AU/ACSC/9797/AY09

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

LEARNING TO GET AHEAD: WHY ORGANIZATIONAL LEARNING IS CRITICAL IN COMBATING THE IMPROVISED EXPLOSIVE DEVICE THREAT

by

Lynn McDonald, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Donald A. MacCuish

Maxwell Air Force Base, Alabama

April 2009

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE **APR 2009**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **Learning to Get Ahead: Why Organizational Learning is Critical in Combating the Improvised Explosive Device Threat**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Command And Staff College Air University Maxwell Air Force Base, Alabama**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

The original document contains color images.

14. ABSTRACT

The Improvised Explosive Device (IED) threat has been termed the grand challenge by leading counter-terrorism organizations. What started as a nuisance has turned into a strategic threat. The US government is spending billions of dollars and thousands of man-hours to develop countermeasures and defeat technologies. Some countermeasures and technical solutions are quick; many are too slow to keep up with warfighter needs. The enemy, on the other hand, adapts quickly and develops weapons that are cheap and easy to build. The fundamental question driving this research is: how can an organization learn more effectively in order to become more flexible, adaptable, and innovative, while learning to make decisions faster and more proactively? This research will address the significance of learning at the operational and strategic levels, and the effect this learning has on the tactical level. Specifically, the research will draw on LTC John Nagls learning organization concept as expressed in his work Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam. Additionally, this paper will draw on a historical example of the British experience with the IED threat in the Northern Ireland conflict. Finally, this research project will discuss how innovative intelligence analysis can help further drive down the decision timelines. Learning and innovative organizations are key to countering current and future asymmetric weapons threats.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**36**	

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

List of Illustrations

Page

Preface

The sensitive nature of much of the information concerning Improvised Explosive Devices (IED), their employment, and countermeasures presented a challenge in writing this paper. Despite the lack of unclassified material, I felt strongly about continuing this research. My interest in this problem grew while working as the counter-IED lead on the Director, Space Forces Staff during my deployment to Al Udeid Air Base, Qatar. During this deployment, I was impressed by the resources being applied to and the complexity of countering this threat. I also grew to quickly appreciate the desire of the forces to have any solution against this threat. As my Army counterparts stated, "even the 30 percent solution is good enough" when it means the difference between life and death. Shortly after the deployment, I started to think how the concept of the "learning organization" in LTC John Nagl's *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam* could be applied to help institutionalize our lessons in combating this threat and help us move from a reactive to a proactive posture. This paper is dedicated to the US Army Functional Area (FA)-40 space professionals in Iraq who taught me how to better apply our space capabilities to the fight on the ground.

Abstract

The Improvised Explosive Device (IED) threat has been termed the "grand challenge" by leading counter-terrorism organizations. What started as a nuisance has turned into a strategic threat. The US government is spending billions of dollars and thousands of man-hours to develop countermeasures and defeat technologies. Some countermeasures and technical solutions are quick; many are too slow to keep up with warfighter needs. The enemy, on the other hand, adapts quickly and develops weapons that are cheap and easy to build. The fundamental question driving this research is: how can an organization learn more effectively in order to become more flexible, adaptable, and innovative, while learning to make decisions faster and more proactively? This research will address the significance of learning at the operational and strategic levels, and the effect this learning has on the tactical level. Specifically, the research will draw on LTC John Nagl's "learning organization" concept as expressed in his work *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam*. Additionally, this paper will draw on a historical example of the British experience with the IED threat in the Northern Ireland conflict. Finally, this research project will discuss how innovative intelligence analysis can help further drive down the decision timelines. Learning and innovative organizations are key to countering current and future asymmetric weapons threats.

Introduction

The Improvised Explosive Device (IED) threat has been termed the “grand challenge” by leading counter-terrorism organizations. What started as a nuisance has turned into a strategic threat, costing the US government millions of dollars in medical, logistical, and readiness costs.[1] The US government, likewise, is spending billions of dollars and thousands of man-hours to develop defeat technologies. Some countermeasures and technical solutions are quick; many are too slow to keep up with warfighter needs. The enemy, on the other hand, adapts easily and constructs weapons that are cheap and easy to build. While the US has made great progress in combating IEDs, the government agencies fighting this threat still struggle with lengthy decision timelines and are largely reactive in nature to the threat.

The enemy is adaptive, flexible, innovative and learns quickly. The adversary evolves technologies and techniques rapidly, and as technologies and techniques mature there is no hesitation to revert back to primitive means and solutions. The US, and other strong nations throughout history, respond with countermeasures that are developed over the course of months and, more often, over a period of years. When the countermeasure is employed, the enemy has long since moved on. These countermeasures have been executed and deployed with success against the threat, but it still begs the question: why is the enemy able to evolve so rapidly and the stronger opponent struggles to adapt quickly?

Countering the IED threat raises many questions. How can the US learn to adapt faster to get inside the enemy’s decision cycle? What lessons will be learned in order to combat future asymmetric weapons threats? Are there smarter ways to use technology against this threat? The fundamental question driving this research, though, is how can an organization learn more effectively in order to become flexible, adaptable, and innovative, while learning to make decisions faster and more proactively?

I addressed the question by using the problem and solution research methodology. The problem is the US government continues to react to the IED threat, while the enemy adapts quickly often rendering US countermeasures obsolete as they are fielded. In this research I will explore solutions to move from a reactive to a more proactive approach to the problem at the strategic and operational levels in order to allow more proactive and timely adjustments at the tactical level.

This research project is focused on how the US government, at the strategic and operational levels, must evolve more quickly with flexibility and ingenuity to drive proactively into the enemy's decision cycle in the IED fight. This paper will draw on a historical example of the British experience with this threat in the Northern Ireland conflict. I will also examine LTC John Nagl's "learning organization" concept as expressed in his work *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam*, and will address the significance of learning at the operational and strategic levels. Finally, I will discuss how we can further reduce the decision timeline through innovative intelligence analysis and move more toward predictive methods of analysis.

Improvised Explosive Devices: Background

If history repeats itself, and the unexpected always happens, how incapable must Man be of learning from experience.

