National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

"THE SILVER BULLET": THE COMPREHENSIVE APPROACH TO COUNTER IMPROVISED EXPLOSIVE DEVICES

By Lieutenant-Colonel Y. Michaud

JCSP 39

Master of Defence Studies

PCEMI 39

Maîtrise en études de la défense

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 39 – PCEMI 39
2012 – 2013

MASTER OF DEFENCE STUDIES – MAITRISE EN ÉTUDES DE LA DÉFENSE

"THE SILVER BULLET": THE COMPREHENSIVE APPROACH TO COUNTER IMPROVISED EXPLOSIVE DEVICES

By Lieutenant-Colonel Y. Michaud
Par le lieutenant-colonel Y. Michaud

Word Count: 18 322

Compte de mots : 18 322

TABLE OF CONTENTS

Table of Contents		ii
List of Figures		iii
Abstract		iv
Introduction		1
Chapter:		
1.	The IED System	8
2.	The C-IED Strategy	35
3.	Owning the Comprehensive Approach	68
Conclusion		96
Bibliography		99

LIST OF FIGURES

Figure 1: IED by Target (August 2010 to August 2012) 13

Figure 2: IED Casualty Figures in Afghanistan (Jan 2004-May 2010) 18

Figure 3: IED Attacks Worldwide by Combatant Commander 28

Figure 4: Typical Threat Network Model 29

Figure 5: IED Threat Network System 33

Figure 6: C-IED Approach with Supporting Activity Pillars 36

Figure 7: IED Incidents in Afghanistan (Jan 2004-May 2010) 51

Figure 8: IED Critical Capabilities and Critical Requirements 57

Figure 9: Find-Fix-Finish-Exploit-Analyze-Disseminate Cycle 62

Figure 10: The Comprehensive Approach 70

LIST OF TABLES

Table 1 – Terrorist Attacks by Weapon Type 46

ABSTRACT

Throughout the spectrum of Stabilization Operations, threat networks use Improvised Explosive Devices (IEDs) against more-powerful coalition forces, both as a strategic and tactical weapon. More than 100,000 attacks, in over 70 countries, have been recorded in the last ten years; IEDs are now a global problem affecting all instruments of national power: diplomatic, information, military, and economic. This paper argues that the most effective long-term counter IED (C-IED) strategy is to attack threat networks using the Comprehensive Approach. This strategy requires collaboration and cooperation from a wide range of non-military partnerships, such as interagency and multinational. Rather than focusing primarily on expensive tactical countermeasures and force protection, the comprehensive C-IED strategy disrupts the IED system well before IEDs are emplaced. Ultimately, the Comprehensive Approach has the greatest impact in reducing the number of casualties, both military and civilian, and therefore protects the friendly government's centre of gravity: national will.

It takes a network to fight a network.

- General Stanley McChrystal, *Foreign Policy*

INTRODUCTION

Improvised Explosive Devices (IEDs) are not an invention of the 21st century. They were used as far back as the year 1605 when Guy Fawkes and his group of conspirators attempted to destroy the Houses of Parliament and assassinate King James I in order to overthrow the British government.[1] IEDs were also used at the battles of Mobile Bay and Petersburg during the US Civil War, exploiting their strategic effects of surprise.[2] During the Arab Revolt of 1916-1918, T.E. Lawrence and Faisal bin Hussein fought "a war of detachment", using IEDs to maximize Arab strengths against Turkish weaknesses.[3]

Similar tactics were used by the Soviets in the Belorussian Rail War of 1944-45, bringing German rail system to "near-complete standstill."[4] The Vietcong used IEDs during the Vietnam War, causing approximately one-third of all US casualties.[5] In Northern Ireland, the Irish Republican Army (IRA) used IEDs extensively against the British security forces, demonstrating how asymmetric warfare using IEDs can negate

---

[1]Department of Defense, *Counter Improvised Explosive Device Strategic Plan 2012-2016* (Norfolk: Joint Improvised Explosive Device Defeat Organization, 2012), https://www.jieddo.mil/content/docs/ 20120116_JIEDDOCIEDStrategicPlan_MEDprint.pdf, 2.

[2]Peter Singer, "The Evolution of Improvised Explosive Devices," *Armed Forces Journal*, February 2012, http://www.brookings.edu/research/articles/2012/02/improvised-explosive-devices-singer.

[3]David Murphy, *Lawrence of Arabia: Leadership, Strategy and Conflict* (Oxford: Osprey Publishing, 2011), 52.

[4]Chris Bellamy, *Absolute War: Soviet Russia in the Second World War* (New York: First Vintage Books Edition, 2008), 613.

[5]Department of Defense, *Counter Improvised Explosive Device Strategic Plan* …, 2.

conventional forces' strengths, particularly in an urban environment.[6] In the 1980s and 1990s, IEDs have been used sporadically, but have maintained their strategic effects. The deadliest IED attack on the US forces overseas occurred in 1983, when Hezbollah killed 241 US Marines in Lebanon, which "ushered in the modern day suicide attacks."[7] In 1993, Al-Qaida bombed the World Trade Center in New York City, demonstrating their ability to attack the US homeland.[8]

Interestingly, the term "IED" only became common in the US in 2003 in the wake of Operation Iraqi Freedom, where IEDs were responsible for more American casualties that any other weapon system.[9] Although present since the 17th century, IEDs were used either for spectacular terrorist attacks or by guerrilla forces to attrite a stronger force, but not as a primary weapon. For example, during the Arab Revolt of 1916-1918, where IEDs were used extensively by the Arabs with great success against the Turkish Army, their purpose was to attack the railway to cut lines of supply. Lawrence and the Arab Army caused the vast majority of Turkish casualties by using ambushes and fire support.[10]

After the US invasion in 2003, IEDs became the weapon of choice of the insurgents in Iraq: they were cheap, easily built using household products, highly lethal,

---

[6]Glenn Zorpette, "Countering IEDs," *IEEE Spectrum* 45, no. 9 (September 2008): 26. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04607910.

[7]House of Representatives Committee on International Relations, *Hezbollah's Global Reach* (Washington, DC: U.S. Government Printing Office, 2006), www.democrats.foreignaffairs.house.gov/archives/109/30143.pdf, 1-5.

[8]Headquarters of Department of the Army, FMI 3-34.119/MCIP 3-17.01, *Improvised Explosive Device Defeat* (Washington: US Department of the Army, 2008), v.

[9]Department of Homeland Security, *IED Attack: Improvised Explosive Devices* (Washington, DC: The National Academies Press, 2007), http://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf, 1.

[10]David Murphy, *The Arab Revolt 1916-1918: Lawrence Sets Arabia Ablaze* (Oxford: Osprey Publishing, 2008), 22-23.

and provided effective stand-off capability.[11] Iraqi insurgents also exploited the effects of globalization and the value of the Internet to exchange the "know-how" between insurgent groups, particularly the use of fertilizer to fabricate homemade explosives (HME).[12] As a result, insurgents migrated from using military explosive and unexploded bombs to primarily HME-based bombs, increasing the number of manufactured IEDs by 500% from 2003 to 2007.[13] This level of success in Iraq enticed the insurgents in Afghanistan to triple the number of IED attacks in the last five years, causing the percentage of IED-related coalition casualties to double in Afghanistan.[14] In addition, these devices have been responsible for more civilian casualties than any other type of attack.[15] The rising casualty rates, both military and civilian, caused Western domestic support for the wars in Iraq and Afghanistan to drop significantly.[16]

However, the IED threat was not exclusive to Afghanistan and Iraq. Over the past ten years, IEDs have become a global, and prominent, problem since they are the weapon of choice for threat networks[17], such as terrorists, insurgents, criminal groups, and the disenfranchised. IEDs are now present in most conflict environments, whether

---

[11]Department of the Army, *Improvised Explosive Device Defeat…*, v.

[12]Department of Defense, *Counter Improvised Explosive Device Strategic Plan …*, iii.

[13]Anthony H. Cordesman, Charles Loi, and Vivek Kocharlakota, "IED Metrics for Iraq: June 2003 – September 2010." *Centre for Strategic Studies*, November 11, 2010, last accessed 23 December 2012, http://csis.org/files/publication/101110_ied_metrics_combined.pdf.

[14]Icasualties.org, "Operation Enduring Freedom", last accessed 18 January 2013, http://icasualties.org/OEF/index.aspx.

[15]UN Secretary-General, *The Situation in Afghanistan and its Implications for International Peace and Security* (New York: United Nations, 2005), http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Afgh%20S%202011%20381.pdf, 5.

[16]Cable News Network, "CNN/ORC Poll – March 24-25 – Afghanistan," *CNN*, March 30, 2012, last accessed 7 January 2013, http://i2.cdn.turner.com/cnn/2012/images/03/29/rel3f.pdf.

[17]For the purpose of this paper, threat networks include any group that uses IEDs as a primary weapon against friendly forces. They include terrorists, insurgents, guerrillas, organized crime syndicates, other criminals, and the disenfranchised. Conventional military forces are also considered threat networks fifth columnists or Special Purpose Forces operating covertly using asymmetric attacks.

asymmetric, conventional, or hybrid.[18] Furthermore, they are no longer just a tactical weapon used to hamper mobility and cause casualties; it is now understood that IEDs have an asymmetric strategic effect and will continue to affect conflicts in the future.[19]

Due the effectiveness of IEDs and their global presence, many western nations, such as the United States, the United Kingdom, and Canada, have spent billions of dollars to counter them. They formed organizations dedicated to fight IEDs, such as the US Joint Improvised Explosive Device Defeat Organisation (JIEDDO) and similar organizations across NATO. With large dedicated budgets, their mission is to defeat the IED threat. However, in its first five years of existence, JIEDDO spent over 80% of its budget on mitigation measures only.[20] This led to many critical reports from the US government, the media, and academia. [21] These reports have provided detailed accounts of the current limitations of early C-IED strategy, arguing that JIEDDO was too focused on detection and force protection equipment.

The reports also recognize one essential fact: IEDs cannot be defeated by physical countermeasures alone, such as jammers, detectors, and mine-resistant vehicles. Though these measures have reduced the number of successful IED attacks, they have not completely mitigated the IEDs' strategic effects. Even though the US, Canada, and the

---

[18]For more details, see National Counterterrorism Center, *Report on Terrorism 2011* (Washington, D.C.: Office of the Director of National Intelligence, 2012), http://www.nctc.gov/docs/2011_NCTC_Annual_Report_Final.pdf.

[19]Department of Defense, *Counter Improvised Explosive Device Strategic Plan …*, iii.

[20]Robert Ackerman, "Improvised Explosive Devices: A Multifaceted Threat," *Signal Online* 7 (July 2008), https://afceaeurope.org/content/?q=node/1638.

[21]Key critical reports of JIEDDO's initial efforts are House of Representatives Subcommittee on Oversight & Investigations, *The Joint Improvised Explosive Device Defeat Organization: DOD's Fight Against IEDs Today and Tomorrow* (Washington, DC: U.S. Government Printing Office, 2008); and Richard Ellis, Richard Rogers, and Bryan Cochran, "Joint Improvised Explosive Device Defeat Organization (JIEDDO): Tactical Successes Mired in Organizational Chaos; Roadblock in the Counter-IED Fight," (seminar paper, Joint Forces Staff College, 2007).

