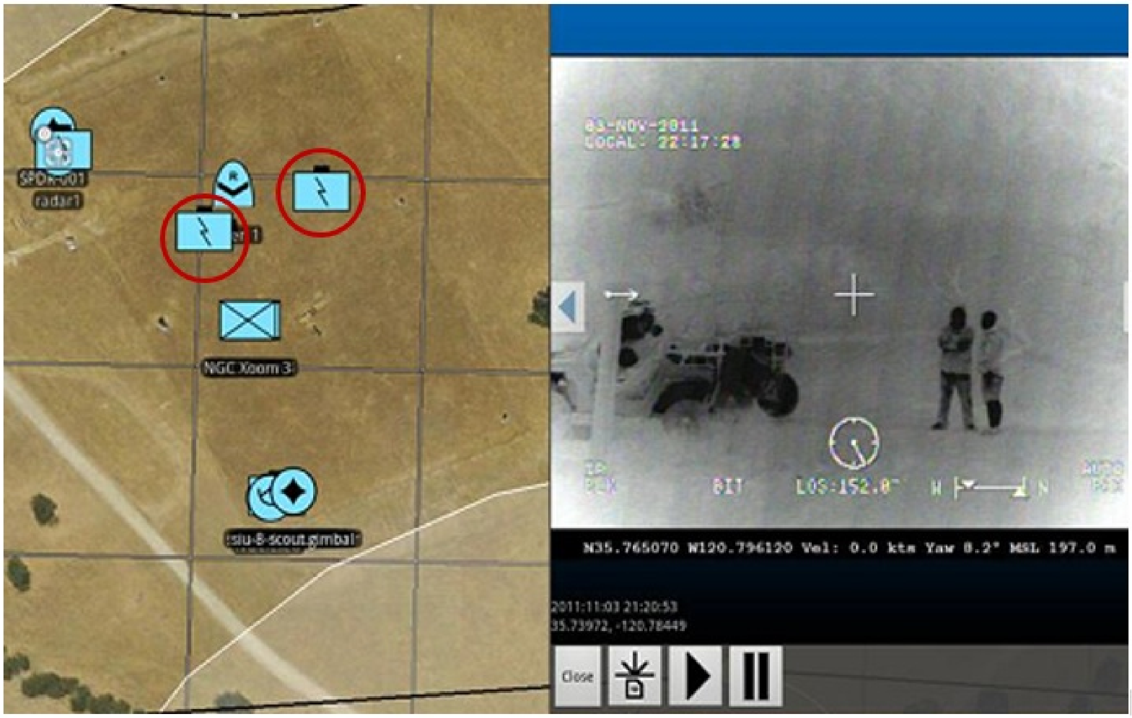


Figure 13. COP Software Displaying New Integrated Frontier TTL Devices Circled in Red (from Klopfenstein and Tober 2014, 107–122)

VIII. CONCLUSION

Traditional Red-teaming looks at a particular plan, document, or briefing “through the eyes” of the opposition or receiving agency depending on the circumstance. This perspective allows the organizations red-teaming output to be incorporated into the plan, document or briefing with the intent of being more thorough and impactful. This opposition’s perspective has not escaped DOD. In fact, DOD has been using red teams for several years to look at operations plans for use on the battlefield. This perspective is taught at DOD schools and educates attendees on red-teaming principles pertaining to operational plans.

The challenge for Adaptive Red Team is to formulate an adaptable, repeatable process that uncovers vulnerabilities and limitations in technology, not operational battle plans, through an adversarial perspective on developmental technology.

This development led Adaptive Red Team down a path that utilized previous experience and limited red-teaming knowledge to build a process for Adaptive Red Team to assess developmental technology. This old process was ineffective for Adaptive Red Team based on stakeholder feedback.

The new Adaptive Red Team process was created using systems thinking and based on initial results is more effective than the previous process used for red-teaming developmental technologies.

Discussion of Research Questions

1. What are the impacts of the Adaptive Red-teaming methods on developmental technology?

Developing technology for use by DOD is sometimes a difficult and challenging mission. All companies are in business to make money and the need to produce a useful product meeting a DOD need is the goal. Any advantage a company can use to make their technology more effective, more capable and less vulnerable to enemy TTP’s is generally in their best interest. This motivation drives the developers to continually improve the technology and mitigate the vulnerabilities discovered. Adaptive Red Team routinely receives submissions from previous developers in order to validate their mitigation attempts, showcase a new feature from collaboration or integration effort. Repeat submissions are one method to gauge the developer community on the impact Adaptive Red Team process.