-- George Bernard Shaw

Today's national security environment is one in which adversaries of the United States (US) seek to exploit US vulnerabilities via asymmetric means in order to erode US power, influence, and national will.[2] At various points in history, terrorists and insurgents have used Improvised Explosive Devices (IED) to advance their cause, attack a stronger adversary, and degrade the opponent's national will. IEDs are attractive weapons as they are relatively low cost, typically easy to build and deploy, and they allow the enemy to achieve both strategic and tactical results.[3] Additionally, improvised weapons can be used to compensate for a lack of conventional arms.[4] The enemy's use of IEDs to achieve strategic and tactical goals is referred to as an IED campaign, and these campaigns are characterized primarily by their asymmetric nature.[5] While it is imperative to understand the IED campaign within the greater context of the insurgency, this research paper is focused specifically on the IED campaign itself.

It is important to understand the background of the IED problem by first addressing the weapon, the casualties and the costs. I will then address the problem from a historical perspective by providing an example of how the British dealt with the IED threat during the Northern Ireland conflict. A brief discussion of the organization formed to deal with the current threat will be provided, and the background will conclude with a discussion on how the IED became the infamous weapon of the 21st century.

Improvised Explosive Devices: The Weapon, Casualities and Costs

In 2004, US and coalition forces in Iraq faced an alarming threat: the IED. While improvised explosives have been used in past insurgencies, this was an unusual (and unexpected) threat for today's military. Military forces faced this threat with few means to counter it and with limited experience in dealing with asymmetric threats on the battlefield.[6] IEDs are weapons that represent a wide range of explosive devices. These weapons range from simple explosives detonated by a "command wire" to the more complex and lethal Explosively Formed Penetrator (EFP) detonated by a motion sensor and remote device. The improvised nature of these weapons allows for quick and easy modification and presents a considerable challenge in developing countermeasures. Additionally, the IED "trigger puller" benefits from decreased risk and increased effect by detonating from remote locations.[7] The Pentagon has stated that "the IED remains the single most effective weapon against our deployed forces."[8] This weapon, hardly on the minds of pre-war planners, quickly developed into a costly and frustrating struggle, and the battle against this weapon has been a continuing fight to seize and maintain the initiative.[9]

The struggle against this asymmetric threat is even more frustrating in light of the resulting casualties. As of 2007, there have been more than 81,000 IED-related attacks in Iraq. IEDs have caused nearly two-thirds of the US combat deaths in Operation Iraqi Freedom and, as of late 2007, IEDs have killed or wounded 21, 200 US personnel.[10] In Iraq, IED events doubled in 2007, and, even though attacks decreased in 2008, this deadly problem persists. Likewise, attacks in Afghanistan continue to increase. The IED casualties are often magnified by insurgents making and distributing videos of the attacks in an attempt to undermine US and coalition efforts and to incite further violence.[11]

The Department of Defense (DoD) has invested significant resources to develop countermeasures against the IED threat. For example, the Joint IED Defeat Organization (JIEDDO) has spent more than $2.3 billion to develop, procure, field and sustain electronic jamming and other countermeasure technologies.[12] These costly technologies and techniques are often developed to prevent simple, cheap triggering devices such as two-way radios or garage door openers. The costs continue to grow in combating these quickly changing devices, and in fielding more heavily armored vehicles to withstand these lethal types of IEDs.[13] JIEDDO's most resource intensive mission area involves technological countermeasures for IEDs, which, in fiscal year 2008, accounted for approximately 53 percent of the organization's budget. These costs have also expanded into material solutions such as Intelligence, Surveillance, and Reconnaissance (ISR) sensors and non-material solutions such as personnel billets for weapons intelligence professionals.[14] The costs of developing countermeasures are staggering, but the costs in lives and mission readiness are equally troubling.

In 2004, to combat the rapidly growing IED threat, senior military commanders called for a focused effort to fight IEDs. This effort started as a small task force (comprised primarily of US Army personnel) and, in early 2006, this task force rapidly expanded into a $14 billion organization: the Joint IED Defeat Organization.[15] JIEDDO's mission is to lead and coordinate all DoD actions and initiatives to "defeat IEDs as weapons of strategic influence."[16] JIEDDO's efforts are organized into several mission areas: defeat the device, attack the network, and train the force. To fully understand the significance of this weapon and the current struggle with this threat, it is important to view it first from a historical perspective.

Learning From History: How the British Dealt With the IED Threat

The IED has posed many new challenges for today's military forces: the need for advanced explosive-resistant vehicle armor, convoy maneuverability, and more sophisticated intelligence surveillance and analysis techniques, to name a few. But the IED is hardly a new concept when it comes to asymmetric threats. The term itself was introduced during the Second World War to describe anti-Nazi resistance devices, and then took root in popular terminology in the late 1960s during the Northern Ireland conflict.[17] For over 30 years the British faced a relentless terrorist threat from the Irish Republican Army (IRA), which proved to be one of the most skillful and organized terrorist groups in recent times.[18] During several decades of conflict, British forces dealt with over 7,000 IEDs. While what the British faced in many years of conflict is less than three months of exposure to this threat in Operation Iraqi Freedom,[19] it is important to understand what was learned during the British experience in Northern Ireland.

The IRA was responsible for the largest and most diverse arsenal of bombs and explosive devices employed by an irregular force; they surpassed any other terrorist group in the types of explosives used.[20] From the command-wire detonated "culvert bomb" (especially dangerous to British army patrols) to radio-controlled detonations, the IRA quickly grew to become the experts in explosive devices.[21] The IRA's weapons ranged from very simple to some of the most sophisticated means of explosive devices and techniques.