UK have fielded a substantial number of mine-resistant ambush protected (MRAP) vehicles, electronic countermeasures (ECM), unmanned aerial vehicles (UAVs), and route clearance packages (RCPs), IEDs are still exploding daily in Afghanistan.

Realizing that technology cannot defeat the IED threat alone, C-IED organizations are now focusing on a C-IED strategy that involves "Left of Boom". This approach disrupts threat networks before IEDs are emplaced by pursuing elements of the network facilitating IEDs, such as builders, planners, suppliers, financiers, and exploiters. As military forces cannot accomplish this alone, since they have limited reach and cannot solely counter the asymmetric nature of the IED system, many military organisations recognize the importance of collaboration across all public spheres through interagency and multinational support. In NATO, and across most of its member states, this collaboration is called the Comprehensive Approach.

The Comprehensive Approach synchronizes the efforts of national departments and agencies, international organizations (IOs), non-governmental organizations (NGOs), multinational partners, and private sector to achieve unity of effort toward a shared goal.[22] This approach can effectively disrupt the IED system since it exploits all instruments of national power: diplomatic, information, military, and economic. As General Stanley McChrystal argues "it takes a network to fight a network."[23] Through collaboration and cooperation, the C-IED network incorporates a wide range of capabilities, from law enforcement to diplomatic.

---

[22]Headquarters of Department of the Army, FM 3-07, *Stabilization Operations* (Washington: US Department of the Army, 2008)1-4.

[23]Stanley McChrystal, "It Takes a Network," *Foreign Policy*, 21 February 2011, http://www.foreignpolicy.com/articles/2011/02/22/it_takes_a_network.

This research paper will demonstrate why the Comprehensive Approach is instrumental to defeating the asymmetric nature of an IED system. It will show why the most effective long-term C-IED strategy is to attack threat networks using the Comprehensive Approach, rather than to focus primarily on tactical force protection and countermeasures to defeat the device. It will also address why it must be done across multinational partnerships, whether in NATO or through a larger coalition. Furthermore, this paper will demonstrate that it cannot be the military driving this strategy due the obstacles that hamper the Comprehensive Approach.

The national governments must synchronize the efforts of various organizations to achieve unity of effort in countering the global threat of IEDs. This approach will ultimately have the greatest impact in reducing the number of casualties, both military and civilian, and therefore protect the instruments of national power. This paper will also consider why IEDs have an asymmetric strategic effect and how the solution is equally asymmetric. More specifically, the investment in attacking the network is considerably lower than the billions spent on force protection which has limited success as it does not primarily focus on "Left of Boom".

This thesis will be demonstrated using three chapters. The first chapter will examine the asymmetric nature of the IED, and why they are effective in both the tactical and the strategic levels. It will also examine how an IED system typically operates and demonstrate why it is difficult to target it using military means alone. The second chapter will examine the current C-IED strategy and its three lines of operation: *Defeat the Device* (DtD), *Prepare the Force* (PtF), and *Attack the Network* (AtN). It will analyse the limitations of each line of operation and highlight why AtN has the greatest effect in

reducing IEDs by disrupting an IED system using the "Left of Boom" approach. It will also show why DtD and PtF are instrumental in supporting AtN activities, and therefore, why the Comprehensive Approach must be applied to maximise effectiveness. The third chapter will demonstrate why the Comprehensive Approach can counter military limitations and effectively disrupt the asymmetric characteristics of an IED system. It will show that governments must bring to bear all instruments of national power to defeat this global threat which erodes public support. It will also address the challenges to the Comprehensive Approach and examine measures to overcome them. To start this analysis, one must consider the nature of an IED system and why IEDs have become the weapons of choice for asymmetric threat forces.

IEDs are weapons of strategic influence because they attack the U.S. national will and try to undermine and eliminate Western influence.

- Lieutenant-General Thomas Metz, *Defense Daily*

CHAPTER 1 – THE IED SYSTEM

Introduction

This paper maintains that there are not IED networks, but threat networks that establish an IED system to build and use IEDs. An IED system is defined as "personnel, resources, and activities that support the execution of an IED event."[24] It includes all elements that fund, supply, plan, build, transport, emplace, trigger, and exploit IEDs. The major challenge when analysing an IED system is that there is no standard template. In armed conflicts, the enemy structure can typically be predicted, even among guerilla and insurgent forces. However, an IED system can be a complex network of individuals, such as Al-Qaida. Alternatively, it can be one or two individuals called "lone wolves".[25]

The other major challenge of an IED system is the nature of the device itself. It can be a simple bomb centered on one small explosive charge designated to kill or maim one or two individuals. On the other hand, it can be a very complex device with multiple explosive charges and counter-intrusion switches designated to also kill first responders such as explosive ordnance disposal (EOD) and IED disposal (IEDD) operators. Understanding all these elements is instrumental in determining how best to disrupt an IED system.

---

[24]NATO Standardization Agency, Allied Joint Publication (AJP)-3.15(A), *(NU) Allied Joint Doctrine For Countering Improvised Explosive Devices* (Brussels: NATO, 2011), 1-2.

[25]Examples of "lone wolves" include Timothy McVeigh and Terry Nichols who bombed Oklahoma City in 1995 or Anders Behring Breivik who bombed Oslo in 2011.

Building IEDs

To analyse the advantages of IEDs for threat networks, one must consider what constitutes an IED and how it is built. The US National Research Council defines an IED as follows:

> An explosive device that is placed or fabricated in an improvised manner; incorporates destructive, lethal, noxious, pyrotechnic, or incendiary chemicals; and is designed to destroy, incapacitate, harass, or distract …. The term *improvised* may apply either to the construction of the device or to its use by irregular forces. Thus, a mine produced for regular forces may be considered an IED if it is used by irregular forces, but an unmodified mine placed by regular forces is not considered an IED. Explosive devices designed to disperse chemical, biological, or radiological material are generally not classified as IEDs.[26]

This definition highlights two key considerations associated with IEDs. First of all, the purpose of the weapon is not just to destroy, but also to harass and distract: it harasses by creating instability affecting military and civilian environments, and it distracts friendly forces that constantly have to deal with the IED threat. Both factors were observed in a number of conflicts, such as the Arab Revolt and the Belorussian Rail War, where IEDs continually disrupted land lines of communications. Second, the improvised nature of the weapon, or the improvised use of an explosive device, creates an asymmetric threat. To understand the asymmetry of the threat, one must consider how the IED is built.

The Canadian C-IED doctrine describes the five major components of an IED.[27] The first component is the switch, which triggers the device. It can be command-activated, time-based, or victim-operated. Command switches include simple electrical

---

[26]National Research Council, *Countering the Threat of Improvised Explosive Devices* (Washington, DC: The National Academies Press, 2007), 1.

[27]Department of National Defence, Canadian Forces Joint Publication 3.15, *Counter Improvised Explosive Devices Operations* (Ottawa: DND Canada, 2012), 1A-1.

wires, cell phones, cordless telephones, and remote car openers.[28] Time-based triggers include digital watches, alarm clocks, and time-fuses.[29] Victim-operated can include a number of innovative switches, such as two pressure plates built using metal saw blades, "low metal content (LMC)" carbon rods, or "no metal content (NMC)" wood plungers, all of which close the circuit when stepped on by the victim.[30] The second component is the power supply, typically a commercial battery.[31] The third component is a container, which can be anything from a plastic jug to a cement truck, or people in the case of suicide IEDs. The fourth component is the explosive charge, which can be military-grade explosives or munitions.[32] For instance, Iraqi insurgents looted hundreds of unsecure ammunition storage sites, allowing them to build thousands of IEDs using conventional munitions.[33] Unexploded ordnance or land mines can also be used, particularly in areas that have been subject to years of armed conflict. In recent years, threat networks have increasingly used fertilizer to manufacture HME, such as ammonium nitrate, potassium chlorate, and even urea.[34] The fifth component is the initiator, which is the hardest to source since it is a military detonator or a commercial blasting cap. However, threat

---

[28]Department of the Army, *Improvised Explosive Device Defeat*…, 4-3.

[29]*Ibid.*

[30]Department of Defense, *Victim Operated Improvised Explosive Devices (VOIED) Recognition Guide – Afghanistan* (Norfolk: Joint Improvised Explosive Device Defeat Organization, 2011), http://info.publicintelligence.net/JIEDDO-VOIED.pdf, 2-9.

[31]Department of the Army, *Improvised Explosive Device Defeat* …, 4-3.

[32]Department of National Defence, *Counter Improvised Explosive Devices Operations*…, 1A-1.

[33]Davi M. D'Agostino, *DOD Should Apply Lessons Learned Concerning the Need for Security over Conventional Munitions Storage Sites to Future Operations Planning* (United States Government Accountability Office: GAO-07-639T, 22 March 2007) http://www.gao.gov/assets/120/115974.pdf, 8.

[34]Charles Johnson, *U.S. Agencies Face Challenges Countering the Use of Improvised Explosive Devices in the Afghanistan/Pakistan Region* (United States Government Accountability Office: GAO-12-907T, 12 July 2012), http://www.gao.gov/products/GAO-12-907T, 6.

networks are finding innovative ways to manufacture initiators in improvised manners using pens, bullet casings, and Christmas tree lights.[35]

The dual-use nature of these components bestows four major advantages for threat networks. First, since they are innocuous objects, IED components can be easily purchased and smuggled through legitimate businesses without attracting the attention of intelligence or law enforcement agencies.[36] For instance, "red flags" would not appear if a person bought cell phones, saws, or computer circuit boards. Even the acquisition of fertilizer can be justified by using a farming cover story. However, trying to buy small arms, rocket-propelled grenades (RPGs), or mortars requires a much more complex network of arm dealers. In addition, they cannot be as easily smuggled since no one can argue that these weapons have peaceful purposes. The second advantage of IEDs is the cost. For example, a jug of HME, a detonator, simple electrical wires, and a battery cost approximately 30 USD.[37] The price of IEDs versus C-IED equipment creates an asymmetric advantage in favour of threat networks. The third major advantage is the simplicity of design of IEDs. As components are mainly commercial products and construction techniques are widely available on the Internet, a high degree of expertise is not required to build IEDs.[38] The fourth advantage is that threat networks can easily adapt the design. A useful example of the ease in modifying IEDs is provided by journalist Glenn Zorpette:

---

[35]Department of Defense, *Victim Operated Improvised Explosive Devices* …, 20.
[36]Department of Defense, *Counter Improvised Explosive Device Strategic Plan*…, iii.
[37]Rachel Martin, "The IED: The $30-Bombs That Cost The U.S. Billions," *NPR*, 17 December 2011, http://www.npr.org/2011/12/18/143902421/in-iraq-fighting-an-improvised-war.
[38]Department of Defense, *Counter Improvised Explosive Device Strategic Plan*…, 3.