Another method to measure the impact of Adaptive Red Team is whether DOD acquires an ART developmental technology through its formal acquisition. This acquisition process can be very rigorous and may present many challenges for solicitors such as key performance metrics pertaining to run-time, fuel type, output power, and usability with other fielded equipment. The INI generator participated in the new Adaptive Red Team process and was identified to have a system limitation. This limitation was the lack of an auto-start feature. This limitation was assessed after the generator collaborated with a battery kit developer. This limitation meant the generator had to be manually started when the batteries needed charged. The manual process meant a soldier had to be dedicated to watch the battery capacity and initiate the generator. The developer clearly felt the need to mitigate this system limitation and build an auto-start feature into the generator. This new capability is a major reason the USMC is acquiring 3,000 new flex fuel generators.

2. What value does the Adaptive Red Team process provide to developing defense technologies?

The new Adaptive Red Team process of uncovering vulnerabilities and system limitation is an assessment venue funded by the government that invites Industry and government developmental technology. The value provided by this Adaptive Red Team ranges from having a subjective team assess the technology, soldier training, and usage of the technology in scenarios. The EW & CNS white cell effort has been discussed by developers as the second most valuable part of the new Adaptive Red Team process. The most valuable part of Adaptive Red Team from the developer perspective, based on personal feedback, is additional information obtained during the operational assessments collected by white cell from usage in the scenarios. This assessment is based on the scenarios and the combined efforts of blue and red cells. Blue cell provides feedback to white cell on equipment training, portability, usage, and operational effectiveness, including effects from red cell. Red cell provides feedback to white cell on effectiveness of threat TTPs (if known) and adaptability. This value is enforced when each technology receives a copy of the report pertaining to their developmental technology. The feedback received from developers, combined with repeat submissions, provides evidence that the new ART process provides value to the development team.

3. How does implementing the Adaptive Red-teaming process help DOD acquire defense system more efficiently?

The new Adaptive Red Team process is executed at each quarterly event. These assessment events accept 25 technologies and assuming no repeats that is 100 different technologies each year that can be assessed by Adaptive Red Team. Those 100 technologies will most likely all have some vulnerability or limitation. If the development team chooses to mitigate those vulnerabilities or limitations, the technology would presumably be more effective or efficient at performing the desired capability. When industry mitigates those vulnerabilities, they utilize internal research and development (IRAD) funding. Those funds are not provided by the government. If the Army or other service acquires any of the 100 annually assessed technology after industry mitigates the vulnerabilities, this act would be more efficient than the traditional process of government contract. In essence, fund the research and possibly procure at the end of the contract.

DOD acquired the INI FFG generator by advertising on the government-contracting website its requirements for a one-person generator. That generator solicitation was awarded after all submissions were evaluated and the chosen technology by DOD was the INI FFG generator with the new auto-start feature. The acquisition of 3,000 FFG is further evidence of how this new process helps DOD acquire new defense systems more efficiently.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Central Intelligence Agency. 2015. “South Asia: Afghanistan.” *The World Factbook: Afghanistan*. Accessed August 1. https://www.cia.gov/library/publications/the-world-factbook/geos/af.html.

Defense Science Board. 2003. *The Role and Status of DOD Red-teaming Activities*. Washington, DC: Department of Defense.

Gilkes, George, and John Klopfenstein. 2014. *New ART Process*. Tampa, FL: Army Research Lab.

Goerger, Nik, and Michael Ferreira. 2012. *Deployable Force Protection Adaptive Red Team*. Point Magu, CA: Naval Air Station.

Klopfenstein, John, and Richard Tober. 2014. *ART/TSOA 14–2 Final Report*. Adelphi, MD: Army Research Lab.

Langford, Gary O. 2012. *Engineering Systems Integration*. Boca Raton, FL: CRC Press.

Kristan, Michael. 2009. *Cursor-on-Target Message Router User’s Guide*, edited by Jeffery Hamalainen, Douglas Robbins, and Patrick Newell. Bedford, MA: MITRE.

Markoski, Larry. 2015. “INI Power Tactical Hybrid Solutions.” *INI Power*. Last modified February. http://www.inipowersystems.com/#!news/cva4.

Seavey, Mark. 2013. “The Battle for COP Keating.” Military.com. American Legion. Last modified May 1. Accessed 05/10, 2015, http://www.military.com/daily-news/2013/05/01/battle-for-cop-keating-afghanistan.html.

University of Foreign Military and Cultural Studies. 2012. *Red Team Handbook*. 6th ed. Fort Leavenworth, KS: University of Foreign Military and Cultural Studies.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California