Explosive technologies evolved quickly and so did the skills of those who built them. The IRA bomb builders and emplacers took risks and were not afraid to assess failures and learn from their mistakes. Their tactics, techniques, technologies and procedures evolved quickly and made it difficult for the British to counter the threat.[22] Innovation and adaptability surfaced as continuing themes in the IRA's ability to learn and adjust rapidly. To evolve and survive, a weaker force must understand its weaknesses and emphasize its strengths. The IRA's ability to capitalize on their improvisation and resourcefulness bled through the entire struggle and was born out of necessity and organizational survival.[23] The IRA continuously innovated in order to manipulate and reduce weapons engagement timelines and to overcome resource limitations. They also displayed vicious ingenuity in their targeting techniques and the rapid evolution of detonation devices.[24] At the close of the 1970s, the IRA had evolved from amateur bomb makers with sophomoric ability to advanced technology experts with unrivaled bomb-making skills.[25]

The IRA came to be known as some of the most proficient bomb builders. This reputation grew largely due to the evolution of their expertise in building timing devices, creating new methods of detonation, and developing a variety of explosive materials (often home-made).[26] The IRA continuously demonstrated they had the capacity and ability to adapt their devices and techniques. They became masters of creating an environment that forced their opponent to overcome the ever-changing threat, and this was usually at the opponent's great expense in terms of lives, mission disruption and resources.[27] The IRA adapted and quickly evolved based on necessity, survival, limited resources and the need to evade detection.

Tactics and technology also evolved in this asymmetric struggle. Remote control technology presented a significant advance in the IRA's technology and this placed increasing pressure on the British to develop countermeasures. A year later—when the British finally developed jamming countermeasures—the IRA reverted back to command-wire detonation, which was immune to electronic jamming.[28] Eventually, the IRA encoded the frequencies to counter the British countermeasures. What started with a simple remote detonation device (a transmitter from a remote control aircraft) evolved to more sophisticated electronic detonation methods.[29]

Despite the evolution to more complex detonators, the IRA's methods remained flexible and easily adaptable. The IRA was not wedded to their technological solutions; they did not allow their advances to plateau or hinder their flexibility to revert back to simple methods. A key strength of the IRA was the organization's ability to take a primitive and improvised weapon, develop it into an advanced weapons series, and then (just as quickly) revert back to a "tried and true" method such as the command-wire detonator.[30] They had an ability to evolve their technology and their tactics to meet the situation, environment and targeting requirements.

The IRA was also in a constant state of personnel change. This continuous rotation facilitated flexibility in the organization, unlike conventional forces in which positions and ranks can become comparatively stagnant for periods of time.[31] Additionally, this organizational flexibility influenced technology acquisition and development. Expertise constantly changed and the need to improvise and evade the British army and intelligence units required the members to learn quickly.[32] The IRA was learning in terms of bomb-making and deployment, and their ability to adapt and improvise with limited resources facilitated an environment of constant change and flexibility.

The IRA learned quickly from its mistakes. The IRA learned internally and they learned from external sources such as Libya and Syria.[33] Specifically, the IRA learned targeting and detonation techniques in the use of EFPs; these weapons surfaced during Operation Iraqi Freedom in some of the most deadly and destructive attacks against US and coalition forces.[34] British explosive ordinance disposal teams, over the course of the conflict, did mature into some of the world's best. This skill has continued into the current insurgencies in Iraq and Afghanistan, where IED attacks (and the changes in technologies and techniques) are relentless.[35]

The IRA learned and adjusted quickly and continuously. The IRA provided numerous examples of a disadvantaged adversary that capitalized on its strengths, and provides an important reminder to never underestimate the ingenuity and innovation of a weaker enemy. If an organization is stagnant or slow to respond, how can it expect to compete with the decision timelines of a more agile and flexible opponent? The ability to innovate and adapt fosters an environment in which an organization can more quickly evolve. It is essential to learn from history. Learning from experience and institutionalizing lessons is essential, and history provides this opportunity. However, there is little history on enemy use and friendly countering of IEDs and asymmetric weapons. In studying past insurgencies, it is important to understand the motivations and strategies of the insurgents; however, it is also important to understand the specific tactics and weapons used in order to combat current and future asymmetric weapons threats. The IED was a signature weapon in the Northern Ireland conflict; it has surfaced again as the weapon of choice in Iraq and Afghanistan.

The 21st Century Weapon of Choice

In 2005, eight British soldiers were killed in Iraq by IEDs that were detonated by infra-red beams—a technology first developed by the IRA.[36] Iraq presented a battleground that, in many ways, caught the military off guard. From the earliest part of the fight, the enemy in Iraq presented military forces with unconventional and asymmetric tactics and methods. A conventional war that quickly evolved into an insurgency presented military forces with a threat they were not yet familiar with. The IED has proven to be the number one threat to US and coalition forces in Iraq and Afghanistan.[37] There have been successes in combating the threat; however, the IED problem persists.

The DoD has dedicated significant effort and resources to develop and field jammers, vehicle armor, IED detection and pre-detonation devices, and other defensive measures to combat the IED.[38] The use of IEDs has demonstrated effects far beyond inflicting causalities. General Thomas Metz, Director of JIEDDO, stated that "IEDs are weapons of strategic influence because they attack the US national will and try to undermine and eliminate Western influence."[39] Additionally, IEDs have been employed to attack "iconic" armored military vehicles. The strategic effect is further magnified by the dissemination of video tapes of the attacks and other insurgent propaganda.[40]

The IED is a weapon of tremendous effect, casualty and cost to the targeted forces. The British dealt with the IED in Northern Ireland for decades. They learned to deal with this threat, but it was not rapid enough to proactively address the threat and gain an advantage on the enemy. This weapon (often made with homemade explosive materials or detonated by a doorbell activator) has caused strategic effects, costs billions of dollars, and is the most significant killer on the battleground. The ability to learn quickly is critical in addressing how to respond faster and more proactively to the enemy's constantly evolving tactics, techniques and technologies.

Organizational Learning

And that's when the ingenuity came out. And you found that a lot of people had a lot of ingenuity.