> Early on, in 2003 and 2004, most IEDs in Iraq and Afghanistan were triggered wirelessly, often with cellphones, long-range cordless phones, key fobs, walkie-talkies, and wireless doorbells. Relying on modified existing hardware and Navy expertise, JIEDDO's predecessor quickly fielded jamming systems…. The insurgents' response to the first jammers, in late 2003, was swift. It established a *Spy vs. Spy* –like competition between counter-IED specialists and the bomb makers, in which sometimes a measure was followed by a countermeasure within days. As jammers proliferated, insurgent groups quickly went back to using command wires—buried pairs of long enameled copper wires attached to a simple switch—and also to "victim-operated" triggers.[39]

As they can rapidly modify IEDs, threat networks can also counter friendly forces tactics. For instance, in Afghanistan, the Taliban observed International Security Assistance Force (ISAF) troops, identified their vulnerabilities, particularly how IEDs were being detected, and focused on building IEDs with low or no metal content.[40] The Taliban also built IEDs using 1,500 pounds of HME to destroy MRAPs and RCPs, sending a message to friendly forces that they can defeat any vehicle, no matter how heavily protected.[41] The IED design can also be modified based on the components readily available; in Pakistan, insurgents shifted to potassium chlorate since the more available calcium ammonium nitrate (CAN) was tracked by US intelligence agencies.[42] All these advantages allow the threat networks to maintain the upper hand. Consequently, friendly forces are often in a reactive mode, needing to adapt their techniques, tactics, and procedures (TTPs) to counter those of the enemy. This further supports the argument that the solution must focus on "Left of Boom".

---

[39]Glenn Zorpette, "Countering IEDs" …

[40]Andrew Johnson, "Taliban make 'undetectable' bombs out of wood," *The Independent*, 10 January 2010, http://www.independent.co.uk/news/world/asia/taliban-make-undetectable-bombs-out-of-wood-1863353.html.

[41]David Eisler, "Counter IED in Modern War," *Military Review* 9, no. 1 (Jan-Feb 2012): 9-10.

[42]Johnson, *U.S. Agencies Face Challenges* …, 5.

IEDs as Weapons of Strategic Influence

The dual-nature of components is not the only advantage of using IEDs. As the epigraph of this chapter highlights, IEDs have strategic effects by attacking a country's strategic center of gravity: its national will. Due to their influence, IEDs became the weapon of choice for threat networks, and have been used in a wide range of conflicts in the past ten years, from the drug war in Mexico to the Islamic insurgency in Somalia.[43] In 2011 alone, there were 8,541 IED events in 70 countries (excluding Afghanistan and Iraq), representing 57% of all types of asymmetric attacks worldwide.[44] They caused 54,290 deaths and injuries, which corresponds to 70% of all terrorist-related casualties.[45]

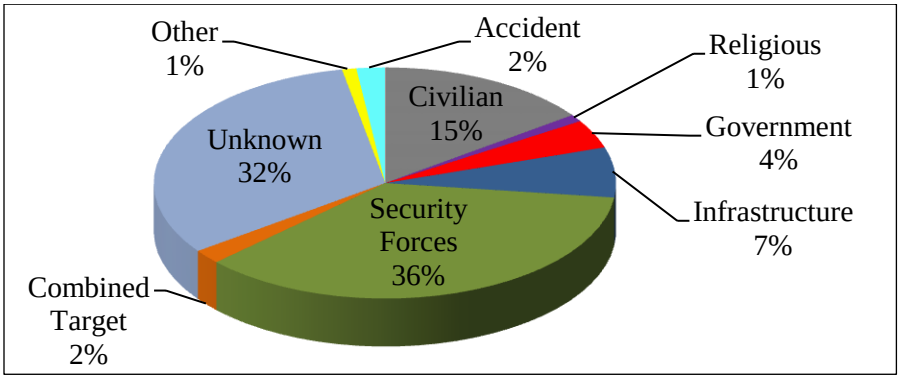


Figure 1 - IED by Target (August 2010 to August 2012)

Source: Department of Defence, "JIEDDO Global IED Monthly Summary Report," 6.

Figure 1 presents the number of IED-related casualties worldwide in 2011 and demonstrates how IEDs affect the four instrument of national power: military, information, economics, and diplomacy.

---

[43]Department of State, *Country Reports on Terrorism 2011*, CRT12, July 2012, http://www.state.gov/j/ct/rls/crt/2011/, 5.

[44]National Counterterrorism Center, *Report on Terrorism 2011* (Washington: Office of the Director of National Intelligence, 2012), http://www.nctc.gov/docs/2011_NCTC_Annual_Report_Final.pdf, 13.

[45]*Ibid*.

Influencing Military Power

As highlighted in the introduction, history provides a number of examples where IEDs were used to avoid an opponent's military strength. By understanding the concepts of asymmetrical warfare and by applying the military philosopher's Maurice de Saxe's principle of "achieving victory without decisive battle", T.E. Lawrence used IEDs to attrite the Turkish Army during the Arab Revolt in 1916 to 1918.[46] He understood that he could use IEDs to attack his enemy's will by destroying food, water, and other supplies, while avoiding a decisive engagement.[47] Therefore, Lawrence used innovative methods to enable the untrained, undisciplined, and ill-equipped Arab army to succeed against the much larger and professional Turkish force.[48]A similar approach was used by the IRA against the British Army in Northern Ireland.[49]

In today's operational environments, threat networks use IEDs to strike friendly forces without being decisively engaged, reducing the impact of the West's considerable combat capabilities of heavy weapons, attack aviation, and close air support. Therefore, IEDs are much like cruise-missiles and armed UAVs, providing a stand-off weapon. By being able to use timed, victim-operated, or remote-controlled switches, they can strike at the location and timing of their choice, without being present at the place of the attack.

---

[46]Thomas E. Lawrence, *Seven Pillars of Wisdom: A Triumph* (Oxford: Alden Press, 1952), 232.

[47]Lawrence W. Moores, "T.E. Lawrence: Theorist and Campaign Planner," (monograph, US Army Command and General Staff College, 1992), 12.

[48]Thomas E. Lawrence, *Seven Pillars of Wisdom*…, 194.

[49]Department of Defense, *Counter Improvised Explosive Device Strategic Plan* …, 2.

Another advantage of using IEDs is that they can be used in complex attacks; combining IEDs with small arms and RPGs which can significant affect friendly forces' tactical plan. As Canadian Senator Pierre Nolin notes:

> IEDs often invalidate conventional military tactics, such as the fire and manoeuvre tactics of troops in contact. IEDs are often used to 'fix' troops in an area before other forms of attack are used, like small arms ambushes or sniper attacks.[50]

The War in Afghanistan provides a number of examples of effective complex attacks. Two occurred in Kabul in January 2013 where militants used a combination of suicide vehicle-borne IEDs (SVBIED) and direct attacks. After exploding the car bomb, they stormed the National Directorate of Security (NDS) building and a police headquarters, which led to firefights lasting many hours.[51] Similar tactics were used in Oslo in 2011. Breivik used a VBIED to distract and misdirect Norwegian counter-terrorism forces, allowing him to attack the island of Utoeya, killing 91 people in the combined attack.[52] These examples demonstrate that IEDs not only disrupt military operations, but those of other security forces as well.

In addition to creating havoc on the battlefield, IEDs have second and third order effects. For instance, IEDs restrict freedom of movement, since friendly forces have to conduct deliberate and time-consuming route clearance operations or avoid entire areas

---

[50]Pierre Claude Nolin, *Countering the Afghan Insurgency: Low-Tech Threats, High-Tech Solutions* (NATO Parliamentary Assembly Special Report: 189 STC 11 E Bis Final, October 2011), http://www.nato-pa.int/default.asp?SHORTCUT=2551, 2.

[51]Hamid Shalizi, "Coordinated Kabul suicide attack targets government building," *Reuters*, 21 January 2013, http://www.reuters.com/article/2013/01/21/us-afghanistan-blast-idUSBRE90K03120130121.

[52]William Boston, "A Killer in Paradise: Inside the Norway Attacks," *Time*, 23 July 2011, http://www.time.com/time/world/article/0,8599,2084835,00.html#ixzz2JJwPxcL7.

designated as "IED hot-spots". [53] Journalist Adam Day also highlights the impacts on civilian mobility:

> The movement-limiting effects of the IEDs impact more than just the military. The bombs force road closures in the worst cases, which leaves whole villages basically deserted, but even when the roads remain open they have an effect on the normal flow of traffic necessary for markets to remain open and farmers to get their crops into the cities and for normal development to occur.[54]

To avoid having negative impacts on local economies, friendly forces must commit troops to repair the roads destroyed by IEDs, or alternatively build their own roads to avoid hot-spots. This was done in Afghanistan when "Canadian troops bulldozed through grape fields and built a paved two-lane highway called Route Summit, which also gave safe passage to local farmers as well as ISAF troops."[55] Building roads to avoid IEDs does have its consequences. Friendly forces must allocate security to these laborious projects, taking away from other security tasks such as securing a village. In addition, there is no guarantee that the road will not be targeted.

IEDs also impact when they damage or destroy friendly forces' vehicles or cause casualties, one of the military critical vulnerabilities. Lieutenant-Colonel Ian Hope, the Canadian Battle Group Commander in 2006, provides an account of how his mission changed when IEDs exploded during offensive operations:

---

[53]Adam Day, "Left Of The Boom," *Legion Magazine*, January 19, 2009, http://www.legionmagazine.com/en/index.php/2009/01/left-of-the-boom/.

[54]*Ibid.*

[55]University of Waterloo, "Engineering Under Fire," last accessed 23 December 2012, https://info.uwaterloo.ca/www/profiles/profile.php?id=103.

> I was adamant that we would never leave a damaged fighting vehicle on the battlefield, even if it were completely burnt out, as a monument for the *Dushman* to gloat over. So vehicle recovery, like casualty evacuation, often became the mission during operations. One may criticize the inevitable loss of momentum this brought. To this I respond that the destruction of no number of Taliban was so important as the safe evacuation of one Canadian (or Afghan) soldier, and that no number of Taliban killed was equal to the propaganda victory they would have by the abandonment of one of our LAVs on a battlefield and its televised image on the evening CNN Broadcast. The reality of wounding and death changed our notions of the need for tactical momentum in a fight.[56]

This statement is particularly important in understanding why IEDs have become a weapon of strategic influence. IEDs have been responsible for more casualties than any other weapon system combined in both Afghanistan and Iraq.

In Iraq, the insurgents emplaced over 81,000 IEDs from 2003 to 2007, which caused more than 66% of US casualties.[57] In Afghanistan, the percentage of IED-related coalition deaths went from 25% between 2001 and 2007, to 54% between 2008 and 2012.[58] Figure 2 illustrates the number of IEDs in Afghanistan and the associated casualties (CAS) in terms of killed in action (KIAs) and wounded in action (WIAs). When examining this figure, IED use increased by 500% between October 2006 and October 2009. For certain troop-contributing nations (TCNs), IED-related casualties were significant. For instance, IEDs were responsible for three quarters of Canadian Forces (CF) casualties in Afghanistan.[59]

---

[56]Ian Hope, *Dancing with the Dushman: Command Imperatives for the Counter-Insurgency Fight in Afghanistan* (Kingston: Canadian Defence Academy Press, 2008), 7.

[57]Rick Atkinson, "The Single Most Effective Weapon Against Our Deployed Forces," *Washington Post*, 30 September 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/29/AR2007092900750.html.

[58]Icasualties.org, *Operation Enduring Freedom* (2013), last accessed 18 January 2013, http://icasualties.org/OEF/index.aspx.

[59]*Ibid.*

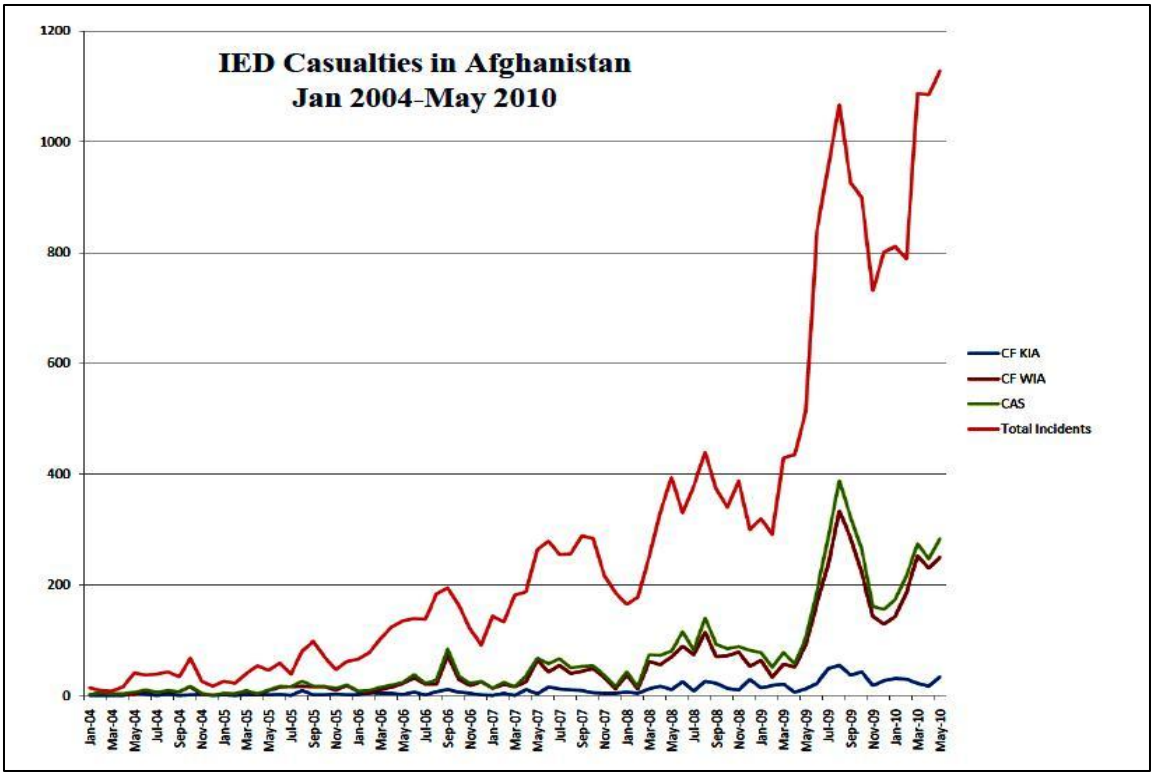


Figure 2 - IED Casualty Figures in Afghanistan (Jan 2004-May 2010)

Source: Cordesman *et al.*, "IED Metrics for Afghanistan," 6.

In total, over 100,000 IEDs were emplaced in Afghanistan and Iraq from 2001 to 2010.[60] Many other sources also provide metrics on the number of casualties in Afghanistan.[61] Although the official numbers vary from one source to another, they all show a significant increase in the number of IED attacks and their impact on the physical domain of friendly forces, killing over a thousand and injuring more than ten thousand ISAF soldiers.

---

[60]Anthony H. Cordesman, Charles Loi, and Vivek Kocharlakota, "IED Metrics for Afghanistan January 2004 - September 2010," *Centre for Strategic Studies*, November 11, 2010, last accessed 23 December 2012, http://csis.org/files/publication/101110_ied_metrics_combined.pdf.

[61]For examples, see Department of Defense, *Joint Improvised Explosive Device Defeat Organization 2006 Annual Report* (Norfolk: Joint Improvised Explosive Device Defeat Organization, 2006), https://www.jieddo.mil/ content/docs/2006_JIEDDO_Annual_Report_(U).pdf; and Icasualties.org, "Operation Enduring Freedom", last accessed 18 January 2013, http://icasualties.org/OEF/index.aspx.

Yet IEDs have affected more than the physical domain. In addition to KIA and WIA, IEDs have caused a significant number of cases of Post-Traumatic Stress Disorder (PTSD). Dr Bruce Capehart has reviewed the cases of PTSD in the US military and has identified that the prevalence is between 13 to 21% among combat veterans with 80% of those cases caused by IEDs.[62] Similarly, Canadian estimates show that up to 13% of CF personnel who served in Afghanistan could be suffering from PTSD.[63] A possible reason for the high rate of PTSD is the nature of the IED attack; they have a considerable psychological effect on victims. Since IEDs provide a stand-off capability, soldiers rarely see their attackers and therefore cannot respond using force. IEDs provide anonymity and the advantage of surprise. Thus, friendly forces may feel that they are fighting an invisible enemy, who can appear anywhere, anytime, and strike without warning. As Adam Day argues, "it is literally a death by a thousand cuts."[64] Unit morale is reduced, which in turn affect cohesion and efficiency on the battlefield.[65] Therefore, by attacking friendly physical and psychological domains, the threat networks affect another instrument of power: information.

---

[62]Bruce Capehart, "Managing Posttraumatic Stress Disorder In Combat Veterans With Comorbid Traumatic Brain Injury," *Journal of Rehabilitation Research & Development* 49, no. 5 (May 2012): 790, http://www.rehab.research.va.gov/jour/2012/495/pdf/capehart495.pdf

[63]Lee Berthiaume, "Over 2,000 Canadians were wounded in Afghan mission: report," *National Post*, 1 February 2012, http://news.nationalpost.com/2012/02/01/over-2000-canadians-were-wounded-in-afghan-mission/.

[64]Day, "Left Of The Boom" …

[65]NATO, *Allied Joint Doctrine For Countering Improvised Explosive Devices* …, xiii.

Influencing the Power of Information

In his in-depth article on IEDs and the efforts of the CF to counter them, Adam Day states that "each Canadian killed means bad headlines and another funeral and one more blow against the Canadian public's perception of the mission."[66] The images of "ramp ceremonies" where flag-draped coffins were loaded into military aircraft have dominated the War in Afghanistan, particularly for Canadians. It is also true in other nations where each soldier killed by this anonymous threat created a strategic effect on their population. IEDs are also killing and wounding thousands of civilians. As reported by the United Nations Assistance Mission in Afghanistan (UNAMA) annual report, "the widespread use of IEDs by Anti-Government Elements was the single largest cause of civilian deaths and injuries in Afghanistan in 2011, with 967 civilian deaths and 1,586 injured."[67] Threat networks use IEDs against civilians to "create fear, incite violence, and generally disrupt efforts to stabilize countries in conflict."[68] It can also demonstrate the friendly forces' inability to "deliver security, leading to widespread feelings of insecurity with a debilitating effect on the host nation population, potentially resulting in a loss of confidence and support for alliance activity."[69] Threat networks understand the power of using information to their advantage, particularly through the use of the Internet and social media.

---

[66]Day, "Left Of The Boom" …

[67]United Nations Assistance Mission in Afghanistan, *Afghanistan Annual Report 2011: Protection of Civilians In Armed Conflict* (Kabul: UNAMA, 2012), http://unama.unmissions.org/Portals/UNAMA/Documents/UNAMA%20POC%202011%20Report_Final_Feb%202012.pdf, 16.

[68]House of Representatives Subcommittee on Oversight & Investigations, *The Joint Improvised Explosive Device Defeat Organization: DOD's Fight Against IEDs Today and Tomorrow* (Washington, DC: U.S. Government Printing Office, 2008), http://www.fas.org/irp/congress/2008_rpt/jieddo.pdf, 14.

[69]NATO, *Allied Joint Doctrine For Countering Improvised Explosive Devices* …, xiii.

With the advent of the digital era, threat network can easily record IED attacks and post them on websites for anyone to see. In his study of terrorist use of the social media, Dr Cori Dauber argues that "their true target is not that which is blown up… What is really being targeted are those watching at home."[70] These arguments reinforce the notion that IEDs are weapons of strategic influence, particularly in the information realm. An IED not only attacks military power, but hits where it hurts the most: the national will. In the wake of the 9/11 attacks, 75% of Canadians approved of the Afghan mission.[71] Yet, after sustaining 158 deaths, of which 110 were caused by IEDs, the approval rating fell to 32% in 2011.[72] The situation is similar in the US, where only 25% of Americans supported the War in Afghanistan in March 2012, down from 50% in September 2006.[73] The images of dead soldiers returning home, combined with the reports of civilian casualties, have considerably eroded public support for both missions.

The number of casualties is not the only factor in the loss of public support. In their paper *Success Matters*, the authors have published an in-depth study on the US support for the War in Iraq.[74] They have examined tolerance for the casualties in relation to the perception of success and the rationale for the conflict:

---

[70]Cori Dauber, "Youtube War: Fighting in a World of Cameras in Every Cell Phone and Photoshop on Every Computer" (monograph, Strategic Studies Institute, 2009), v.

[71]Canadian Broadcasting Corporation, "Fewer Canadians 'strongly approve' of Afghan mission: survey," *CBC News*, 9 November 2006, last accessed 29 January 2013, http://www.cbc.ca/news/canada/story/2006/11/08/afghanistan-survey.html.

[72]Angus-Reid, "Britons and Canadians Oppose Afghan War; Americans Evenly Divided," last accessed 7 January 2013, http://www.angus-reid.com/polls/43776/britons-and-canadians-oppose-afghan-war-americans-evenly-divided/.

[73]Cable News Network, "CNN/ORC Poll – March 24-25 – Afghanistan" ….

[74]Christopher Gelpi, Jason Reifler, and Peter Feaver, "Success Matters: Casualty Sensitivity and the War in Iraq," *International Security* 30, no. 3 (Winter 2005/06): 7-46, http://www.mitpressjournals.org/toc/isec/30/3.