--Shane Paul O'Doherty, IRA bomb-maker

Insurgent IED Tactics: Adaptation and Evolution

What has been referred to as an "arms race" between the IRA and the British was an on-going struggle throughout the conflict. The IRA developed detonation devices, the British army countered them; the IRA developed a new device or tactic, and the army responded to defeat it. It was a vicious "race" and a vicious cycle. The IRA's strength was its ability to learn and quickly adapt its tactics in the bombing campaign. British intelligence noted that the IRA was "continually learning from their mistakes and developing their expertise."[41] This same technology race or "act/react" cycle that the British and IRA experienced is occurring today in Iraq and Afghanistan between military forces and insurgents. Insurgents today are combining techniques and technologies that were developed by the IRA over the course of many years, and these current techniques and technologies are evolving rapidly and creating endless threats to be countered.[42]

Recently, the Chairman of the Joint Chiefs of Staff noted that the IED gap is closing; however, he remarked that the speed of the US' evolving tactics still needs improvement.[43] Enemy tactics continue to evolve quickly and the expansion of IEDs from one warfighting theater to another continues to proliferate. There are several reasons for this expansion: explosive materials are widely and easily available; there are numerous (and simple) triggering methods; and the tactics and techniques change constantly and can be disseminated easily on the Internet and other electronic media. However, the primary reason for the rapid expansion and proliferation of the use of the IED is it has been highly effective against more powerful, technically superior military forces.[44] For an adversary seeking an asymmetric advantage, this weapon and its means of employment are invaluable for the achieved effect.

The ability of the adversary to learn and evolve has been an important characteristic of IED campaigns in past and present insurgencies. Insurgents have shown an ability to adapt that is short relative to the ability of US forces to develop and field IED countermeasures.[45] Additionally, countermeasures often have the unintended effect of shifting the threat from one device, technology or tactic to another.[46] One of the most important aspects of adapting and evolving is the ability to learn. Learning occurs at the individual and organizational levels. An organizational environment that supports risk-taking, open communication, honest assessment of success and failure, and learning from these experiences fosters an environment that responds more efficiently to external inputs.

Learning at the Strategic and Operational Levels

Learning from history, one can see that the IRA was flexible, adaptable, and innovative. Their technologies evolved and demonstrated remarkable ingenuity. The British had successes in combating this deadly threat, but they did not enjoy the same flexibility as their enemy. The British dealt with long timelines to develop countermeasures, they reacted to the threat, and they did not respond quickly enough. The British, however, successfully countered an insurgency in Malaya. Much of this success was attributable to an organizational culture that fostered flexibility, open communication, and learning.

In his book, *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam*, LTC John Nagl discusses the "learning organization." The concept is explained by comparing the British success in Malaya with the struggles the US Army faced in Vietnam. The British learned continually from their mistakes and trials; they were flexible and encouraged innovation from the bottom up. LTC Nagl remarks that the British army "demonstrated a remarkable openness to learning"[47] in the later years of the counterinsurgency. They also encouraged learning from the lowest ranks and welcomed innovation at the tactical and operational levels. There was openness in communication at the senior levels that allowed questioning, learning and discovery. Sir Gerald Templer, the British High Commissioner in Malaya, fostered innovation throughout the ranks. He encouraged risk taking and frank assessments of the results, which was particularly important in improving performance and learning. Despite the success, Templer still believed the learning process should have been faster.[48] LTC Nagl points out that the British army's learning experience was attributed to the organization's culture, its openness to innovation, and its ability to adapt the institution, doctrine, and training.[49]

The US Army went into Vietnam with a conventional mindset. The organization did not foster innovation and often stuck to the status quo even when it was no longer working or no longer applied to the situation.[50] When the US Army applied its mighty firepower against the Viet Cong, the enemy quickly adjusted its tactics and drew in close to the units. The Viet Cong, like the IRA, were flexible and they quickly learned from their mistakes and adjusted their operations.

At the tactical level, there was innovation and learning in the US Army; however, at the operational and organizational level learning was stifled. According to Nagl, doctrinal learning, institutionalization of tactical lessons, and effective communication of these lessons was highly ineffective throughout the organization. The US Army was not open to feedback and struggled to learn lessons during and after the conflict. When an organization learns, it evolves. When this learning is ingrained and institutionalized it eventually occurs more rapidly. This was not the case for the US Army in Vietnam. Today, there is still lacking consensus on the lessons drawn from Vietnam, and counterinsurgency doctrine changed very little (until recent years) in the years after Vietnam.[51]

Breaking Away From the Conventional Mindset

During the Malayan conflict, the culture of the British army fostered innovation and flexibility.[52] Templer helped the British army move from a kinetic strategy to a more non-kinetic approach focused on winning "hearts and minds." To do this he had to evolve his organization's mindset. Templer provides an example of leadership's influence on the organization's culture and disposition to learning. Prior to Templer, the British leadership in the Malayan counterinsurgency was resistant to change and more interested in a conventional approach, as successful lessons from the Second World War provided the framework for the entry into the Malayan conflict. Templer changed this mindset in his organization. He encouraged open communication, an entrepreneurial spirit among is men, and, as LTC Nagl explains, the "flexibility of thought and action."[53] Nagl emphasizes that the key to organizational learning is leadership that allows, fosters, monitors and ensures—through doctrine—that learning is ingrained throughout the organization.[54] Leadership at the operational level is vital in creating an organizational culture of innovation, openness and adaptability.

The US Army, on the other hand, stuck to a conventional mindset throughout its experience in Vietnam. Nagl explains the contrast in the American experience in Vietnam when he states that the US Army held to a "Jominian emphasis on defeating the enemy army in the field,"[55] which prevented an emphasis on the bottom-up innovation that led to British success in Malaya. Even as the search-and-destroy, kinetic missions failed the US Army, General Westmoreland, Commander of US forces in Vietnam, held tightly to this style of warfare. However, the problem was more deeply rooted than one leader. General Abrams, who replaced General Westmoreland, recognized the conventional approach was not working. He tried to change the search-and-destroy strategy of the US Army in Vietnam, but the culture was so deeply steeped in conventional operations that his ideas and strategies were disregarded. Nagl also notes that the US Army leaders of the Military Assistance Command-Vietnam and the Military Assistance Advisory Group often dismissed counterinsurgency doctrine during the war.[56] Leaders at the strategic and operational levels must set the conditions to allow and encourage their organizations to take risks and innovate.