> We believe that the decline in public support for the war reflects the mounting death toll combined with a perceived lack of measurable progress toward "success" that eroded the public's hopes that the war may eventually be won.[75]

This statement is important to understand how the "information war" can be won or lost. If the public believes that IEDs cannot be defeated or the number of attacks is continually rising, then maintaining popular support will be difficult. If the public believes that IEDs are undefeatable, the government and the military must inform the public on steps being taken to defeat them. In the past few years, western countries have announced the creation of C-IED task forces and organizations. However, the initial thrust was focused on announcing the purchase of millions of dollars' worth of force protection equipment. As an example, when the UK Secretary of Defense announced the acquisition £400m of protected vehicles and other C-IED measures, he stated "protecting our forces from IEDs is our most urgent challenge."[76] There is a belief in government that force protection is the critical element in C-IED strategy. The loss of public support drives governments to find quick solutions to regain the advantage in the information domain as highlighted by Rear-Admiral Arch Macy: "Americans want technical solutions. They want the silver bullet…. [Yet], the solution to IEDs is the whole range of national power -political-military affairs, strategy, operations, and intelligence."[77] This is an example of military officers understanding the importance of the "Left of Boom" strategy. Chasing "silver bullets" also significantly impact the economy.

---

[75]Christopher Gelpi, Jason Reifler, and Peter Feaver, "Success Matters…," 9.

[76]David Pugliese, "More Counter-IED Equipment and Protected Vehicles Being Sent to British Forces in Afghanistan," *Ottawa Citizen*, 23 December 2011, http://blogs.ottawacitizen.com/2011/12/23/more-counter-ied-equipment-and-protected-vehicles-being-sent-to-british-forces-in-afghanistan/.

[77]Atkinson, "The Single Most Effective Weapon…"

Influencing Economics

If IEDs are an asymmetric threat, then the cost of C-IED is equally asymmetric. Though an IED can be built for less than $100, it effectively destroys resources that cost millions of dollars. For example, a CF report indicates that 34 CF vehicles were destroyed in Afghanistan, and another 359 were damaged.[78] It included thirteen Light Armored Vehicles III (LAV-III) and three Leopard-2 tanks. Though the report does not provide their replacement cost, the price tag will be in the tens of millions of dollars.

The Canadian Government has reported that the estimated cost of the Afghan mission is $11.3 billion, with $8.8 billion related to CF operations.[79] It recognizes that there will be incremental costs for replacing equipment destroyed by IEDs and for providing psychological support to soldiers and veterans suffering from PTSD. The independent research conducted by the Rideau Institute considers the figures to be inaccurate and argue that the cost is much higher, reaching $28.4 billion. The cost of replacing soldiers killed or injured during the mission is estimated to be $7.6 billion.[80] When considering that 75% of CF casualties were IED-related, it can be deduced that these weapons caused $5.7 billion in economic loss.[81]

For the US, the amount expended to counter IEDs in Iraq and Afghanistan has been significant. JIEDDO spent over $18 billion funding C-IED initiatives, such as ECM,

---

[78]David Pugliese, "34 Canadian Forces Vehicles Destroyed, 359 Damaged During Afghan War," *Ottawa Citizen*, 19 July 2012. http://blogs.ottawacitizen.com/2012/07/19/34-canadian-forces-vehicles-destroyed-359-damaged-during-afghan-war-list-includes-3-leopard-tanks-destroyed/.

[79]Government of Canada, "Cost of the Afghanistan Mission 2001-2011," last accessed 7 January 2013, http://www.afghanistan.gc.ca/canada-afghanistan/news-nouvelles/2010/2010_07_09.aspx?view=d.

[80]Michael Higgins, Jonathan Rivait, and Andrew Barr, "Blood and Treasure," National Post, 22 June 2011, http://afghanistan.nationalpost.com/graphic-blood-treasure/.

[81]Icasualties.org, *Operation Enduring Freedom* (2013), last accessed 18 January 2013, http://icasualties.org/OEF/index.aspx.

RCPs, and other countermeasures. [82] DoD funded another $47 billion for the procurement of 28,000 MRAPs.[83] The UK has also procured over 1,000 mine-protected vehicles at the cost of £1 billion.[84] Yet, threat networks continue to increase their attacks, and successfully demonstrate that hardened vehicles and jammers cannot entirely protect against IEDs. U.S. Secretary of Defence Donald Rumsfeld recognized this fact when he stated: "If you think about it, you can have all the armor in the world on a tank and a tank can be blown up."[85] The pursuit of a technological "silver bullet" has cost western nations billions of dollars, but has not avoided the IED's strategic influence. Consequently, the blood and treasure spent by western countries has taken its toll on the national will. Spending billions fighting a threat perceived as undefeatable affects the last instrument of power: diplomatic.

Influencing Diplomacy

When a nation loses popular support for a military intervention, politicians start questioning the value of the mission, especially if the costs are high. This was seen in the past during the US interventions in Vietnam and Lebanon. In both cases, IEDs were used by the enemy to influence the US government's will, either through protracted campaigns or by spectacular attacks to kill hundreds. Both approaches are used in Afghanistan. The

---

[82]International Institute for Strategic Studies, "IEDs: The Home-Made Bombs that Changed Modern War," *Strategic Comments* 18, no. 24 (August 2012): 2, http://www.iiss.org/publications/strategic-comments/past-issues/volume-18-2012/.

[83]*Ibid.*

[84]Ministry of Defence, "UK Forces: Operations in Afghanistan," last accessed 7 January 2013, https://www.gov.uk/uk-forces-operations-in-afghanistan.

[85]Eric Schmitt. "Iraq-Bound Troops Confront Rumsfeld Over Lack of Armor." *The New York Times*, 8 December 2004. http://www.nytimes.com/2004/12/08/international/middleeast/08cnd-rumsfeld.html?_r=0.

cost in casualties has caused many nations to question the value of the mission, creating tension within NATO. For example, US Secretary of Defence Robert Gates criticized NATO member states when he said: "Frankly, there is too much talk about leaving and not enough talk about getting the job done right."[86] Due to human and material costs, every nation is trying to find its own exit strategy. The diverging views on how to end the war has caused considerable strain on the Alliance. In the wake of the high number of CF casualties, the Canadian Parliament debated the future of the Afghan mission in 2008, resulting in a confidence motion.[87] Though the motion passed and the mission was extended, the CF ended its combat mission in 2011.

In some cases, IEDs have affected a nation's foreign policy. For instance, in 2004, three days before the Spanish national election, ten IEDs exploded in Madrid, killing 191 and injuring over 1,800 people.[88] The impact of the explosions was more than just death and destruction. As Dr Tom Dannenbaum argues, the attacks directly influenced the election result: the newly elected Spanish government pulled out of the coalition in Iraq.[89] The Spanish action reduced the number of available forces for the coalition and soured the relationship with the US and other allies. They felt that the Spanish had appeased the

---

[86]Robert M. Gates, (speech, NATO Headquarters, Brussels, Belgium, March 11, 2011), http://www.defense.gov/speeches/speech.aspx?speechid=1547.

[87]Canadian Broadcasting Corporation, "Canada's Military Mission in Afghanistan: Training Role to Replace Combat Mission in 2011," *CBC News*, February 10, 2009, last accessed 23 December 2012, http://www.cbc.ca/news/canada/story/2009/02/10/f-afghanistan.html.

[88]Department of Homeland Security, *IED Attack: Improvised Explosive Devices* (Washington, DC: The National Academies Press, 2007), http://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf, 1.

[89]Tom Dannenbaum, "Bombs, Ballots, and Coercion: The Madrid Bombings, Electoral Politics, and Terrorist Strategy," *Security Studies* 20, no. 3 (July 2011): 303–349.

terrorists and sent out a message that terrorists can successfully influence political decisions.[90]

IEDs also affect the diplomatic instruments of power when they are used to directly target political and diplomatic elements. As Figure 1 demonstrated, government institutions and personnel were direct targets in IED attacks. Though the government only represent 4% of targets over a 25-month period, it does not take many IEDs to destabilize a government's resolve. Such was the case in Afghanistan when an IED killed Canadian diplomat Glyn Berry. As General Hillier noted in his book *Soldier First*:

> Berry was the first Canadian diplomat ever to be killed in the line of duty, and his death caused near panic in the Department of Foreign Affairs (DFAIT) and [Canadian International Development Agency] CIDA. Both departments essentially disappeared from Kandahar after that and stayed away for much of the critical period that followed.[91]

As a result, the CF was left to implement development and improve governance with little support from other government departments (OGDs). The absence of DFAIT and CIDA representatives seriously affected the Canadian government's diplomatic efforts in Kandahar. A single IED had impacted the Government of Canada's efforts in Afghanistan at the strategic level.

A similar situation occurred in Iraq on August 19, 2003 when a SVBIED exploded at the United Nations compound in Baghdad, killing 22 UN workers including the UN Special Representative, Sergio Vieira de Mello.[92] Fearing for the safety of its

---

[90]Tom Dannenbaum, "Bombs, Ballots, and Coercion…," 305.

[91]Rick Hillier, *A Soldier First: Bullets, Bureaucrats and the Politics of War* (Toronto: HarperCollins Publishers, 2009), 388.

[92]Talif Deen, "U.N. Pullout from Baghdad Threatens to Undermine U.S.," *Inter Press Service*, 31 October 2003, www.ipsnews.net/2003/10/politics-un-pullout-from-baghdad-threatens-to-undermine-us/.

staff, the UN withdrew close to 500 personnel, leaving only 60 in Iraq.[93] This decision significantly shaped the UN's diplomatic mission and also raised concerns that other IOs and NGOs would follow suit. These examples show how a single IED can disrupt diplomatic efforts of western governments involved in stabilization operations.

Overall, all four instruments of power are interlinked. A costly mission, both in terms of human and economic resources, is hard to "sell", and erodes public support, as seen in Iraq and Afghanistan. Though IEDs are not the only factor in play, when threat networks inflict over two-thirds of military casualties, and force nations to spend billions countering cheap devices, insurgents gain the upper hand. The cost of the war causes politicians to re-consider their nation's participation, especially if their government officials are directly targeted. This is why governments must protect their instruments of power by using all available resources, not only the military, to counter IEDs. To do so, they must understand how an IED system operates.

The IED System

Though an IED system is difficult to attack since there is no single model on how it operates, there are ways to predict their structure based on the activities related to emplacing IEDs. The following section will analyze how threat networks are typically organized and how they facilitate, deploy, and employ IEDs. Understanding their IED system reveals the vulnerability of threat networks. To start, one must examine a typical IED-facilitating network.

---

[93] *Ibid.*

IED as a Weapon of Choice

Figure 3 shows that IED attacks occurred throughout every US Combatant Command (COCOM) Area of Responsibility (AOR) in one month alone in 2011. IED attacks were carried out by a wide range of threat networks; from drug cartels and insurgents in Columbia to Chechen separatists in Russia.

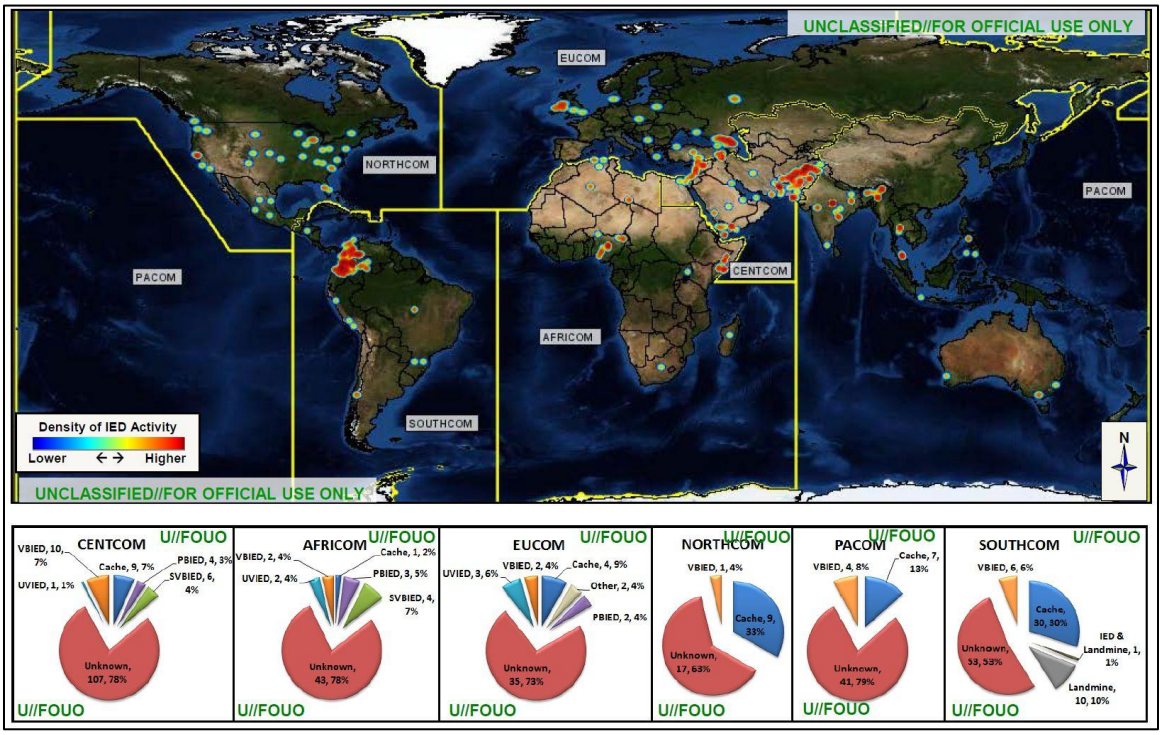


Figure 3 - IED Attacks Worldwide by Combatant Commander

Source: Department of Defence, "JIEDDO Global IED Monthly Summary Report," 4.

The document reveals that IEDs are not just weapons of Islamist terrorist and insurgent groups, or exclusive to the Central Command (CENTCOM) and African Command (AFRICOM) AOR. In fact, IEDs are a regular occurrence in the European Command (EUCOM), Northern Command (NORTHCOM), and Southern Command (SOUTCOM) AORs. IEDs are used by Christian terrorists, white supremacists, anarchists, transnational

crime syndicates, and drug trafficking organizations.[94] They are present in every continent, in failed and failing states, as well as in western nations.

IED Threat Network

To be able to target threat networks that use IEDs, one must understand how the network is organized, the relationship between different actors, and their vulnerabilities. Figure 4 describes a typical model of a threat network employing IEDs using a notional timeframe.

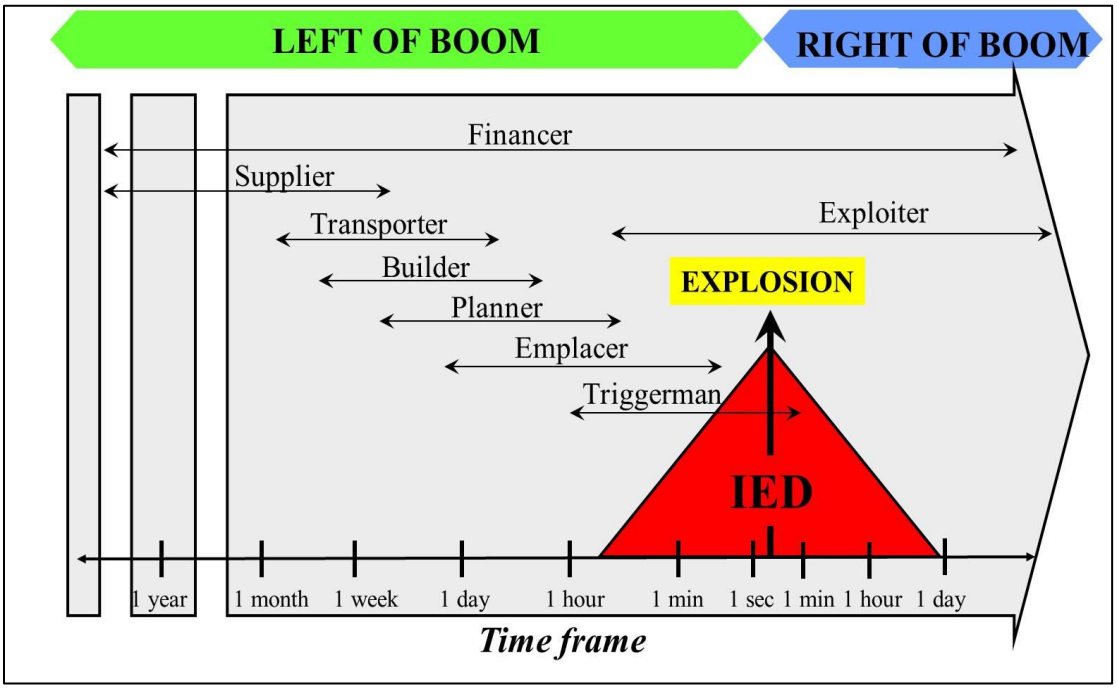


Figure 4 – Typical Threat Network Model

Source: Allied Command Transformation, "ACT C-IED IPT Briefing to COE C-IED, 18 Jan 2011," 58.

[94]Department of Defence, *JIEDDO Global IED Monthly Summary Report* (Norfolk: Joint Improvised Explosive Device Defeat Organization, 2012), http://publicintelligence.net/jieddo-global-ieds-aug-2012/, 1-34.

This model is particular useful in understanding how various people are required to facilitate the production, the use, and the exploitation of IEDs over time. It is noted that there may be only one individual performing every function, such as Anders Behring Breivik when he planned and executed the attack in Norway. However, it is typically a complex network of individuals, and can involve different insurgent, terrorist, and criminal groups, all working towards their own objectives. For instance, organized crime syndicates (OCS) can facilitate the transport of IED components across borders, since they already have an established network to traffic other illicit material, such as drugs and weapons. OCS does not need ideological links with insurgent or terrorist groups as their primary objective is to make money. This is evident in Somalia where the terrorist group Al-Shabaab, an Al-Qaida ally, is suspected of using Kenyan criminal networks to smuggle IEDs across the border.[95]

Suppliers could be persons that have absolutely no ties to the threat network. As IED components are most commonly commercial products, the supplier could be a legitimate business that has no knowledge of the intended use of their product, such as circuit boards or cordless phones. Alternatively, it can be a nation-state that provides components, as seen in Iraq where the Iranians are supplying explosive formed projectiles (EFPs) and other IED-making devices.[96]

---

[95]Department of Defense, *Al-Shabaab's Exploitation of Alternative Remittance Systems (ARS) in Kenya*, (Norfolk: Joint Improvised Explosive Device Defeat Organization, 2009), http://info.publicintelligence.net/JIEDDO-AlShabaabARS.pdf, 4.

[96]Michael R. Gordon and Scott Shane, "The Struggle for Iraq; Behind U.S. Pressure on Iran, Long-Held Worry Over a Deadly Device in Iraq," *The New York Times*, 27 March 2007, http://query.nytimes.com/gst/fullpage.html?res=F40C1EF639540C748EDDAA0894DF404482.

The IED builder could be an expert from another terrorist group, who may or may not have similar ideology. The conflict in Columbia, where the IRA sent IED experts to train the Revolutionary Armed Forces of Colombia (FARC) and the Ejército de Liberación Nacional (ELN), provides an example of cross-exchanging IED building expertise. With regards to the emplacer and triggerman, they can be people that have very little to do with the threat network. The motivation to convince someone to emplace and/or trigger IEDs may be through financial gain, coercion, or brainwashing. For instance, Afghanistan insurgents pay locals approximately $250 to $300 to emplace IEDs.[97] This is a significant amount of money when you consider that the average annual income of an Afghan civilian is $1,000.[98] In addition, it is reported that 90% of suicide bombers in Pakistan are aged between 12 and 18, and some are as young as five years old.[99] Therefore, targeting emplacers and triggermen will have little effect on disrupting IED systems. The strategy must also pursue the other elements that facilitate IEDs.

The examples above demonstrate the various relationships between the elements in an IED system which is a fundamental consideration in analyzing its organization. The US Joint Publication on C-IED Operations notes this importance:

> IED networks are centrally and de-centrally organized because of the need to protect relationships and hide activities at the tactical, operational, and strategic levels. The leadership of these IED networks plan, organize, and execute many critical activities necessary to accomplish their objectives.

---

[97]William H. Graham, *Learning From The Enemy – Offensively, What IEDs Should Teach The U.S.* (civilian Research Paper, U.S. Army War College, 2010) http://www.dtic.mil/dtic/tr/fulltext/u2/a545052.pdf, 5.

[98]Central Intelligence Agency, "CIA World Factbook: Afghanistan," last accessed on 7 March 2013, https://www.cia.gov/library/publications/the-world-factbook/geos/af.html.

[99]Kalsoom Lakhani, "Indoctrinating Children: The Making of Pakistan's Suicide Bombers," *CTC Sentinel* 3, no. 6: 11. http://www.ctc.usma.edu/wp-content/uploads/2010/08/CTCSentinel-Vol3Iss6-art4.pdf.

> Within these IED networks, functional plans and operations are interconnected and may impact each other in direct and indirect ways and at all levels. Recognizing these interrelationships is critical when attempting to attack a network.[100]

A number of in-depth analysis in books and academic papers have been written on the various relationships among threat networks.[101] They show that recent threat networks are loose networks of like-minded individuals, sometimes working together, sometimes working independently. They are also less hierarchical and more interconnected, either based on geography, ideology, or through a common enemy. Furthermore, they can form spontaneously by self-recruitment and self-organization.[102]

In addition, threat networks can operate across national boundaries. For instance, builders, planners, and triggermen may be operating in the conflict state, but they can also be based in a neighboring country. Financiers and suppliers could be anywhere, smuggling money and components through transporters. This loose network is hard to disrupt using military means alone, since the military is often restrained to operate inside a designated battlespace, such as a Joint Operations Area (JOA).

Another important notion to understand is how the IED system operates both within and outside the JOA. Figure 5 illustrated a model for threat networks IED activities:

---

[100]Department of Defense, Joint Publication 3-15.1, *Counter-Improvised Explosive Device Operations* (Washington, D.C: Joint Chiefs of Staff, 2012), II-1.

[101]For more see Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004); and Peter Curry, "Small Wars are Local: Questioning Assumptions about Armed Groups," In *Pirates, Terrorists and Warlords,* edited by Jeffery H. Norwitz, 156-165 (New York: Skyhorse Publishing, 2009).

[102]Marc Sageman, *Understanding Terror Networks*…, 142.