When looking at the British in Malaya and the US Army in Vietnam, one can see the difference in the organizational cultures. Despite the initial resistance to counterinsurgency operations, the British army's culture had already been developed over many years of colonial wars.[57] This facilitated the necessary shift in strategy in Malaya. The US Army, even though historically involved in numerous political and limited campaigns, was culturally and organizationally focused on fighting conventional battles. British leadership encouraged communication, risk-taking, innovation, and honest assessments. The US Army leadership in Vietnam, on the other hand, clung to a conventional approach. When faced with challenges in Vietnam, the Army did not adapt.

Asymmetric weapons and methods, outwitting the opponent, and pitting strength against weakness are as old as warfare itself.[58] A military force that has a deeply ingrained conventional mindset has to have that mindset and culture challenged; the culture of the military institution has not been trained and is not designed to react at the speed of an asymmetric enemy.[59] The lessons for today are the need for an organizational culture that is flexible, comfortable with risk, innovative, adept at assessing performance and constantly learning.

Institutionalizing A Mindset to Deal with Future Asymmetric Threats

In 2008, a DoD Policy Analysis and Evaluation study group assessed the institutionalization of JIEDDO's capabilities to address future asymmetric weapons threats. This group examined the long-term organizational needs to address future asymmetric threats and reviewed measures of effectiveness and performance in JIEDDO's countering of the IED threat.[60] The study acknowledged that the use of IEDs will persist and is expected to grow based on the successful use of these weapons in Iraq and Afghanistan. The study group also noted that IEDs will remain a force-protection issue in the future.[61]

There have been signs of success in defeating IEDs—decreased attacks and disruption of enemy networks—but how can today's lessons be applied to fighting future asymmetric weapons threats? Additionally, when learning at the organizational level is examined, what has JIEDDO's role been in this success? Unfortunately, there is little *specific* information on the success against combating IEDs based on JIEDDO's efforts.[62] This challenge of measuring organizational effectiveness has been identified. JIEDDO has begun to track specific changes in enemy techniques and tactics, such as specific IED technology, types of detonating devices and locations of attacks. JIEDDO plans to compare this information with warfighter trend analysis to provide insight on the success and effectiveness of their initiatives.[63] The IED is just one example of an asymmetric threat that can be used in both irregular and conventional warfare. DoD organizations responsible for future warfare and stability and security operations planning are considering a broader range of future asymmetric threats against the US and its allies. There are also recent indications that JIEDDO is expanding its scope to address other asymmetric threats.[64]

Lessons learned from previous conflicts should be used as a basis for countering future asymmetric weapons threats, and analysis should anticipate other potential employment of asymmetric weapons. Specific focus should be placed on how the threat may migrate from one conflict to another and what form the threat it is likely to take. Additionally, it is essential to understand and examine how tactics are imitated, communicated within and between cultures, societies, local insurgents and international terrorists.[65] While counter-IED experts and task force personnel do share information, tactics, techniques, technologies, and procedures across the warfighting theaters, personal experience revealed that there was just as much information that was not being shared between these professionals. Countermeasures and lessons learned should flow more readily across warfighting theaters in order to combat migrating and future asymmetric threats.

Countermeasures and the IED "Threat Chain"

When addressing countermeasures, there are various aspects of the IED threat chain that must be addressed. The basic threat chain can be categorized into three components: organization, resources and operations. Typically, counter-IED efforts are focused on the operational element of the threat chain; however, an ideal approach to defeating the threat should include efforts to tighten the noose on the adversary at each stage of the threat chain.[66]

There are key points in the IED threat chain leading up to an IED attack in which improved disruption and intelligence analysis technologies should be applied. As discussed in the case of the Northern Ireland conflict and the British success in the Malayan Emergency, flexibility and innovation are key in an organization's ability to adapt, learn and evolve. This is vital in countering the threat at each stage in the threat chain. It is important to apply pressure at each point in the threat chain and disrupt activities in the financing and leadership of the organization, the development and trafficking of materials, and weapons building and emplacing.[67] Identifying critical and vulnerable elements in the IED threat chain is important particularly in developing countermeasures and understanding how enemy decisions are made. The elements of time and risk are critical in the IED threat chain and in developing defeat technologies. In the following graphic, I display the relationship between time and risk:

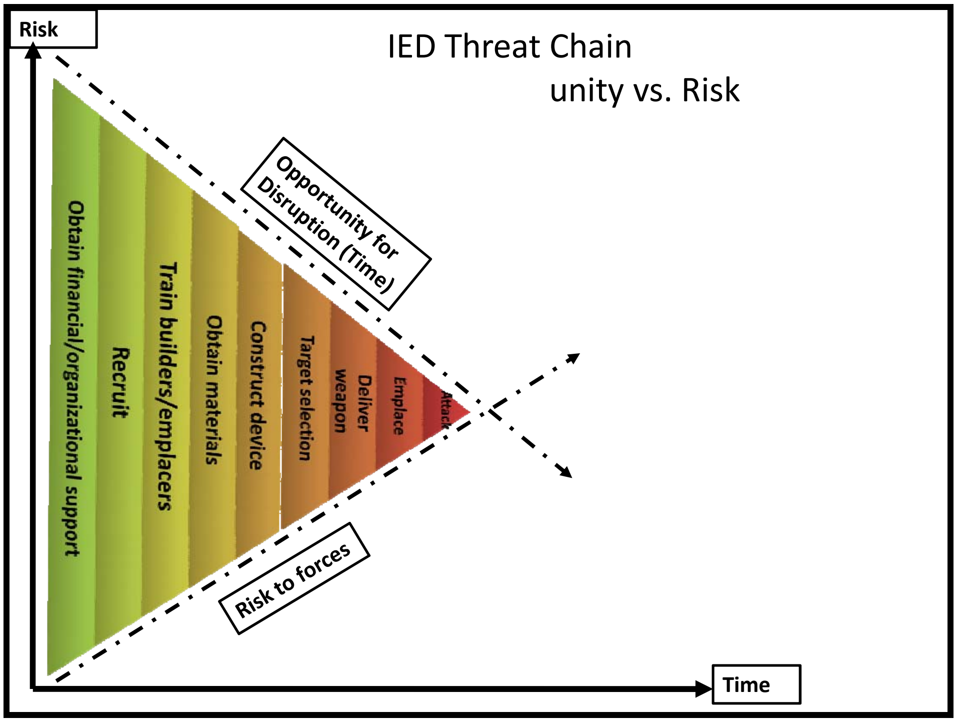

Figure 1. IED Threat Chain: Disruption Opportunity versus Risk

In the graphic, time is measured in terms of opportunity for disruption leading up to the IED attack. Opportunity for disrupting the threat diminishes and becomes crucial as time approaches the attack event. Risk, on the other hand, increases as the attack event draws near. The brief amount of time and increased risk to military forces in the events leading up to the attack are the most dangerous, hardest to disrupt, and the most crucial moments in the IED threat chain. While each element of the threat chain must be countered, the greatest challenge is in the hours, minutes and seconds leading up to the attack. Innovation and organizational learning must be so deeply ingrained in the organization that forces can outsmart the enemy throughout the threat chain—up to the event and in the post-event phase. The intelligence, information, and indicators during this crucial period are often clouded by the "friction" of war, not recognized unless fused with other intelligence, or not timely enough for the forces on the ground.

Innovative Intelligence Analysis

Smart Information, Not More Information

Intelligence proved to be crucial in the British conflict in Northern Ireland, and it was the area that provided one of the greatest challenges to the British forces. From the start of the insurgency, the IRA grabbed hold of the intelligence initiative and used it to their advantage. The IRA was superior in intelligence operations and the British were forced to overcome a significant hurdle in this mission area.[68] Intelligence is vital also in today's counterinsurgency efforts and in combating the IED threat. JIEDDO's Counter-IED Operations Integration Center (COIC) responds to hundreds of intelligence-related requests each month from deployed forces. These requests generally seek fused information from multi-intelligence resources, law enforcement, and operational and analytic centers to provide combat forces information for mission planning and maneuvering safely in the battle space. Deployed forces have been positive about this support because it can provide intelligence support that previously was not available at the tactical level.[69] Fused data is increasingly requested by combat forces. JIEDDO supports analytical tools that fuse and display intelligence and information from multiple sources, to include national intelligence data, tactical data from deployed units, geographical and cultural information, and imagery. JIEDDO views these tools and capabilities as “truly revolutionary.”[70]

Each “link” in the IED threat chain provides observables, signatures, and opportunities for interception and exploitation.[71] There is a need to detect the activities that precede an IED attack at each step in the threat chain in order to increase prediction at multiple points prior to an attack. This requires a breadth of information from human and technical sources and the ability to infer knowledge from large amounts of diverse, potentially incomplete, and near-real time data.[72] The timely and accurate use of data dictates the ability to automate data integration and analysis. As timing is critical (especially leading up to an IED attack), the ability to produce reliable, actionable intelligence from “noisy,” time-sensitive, incomplete, and multi-source data becomes increasingly important. Even more vital are the needs for data acquisition, analysis, and inference as part of an integrated effort.[73]

Exploiting Intelligence Analysis

JIEDDO is also focused on intelligence support; this falls primarily under the “Attack the Network” line of operation. This line of operation is focused on the financial support network, the bomb builders, adversary training, and associated weapons infrastructure.[74] As this research is focused primarily on the time-sensitive intelligence necessary for deployed military forces, route clearance teams, and time-sensitive training, this is the mission area of interest for the exploitation of intelligence analysis.

A study in 2004 by the United States Military Academy (USMA) found a lack of focused and centralized theater collection and analysis of IED information.[75] While some of this has been resolved by JIEDDO's COIC, national intelligence agencies and military intelligence units, there is still room for growth. This study found a full assessment of IED information is important in examining ways to "exploit existing information sources, providing near real-time information on IED activity for implementation of preventative and responsive measures, and prediction of IED changes or improvements" to enemy tactics.[76] The study revealed the need to mine the IED data to develop a better and more thorough understanding of enemy tactics evolution and to better predict future adversary uses of asymmetric weapons.[77] It was also found that there is a continuing need for data collection and automated intelligence systems that can mine large volumes of data and find relationships in this data.[78]

The USMA study found large volumes of IED incident information reported by military forces in Iraq, but found the information inconsistent to an extent that made predictive analyses of IED tactics and technology evolution very difficult. Further, the study identified a need for improved analysis capability through the leveraging of information technology capabilities and refined skill sets for assessment and analysis of IED-related intelligence information.[79] Finally, the study found that in the IED threat chain the initial stages of IED emplacement provide opportunities for interdiction through a more thorough intelligence and information analysis process.[80]

Continued advancements in information and intelligence fusing and correlation technologies can provide the opportunity for combat forces to make decisions faster and with more accurate information. The fusion of information and integration of sensors, platforms and operational organizations can provide potential for IED detection in a more rapid and effective manner. This is critical for military forces to increase battle space awareness and gain a clearer and more comprehensive picture of friendly and adversary activities. Despite technological advances, filtering, correlating, fusing, and analyzing information to derive actionable intelligence remains a difficult task.[81] There is no single solution and many of the IED countermeasures will never fully erase the "fog and friction" on the battlefield. However, the ability to integrate, synchronize and synthesize will improve operational awareness, decrease decision-making time, and enhance detection, destruction and reduction of these asymmetric weapons.[82]

Recommendation

Ministry of Defence (MoD) Counter Terrorism Centre[83]

Following my deployment to USCENTCOM as the lead space professional for counter-IED, I was invited to a meeting at Cambridge University with the National Transport Innovation Incubator (NATII) Consortium[84] to discuss potential counter-IED intelligence and analytic processing solutions for the UK MoD Counter Terrorism Centre. The problem was discussed in terms of timeliness and relevance of IED threat data, management of the data, and data flow of threat information to the warfighter. This section will provide a background on the issue and will address the idea proposed to the MoD Counter Terrorism Centre.

In an unconventional and asymmetric environment, operations and intelligence centers must evolve techniques and procedures much more rapidly than in past "static" wars. Current operations have changed to reflect the demands of today's asymmetric style of warfare. Previously, structured intelligence data and information was effective when the target set was limited. Today's intelligence challenges—against a far more complicated target—are "compounded by a growing data glut, increasing noise in the environment and decreasing time available to perform analysis."[85] Instant message chat rooms have become common in today's operations and intelligence centers and have been used effectively by US and coalition forces to share tactical intelligence and threat indications. However, the amount of data can quickly become overwhelming and real-time analysis is difficult due to the unstructured nature of the data, lack of training, and other operational demands that detract from the timely value of the data.

During the NATII Consortium's meeting to discuss counter-IED intelligence solutions, much of the discussion focused on intelligence collected on the enemy and enemy systems. Based on my experience from the deployment and previous intelligence center operations, I proposed addressing IED threat information passed in "friendly" (US and coalition) classified chat rooms. During my deployment, I was impressed by the extent of communication conducted in chat rooms and the challenge of managing vast amounts of information and intelligence in these chat rooms.

Chat rooms provide information gathered from tactical operations centers, intelligence organizations, route coordination and clearance personnel, and airborne platforms, to name a few. These chat rooms—with varied sources of IED threat information—provide an opportunity to discover previously unknown activity trends or key words that may provide warning of an impending IED attack. Operations center personnel and intelligence analysts often have up to a dozen or more chat rooms open simultaneously. Operations and intelligence personnel interact with and monitor real-time chat with dozens to hundreds of other operators, analysts, and warfighters. Whether one likes it or not, these chat rooms have become a fundamental communications tool in the warfighting environment. Information in these chat rooms is often not vetted, but the real-time value of threat information from a broad base of sources is important.

Technologies to archive and characterize the data flowing though these chat rooms have not kept up with the proliferation of these communication tools. The growth in data volumes makes it difficult to track trends, produce statistics that add value, and track the data flow itself. Analysis of the unstructured data flow through these chat rooms could reveal new information on the adversary's training, tactics, technologies and procedures. Integration of data trend applications may reveal previously unknown activity trends or key words related to impending IED activity and attacks.[86] This analysis is essential at each event in the IED threat chain. As time decreases and risk increases (Figure 1) approaching the IED attack, the near-real time value of threat information becomes increasingly critical. Chat room threat analysis is conducted manually and this poses several problems.

Analysts (often not formally trained) do not have the skills or time to manually identify trends or produce trend statistics across all areas of interest. They may only accomplish manual analysis for the highest priority (or most obvious) targets. Manual analysis has not been effective because it requires a significant amount of training (often for personnel with little analytic experience), and the pace of current operations makes such training impractical in the warfighting theatre. Most importantly, manual analysis sacrifices the real-time value of the data while increasing the risks (error rate) associated with a man-in-the-loop solution. Technology that can automate this analytic process and identify trends in the threat data should be integrated into intelligence and operations centers to improve the speed and detection of key words relevant to the threat environment.

The idea was further developed by members of the NATII Consortium and the Cambridge Mathematical department proposed the technical solution to the MoD Counter Terrorism Centre. The Counter Terrorism Centre has embraced the idea and is pursuing further exploration of the proposal. This was not a radical idea, but one based on experience and lessons learned working the counter-IED threat mission. There are many more practical ideas and solutions from personnel who have worked to counter this threat. Many ideas are incorporated immediately in the warfighting theater; other ideas evolve into solutions when these personnel return to their home stations. However, just as many ideas and solutions are never realized due to insufficient means to capture these observations or lacking opportunities to share ideas and operational experiences with those who can provide a solution.

Conclusion

The IED is a weapon of strategic effect. It has become the weapon of choice in Operations Iraqi and Enduring Freedom. With the success asymmetric enemies have had against US and coalition forces, it is expected that this threat will persist in the future. The threat may change and evolve, but weaker adversaries will continue to exploit the stronger opponent's vulnerabilities. These adversaries, based on survival, are often highly adaptive, innovative and flexible. To counter this—as demonstrated in historical examples—an organization must foster innovation, flexibility, and risk-taking to breed a culture of warfighters, at every level, who learn to adapt and make decisions quickly. The significance of learning at the operational and strategic levels in the fight against IEDs is crucial. Tactical flexibility is impaired when the organizational culture does not promote risk taking, ingenuity, and the ability to learn from success and failure.

History has also shown the significance of intelligence in the fight against IEDs. The British struggled with it in Northern Ireland and fought to regain the initiative that the IRA seized. Intelligence is just as critical in today's fight against the IED and innovative intelligence analysis can help further drive down the decision timelines. Advancements in data manipulation and trend analysis may improve the predictive value of intelligence. This will facilitate faster decisions with more relevant threat information. As a result of observations from my deployment, work with the NATII Consortium and this research, I recommend the proposal to the UK Counter Terrorism Centre be adopted by JIEDDO and US intelligence and operations centers. This proposal is an evolution of an idea based on lessons and observations from my deployed experience.

In addition to this proposal, I recommend that JIEDDO develop a more robust means for gathering lessons learned and post-deployment debriefings from personnel working the IED threat. This is critical for both current and future development of counter-IED tactics, techniques, technologies and procedures. This should include a more extensive outreach program to draw on the experiences and lessons from deployed personnel working the counter-IED mission area. Capturing (and institutionalizing) observations and lessons breeds a culture that can better learn from success and failure and learn more efficiently. It may also prevent re-learning the same lessons in subsequent conflicts.

Organizational learning, innovation, and technology are essential in IED defeat operations. As described in Field Manual 3-90.119, *Combined Arms Improvised Explosive Device Defeat Operations,* the goal of operational planning is to “achieve a faster decision cycle than the threat.” Additionally, it states that if the enemy responds or adapts to friendly technologies and procedures, friendly forces must also rapidly change tactics, techniques, technologies and procedures.[87] This ability to adapt and remain ahead of the enemy’s decision cycle must be cultivated and fostered at every level in the organization. From new defeat technologies to the way data is analyzed and managed, innovation in every aspect of the fight against IEDs is critical in gaining and maintaining the initiative against the enemy. Learning and innovative organizations are essential to countering current and future asymmetric weapons threats. Aggressive ingenuity and a culture that promotes a flexible mindset must permeate every level in the organization or it will remain a step behind a highly adaptive enemy.