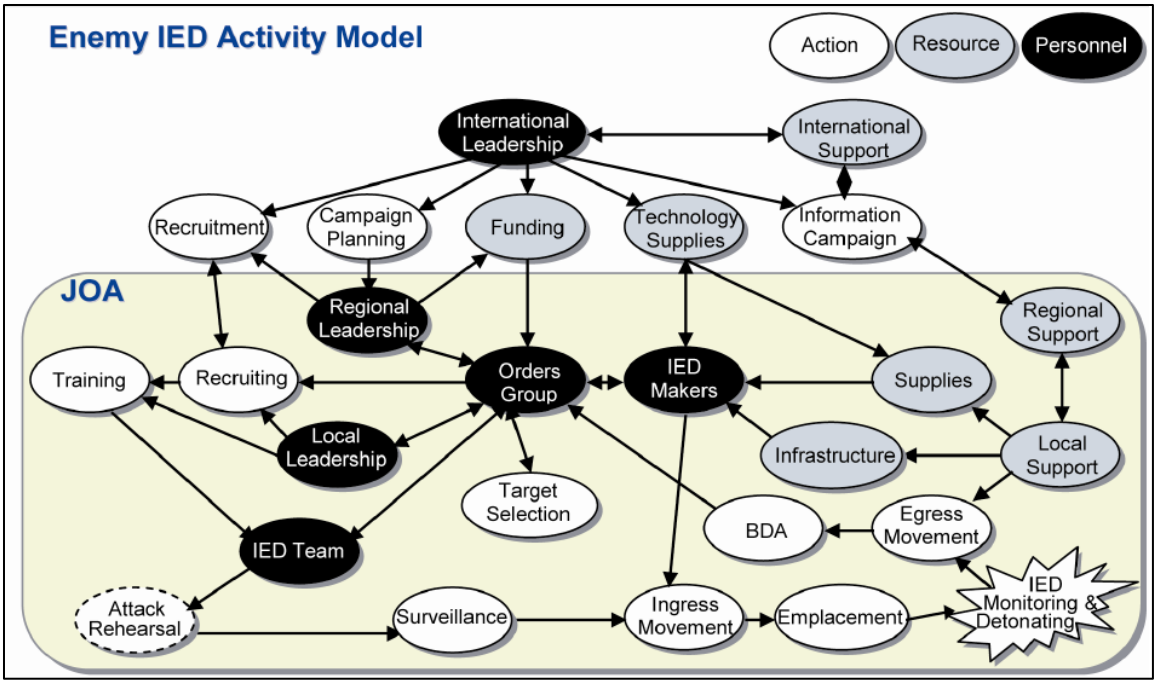


Figure 5 – Threat Network IED System

Source: Headquarters of Department of the Army, *Improvised Explosive Device Defeat*, 3-3.

This figure identifies the numerous actions performed by the threat network. As the source document notes:

> There are multiple vulnerabilities that the joint task force (JTF) commander can exploit to bring about IED defeat. By attacking or isolating one or more key actions (resources or groups of personnel), the JTF commander can prevent the effects of IEDs in a proactive manner. The challenge is to identify which nodes the JTF commander can affect and which of those has the largest payoff for IED defeat.[103]

In other words, the JTF commander needs to identify and target the critical nodes in the schematic above to effectively disrupt the network. This paper argues that the greatest effect will not be achieved within the JOA. To completely disrupt the threat network's

[103]Department of the Army, *Improvised Explosive Device Defeat*…, 3-3.

use of IEDs, the government must remove sources of financing, neutralize leadership, and reduce the ability to supply and move IED components.

Conclusion

This chapter has examined the asymmetric nature of an IED system and why it is difficult to target using military forces exclusively. Threat networks can easily acquire and smuggle IED components due to their commercial availability and their dual-nature use. This makes them cheap, easy to manufacture, and to adapt, especially since threat networks share design techniques through the internet. Providing a stand-off capability and able to defeat armour, they negate friendly forces' military strengths by avoiding direct and decisive engagements. IEDs can also be used to target a range of targets, whether military, economic, or diplomatic, inflicting casualties, destroying material and infrastructure.

Exploiting these advantages, IEDs are now the weapon of choice for a range of threat networks across the globe since they influence all instruments of national power. Friendly forces have to painstakingly clear roads and areas of IEDs, which significantly affects freedom of manoeuvre. IEDs are responsible for more military and civilian casualties than any other weapon system in Afghanistan and Iraq. To mitigate their effects, western nations have spent billions on force protection and countermeasures, with marginal impact. In terms of blood and treasure, the effects of IEDs have considerably eroded public support for the wars in Afghanistan and Iraq. For western countries, national will is the strategic centre of gravity. This is why developing C-IED strategy is fundamental in today's operational environment.

All the armour in the world and it just doesn't really matter. The vehicles get tougher but the blasts get bigger.

- Adam Day, *Legion Magazine*

CHAPTER 2 - C-IED STRATEGY

Introduction

Although history has shown that the IED is not a 21st century invention, C-IED strategy did not exist before the early 2000s. [104] There were Explosive Ordnance Disposal (EOD) and Military Search publications, but the development of C-IED doctrine is a recent endeavour.[105] Due to the increased IED threat in Iraq, Afghanistan, and the rest of the world, there has been a proliferation of C-IED publications in the last ten years. One of the first dedicated C-IED doctrines was published by the UK in 2006 as Joint Doctrine Note 5/06 *Countering Improvised Explosive Devices*.[106] Other nations followed suit; the Australian doctrine in 2007, and the US C-IED Operations Joint Publication 3.15 in 2012 and the Canadian Forces Joint Publication (CFJP) 3-15 in 2013.[107] The NATO Allied Joint Doctrine 3.15(A) was created in 2008 but was revised in 2011 based on inputs from allied nations. All these doctrines provide an in-depth analysis of the IED threat, mitigation measures, and the roles and responsibilities of various elements contributing to C-IED operations.

---

[104]Department of Defence, "Joint Doctrine Update: Joint Chiefs of Staff J7 Joint Education and Doctrine Division," *Joint Force Quarterly* 57 (April 2010): 134.

[105]EOD involves the neutralization and disposal of any type of explosive device, including unexploded ordnance (UXO) and IEDs. Military Search incorporates deliberate military operations to search for explosive devices.

[106]Department of National Defence, *Counter Improvised Explosive Devices* …, REF-1.

[107]*Ibid.*

Of note, the various doctrinal publications have a common C-IED strategy based on three lines of operations or pillars: *Defeat the Device* (DtD), *Prepare the Force* (PtF), and *Attack the Network* (AtN), with a foundation of *Understanding and Intelligence*.[108] Each line of operation has unique key operational activities: *Understand*, *Prepare*, *Protect*, *Prevent*, and *Pursue*. Figure 6 illustrates the relationship between the various pillars and the key operational activities.

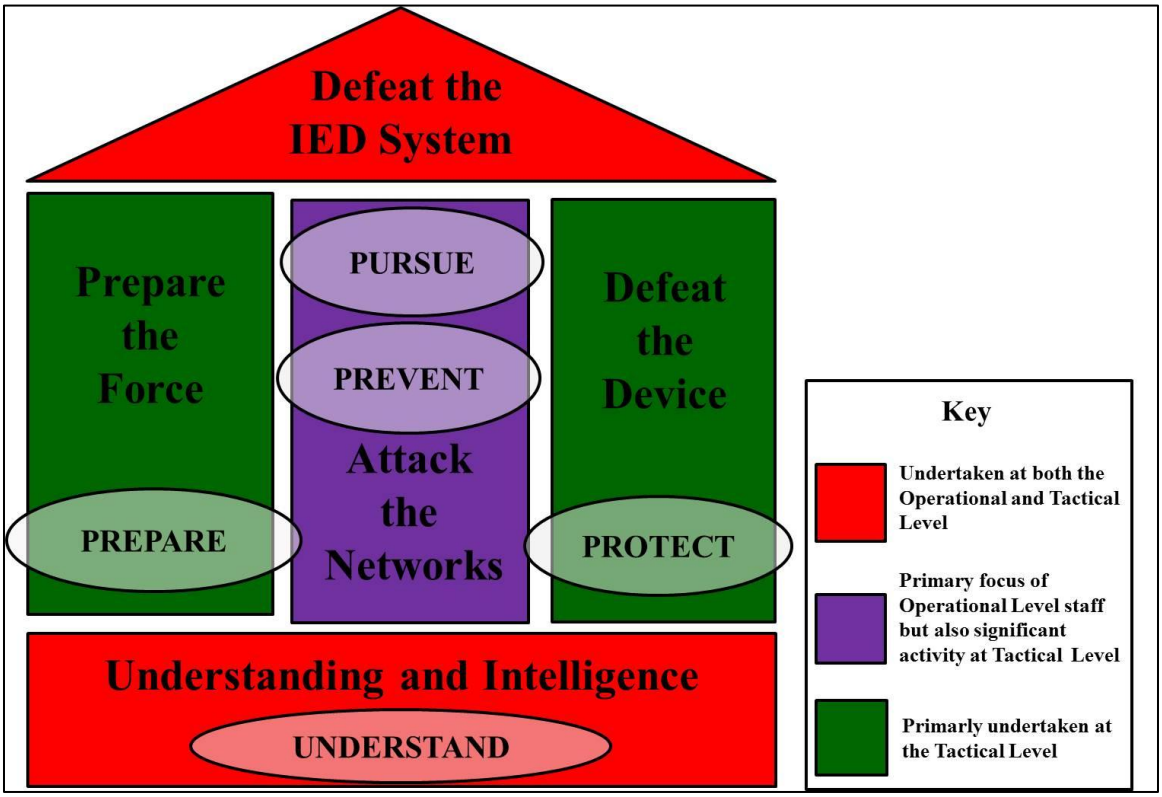


Figure 6 – C-IED Approach with Supporting Activity Pillars

Source: NATO ACT, Commanders' and Staff Handbook for Countering Improvised Explosive Devices, 7.

As this figure's legend indicates, the two lines of operations DtD and PtF are primarily military functions involving the tactical and operational level. The third line,

[108]It is noted that some national doctrinal publications use different terms, such as the US refers to "Train the Force" instead of "Prepare the Force". Yet, the three lines of operations are very similar.

AtN requires strategic, operational, and tactical resources. AtN entails a number of actions that cannot be entirely done by the military, due to the nature of IED systems and the military's inability to operate outside a designated JOA.

Consequently, latest C-IED doctrine emphasizes the importance of the Comprehensive Approach to support all three pillars, particularly AtN. For NATO, the Comprehensive Approach is an instrumental part of the C-IED strategy, highlighting "the close co-operation and co-ordination between the diplomatic, military, economic, and the information levers of power."[109] Similar terminology is present in the American, Australian, British, and Canadian publications, though some use the terms Whole of Government or Joint, Interagency, Multinational, and Public (JIMP).[110]

Regardless of the term, the approach harnesses all instruments of national power across a wide range of government departments to defeat IED systems. The major problem with C-IED doctrine does not lie with the concepts themselves, but with the way they are implemented. Specifically, C-IED doctrine is only being developed and implemented by military forces.