Notes

[1] Atkinson, "Left of Boom," p.x.
[2] Applied Warfare Studies, Air Command and Staff College.
[3] National Research Council, "Countering the Threat of IEDs," p.1.
[4] Oppenheimer, "IRA: Bombs and the Bullets," p.5.1
[5] National Research Council, "Countering the Threat of IEDs," p.x.
[6] Subcommittee on Oversight, "JIEDDO," p.11.
[7] Ibid..
[8] Atkinson, "Left of Boom," p.5.
[9] Ibid.
[10] Ibid.
[11] Wilson, "Improvised Explosive Devices in Iraq," p.1.
[12] Subcommittee on Oversight, "JIEDDO," p.13.
[13] Ibid., p.14.
[14] Ibid., p.16.
[15] Ibid., p.11.
[16] National Research Council, "Countering the Threat of IEDs," p.x.
[17] Oppenheimer, "IRA: Bombs and the Bullets," p.8.
[18] Art and Richardson, "Democracy and Counterterrorism," p.63.
[19] Atkinson, "Left of Boom," p.4.
[20] Oppenheimer, "IRA: Bombs and the Bullets," p.7.
[21] Ibid., p.177.
[22] Ibid., p.43.
[23] Ibid., p.43.
[24] Ibid., p.213.
[25] Ibid.
[26] Ibid., p.199.
[27] Ibid., p.xviii.
[28] Ibid.
[29] Ibid., p.211.
[30] Ibid., p.231.
[31] Ibid., p.42.
[32] Ibid.
[33] Ibid., p.255.
[34] Ibid., p.211.
[35] Ibid., p.291.
[36] Ibid., p.294.
[37] Subcommittee on Oversight , JIEDDO, p.13.
[38] Ibid., p.12.
[39] Ibid., p.13.
[40] Atkinson, "Left of Boom," p.5.
[41] Art and Richardson, "Democracy and Counterterrorism," p.71.
[42] Oppenheimer, "IRA: Bombs and the Bullets," p.283.
[43] Air Command and Staff College Lecture.
[44] Subcommittee on Oversight , JIEDDO, p.13.
[45] National Research Council, "Countering the Threat of IEDs," p.ix.
[46] Ibid., p.2.
[47] Nagl, "Learning to Eat Soup," p.105.
[48] Ibid., p.107.
[49] Ibid., p.107.
[50] Ibid., p.ix.
[51] Ibid., p.205.
[52] Nagl, "Learning to Eat Soup," p.xii.

[53] Ibid., p.192.
[54] Ibid., p.195.
[55] Ibid., p.198.
[56] Ibid., p.201.
[57] Ibid., p.216.
[58] Atkinson, “Left of Boom,” p. 3-11
[59] Ibid., p. 3-11
[60] Ibid., p.43.
[61] Ibid., p.43.
[62] Subcommittee on Oversight , JIEDDO, p.39.
[63] Ibid., p.40.
[64] Ibid., p.44.
[65] National Research Council, “Countering the Threat of IEDs, p.5.
[66] Ibid., p.3.
[67] Ibid., p.3.
[68] Fierro, “British Counterinsurgency Operations,” p.17.
[69] Subcommittee on Oversight , JIEDDO, p.22.
[70] Ibid.
[71] National Research Council, “Countering the Threat of IEDs”, p.2.
[72] Ibid., p.3.
[73] Ibid., p.6.
[74] Subcommittee on Oversight, “JIEDDO,” p.20.
[75] USMA, “Analysis of IED Employment,” p.4.
[76] Ibid., p.5.
[77] Ibid., p.6.
[78] Ibid., Enc 1-1.
[79] Ibid., p. Enc 1-2.
[80] Ibid., p. Enc 1-3.
[81] Ibid., p. Enc 12-1.
[82]Ibid., p. Enc 12-3.

[83] Discussion on proposal to the Ministry of Defence Counter Terrorism Centre. Please note British spelling in reference to the organization.
[84] The NATII Consortium consists of members from Cambridge University Mathematical Sciences, Syzygy Ltd, Thales and Lockheed Martin. I worked with individuals from the Consortium throughout this research project and was given permission to use material from our meetings.
[85] John Hollywood et al., *Out of the Ordinary*, p.3.
[86] NATII Consortium, “Proposal to UK Counter Terrorism Center,” p. 3.
[87] Department of the Army, *Combined Arms IED Defeat*, p. 4-1.

Bibliography

Art, Robert J. and Louise Richardson. *Democracy and Counterterrorism: Lessons From the Past*. United States Institute of Peace Press, Washington DC, 2007.

Atkinson, Rick. "Left of Boom." Washington Post series, 2007.

Department of the Army. *Field Manual 3-90.119, Combined Arms Improvised Explosive Device Defeat Operations*. September 2007.

Fierro, Michael R. "British Counterinsurgency Operations in Ireland 1916-1921: A Case Study." Naval War College, Newport RI, 1997.

Hollywood, John, Diane Snyder, Kenneth McKay, and John Boon. *Out of the Ordinary: Finding Hidden Threats by Analyzing Unusual Behavior*. RAND Corporation, Santa Monica, CA, 2004.

Military Academy West Point, *An Analysis of Improvised Explosive Devise (IED) Employment*. USMA, West Point, NY, November 2004.

Nagl, LTC John A. *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam*. The University of Chicago Press, Chicago, IL, 2002.

National Research Council. *Countering the Threat of Improvised Explosive Devices: Basic Research Opportunities*, The National Academies Press, Washington DC, 2007.

Oppenheimer, A.R. *IRA: The Bombs and the Bullets*. Irish Academic Press, Dublin, IR, 2009.

NATII Consortium. "Proposal to United Kingdom Counter Terrorism Center." 28 Sep 2008.

Subcommittee on Oversight and Investigations. *The Joint Improvised Explosive Device Defeat Organization: DoD's Fight Against IEDs Today and Tomorrow*, November 2008.

Wilson, Clay. "Improvised Explosive Devices in Iraq: Effects and Countermeasures." Congressional Research Service, Library of Congress, 2005.