This chapter will examine the C-IED strategy and demonstrate why it cannot be solely performed by the military. Each line of operation will be analysed based on the five key operational activities. It will also show why the DtD and PtF lines of operations will have limited effects in disrupting an IED system and why AtN is the most effective way of defeating the IED threat. To begin this analysis, one must consider the foundation for all lines of operations: *Understanding and Intelligence*.

---

[109]NATO, *Allied Joint Doctrine For Countering Improvised Explosive Devices* …, 1-3.

[110]The differences between the terms Comprehensive Approach, JIMP and Whole of Government will be addressed in Chapter 3.

Understanding and Intelligence

To conduct the three lines of operations, friendly forces must have a common understanding of the IED threat, the operational environment, and the military capabilities and limitations. This comprehension forms the basis for the four other key operational activities as shown in Figure 6. Rather than focus solely on the enemy, *Understanding and Intelligence* entails "an understanding of significant relationships within interrelated political, military, economic, social, information, infrastructure, and other systems relevant to a specific joint operation."[111] This implies developing the comprehensive Joint Intelligence Preparation of the Operational Environment (JIPOE). It is particularly important to the C-IED strategy, since threat networks rely on human, physical, and information environments to support their IED system.

As Figure 5 illustrates, threat networks require a number of resources to facilitate IEDs. For instance, they need local support to move components, to provide intelligence on friendly force movements, and, in most cases, provide emplacers and triggermen. Therefore, friendly nations must understand the local culture and social dynamics, particularly when operating in a counterinsurgency (COIN) environment. By knowing the relationship between the local population and the threat networks, friendly forces can counter enemy activities.

---

[111]Department of Defense, Joint Publication 2-01.3, *Joint Intelligence Preparation of the Operational Environment* (Washington, D.C: Joint Chiefs of Staff, 2009), xii.

As noted in *Fixing Intel*, the primary intelligence requirement in COIN is not enemy-centric, rather population-centric.[112] Though this paper addresses COIN strategy, understanding the local population is also essential to all types of stability operations, such as counter-terrorist and counter-criminal. Appreciating the importance of population-centric intelligence requirements, western militaries have developed the concept of "human terrain".[113] Human terrain is a key factor in JIPOE since it determines how IED systems recruit locals and use criminal groups or legitimate businesses to move IED components. Yet, as it will be demonstrated in Chapter 3, the military does not have human terrain expertise, and must rely on academics to provide socio-cultural information on the local population, which further highlights military limitations in implementing C-IED strategy.

Another key element of the operational environment is the geospatial domain. To develop detailed knowledge of the terrain, friendly forces require geospatial intelligence (GEOINT) capabilities. GEOINT provides analysis on potential IED "hot-spots", smuggling routes, IED caches, and other geospatial factors. However, GEOINT organizations are national-level agencies, such as the National Geospatial-Intelligence Agency (NGA). Though formally reporting to DoD, NGA receives priorities from the Director of National Intelligence and the Under-Secretary for Defence (Intelligence),

---

[112]Michael Flynn, Matt Pottinger, and Paul Batchelor, "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan." *Voices from the Field* (Washington: Centre for a New American Security, 2010), http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf, 23.

[113]The concept of human terrain will be discussed in Chapter 3.

both strategic-level organizations.[114] In Canada and the UK, GEOINT belongs to Chief of Defence Intelligence (CDI), a strategic-level organization. In all three nations, GEOINT units provide teams to support decision-making at the strategic, operational, and tactical levels. However, the bulk of GEOINT assets reside at the strategic level. Therefore C-IED requires national reach-back support. In addition, since resources are finite, GEOINT units need to work together to foster cooperation, interoperability, and burden sharing.[115]

Friendly forces face similar challenges when gathering intelligence on threat networks operating outside the JOA. For instance, considering the activity model in Figure 5, friendly forces must identify international leadership nodes, and sources of funding and components. The identification of threat network elements outside the JOA involves Signals Intelligence (SIGINT), Human Intelligence (HUMINT), and foreign financial information. In the US, these are activities performed by the National Security Agency (NSA), the Central Intelligence Agency (CIA), and the Department of Treasury respectively, which do not report to the military. [116] In Canada, SIGINT is performed by the Communications Security Establishment Canada (CSEC), HUMINT is done by the Canadian Security Intelligence Service (CSIS), and terrorism financing and money laundering is tracked by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). CSIS and FINTRAC report to Public Safety Canada (PSC), not the

---

[114]National Geospatial-Intelligence Agency, *NGA Strategy 2013-2017* (Springfield: National Geospatial Intelligence Agency, 2012), https://www1.nga.mil/About/NGAStrategy/Documents/19639_NGA% 20Strat%20Pub_Public_Web.pdf, 6.

[115]National System Geospatial for Intelligence, Directive NSGD FM 1100, *Roles and Responsibilities of the Department of Defense (DoD) Geospatial Intelligence (GEOINT) Manager and Intelligence Community (IC) Functional Manager (FM) for GEOINT* (Fort Belvoir: National Geospatial-Intelligence Agency, 2011) http://www.gwg.nga.mil/documents/fm1100.pdf, 12.

[116]Department of Defense, Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations* (Washington, D.C: Joint Chiefs of Staff, 2012), II-12.

Department of National Defence (DND). Therefore, to access this type of intelligence, friendly forces need interagency support and information sharing.

Another crucial aspect of *Understand and Intelligence* is to identify the capabilities and limitations of friendly forces, particularly during multinational operations. Since each participating nation have varying degrees of competencies, understanding the level of readiness, equipment capabilities, and national policies are essential to work as a coalition in disrupting an IED system. Developing this common understanding requires a multinational approach, with all countries declaring their capabilities, and addressing interoperability and information exchange policies. This is particularly important for the first line of operation: *Prepare the Force*.

Prepare the Force

This line of operation is defined as "the supporting measures and activities necessary to ready a force for operations where there is the threat of an IED system."[117] PtF surrounds the key operational activity *Prepare* which creates the conditions for friendly forces to conduct offensive C-IED operations.[118] *Prepare* is primarily focused on the integration of training and education at the individual and collective levels across the coalition. Developing common TTPs, policies, and addressing interoperability are particularly important considerations for the other C-IED pillars.

Preparing forces for C-IED operations is a national responsibility. However, there are clear advantages in working together across NATO or a larger coalition. It avoids

---

[117]NATO, *Allied Joint Doctrine For Countering Improvised Explosive Devices* …, 5-1.

[118]Allied Command Transformation, *(NU) Commanders' and Staff Handbook for Countering Improvised Explosive Devices* (Norfolk: NATO, 2011), 11.

duplication of efforts, reduces costs, and ensures a common approach. This is why NATO has created a number of C-IED working groups (WG) and Centres of Excellence (COE) supporting C-IED, such as the C-IED COE in Spain, the EOD COE in Slovakia, and the Defence Against Terrorism (DAT) COE in Turkey. These centres serve many purposes as defined by NATO:

> Centres of Excellence (COEs) are nationally or multi-nationally funded institutions that train and educate leaders and specialists from NATO member and partner countries, assist in doctrine development, identify lessons learned, improve interoperability, and capabilities and test and validate concepts through experimentation. They offer recognized expertise and experience that is of benefit to the Alliance and support the transformation of NATO, while avoiding the duplication of assets, resources and capabilities already present within the NATO command structure.[119]

COEs allow the Alliance to develop a common approach to C-IED operations, exchanging lessons learned and best practices. Through COEs and WGs, C-IED Communities of Interest have been formed to share information and intelligence. These communities have created Internet portals, such as NATO's *C-IED.org* and JIEDDO's Joint Knowledge and Information Fusion Exchange (JKnife), to exchange information multi-nationally. However, they are strictly for unclassified information.

The exchange of classified intelligence can be a significant obstacle since it involves complex bureaucratic and policy hurdles, particularly across a multinational environment. Yet sharing intelligence is instrumental in achieving situational awareness across the theatre of operations. Since threat networks exploit the Internet to communicate IED design techniques, a new device can emerge in different areas, within

---

[119]NATO Multimedia Library, "NATO Centres of Excellence," last accessed 10 February 2013, http://www.nato.int/cps/en/natolive/topics_68372.htm.

and outside the JOA. Friendly forces need to adapt rapidly to these new threats. Therefore, it is crucial that friendly forces transmit classified Flash Reports rapidly across the theatre. C-IED Flash Reports are designed to "rapidly disseminate new threats and enemy TTPs by technology or region to friendly forces."[120] However, there are two main obstacles to passing on classified information: policy and interoperability.

IED-related intelligence involves a wide range of classified sources, such as HUMINT and SIGINT. Since intelligence services need to protect their sources, they establish strict policy and guidelines for sharing with other nations. For instance, the US Joint Publication 2-01 clearly articulates the policy of the United States Government (USG) for releasing intelligence to multinational partners:

> USG policy is to treat classified [intelligence] as a national security asset, which may be shared with foreign governments and international organizations only when there is a clearly defined advantage to the United States.[121]

In some instances, allied countries established intelligence-sharing agreements which allow seamless exchange, such as the Five-Eyes community[122] where SIGINT, GEOINT, and other intelligence is freely passed on. [123] However, this is not the case in NATO, where the US applies a sanitization process to release SIGINT and GEOINT.[124] Disclosing to non-government partners is more complicated as it requires a "tear line reporting" system. Tear Line completely scrubs the report down using a "write to release"

---

[120]Allied Command Transformation, *Commanders' and Staff Handbook …*, A-5.
[121]Department of Defense, *Joint and National Intelligence Support…*, II-12.
[122]The Five-Eyes intelligence community consists of the Australia, Canada, New Zealand, the United States, and the United Kingdom.
[123]Department of Defense, *Joint and National Intelligence Support…*, II-26.
[124]*Ibid.*, II-25.

approach where only the basic essential information remains.[125] This report can then be disclosed to IOs, NGOs, and other key stakeholders. However, it does not include information that would allow other partners to fully understand the implications of the intelligence and make their own analysis. Though C-IED Flash and Tear Line reports do save lives, they do not promote complete situational awareness across the coalition. This limits other nations' abilities to contribute to C-IED efforts.[126]

The other major obstacle to *Prepare* is interoperability. During combined C-IED operations each nation must be able to de-conflict their equipment with those of other nations. For instance, friendly forces deploy national electronic countermeasures (ECM), such as Counter Remote-Controlled IED Electronic Warfare (CREW) jammers. CREW systems work in different bandwidths of the electro-magnetic spectrum (EMS).[127] This can cause signal interference and jam friendly communications. To avoid signal fratricide, Electronic Warfare (EW) units must cooperate and de-conflict the EMS.[128] It is also the case when military forces operate with police agencies, NGOs, and IOs. These organizations use commercial communications equipment that can fall within the EMS jammed by CREW systems. Therefore, all elements must collaborate to de-conflict the EMS to avoid system interference.

Interoperability also involves common databases, terminology, and Information Technology (IT) standards to ensure that friendly forces can freely exchange information and intelligence. Since each nation has its own classified networks, there are significant

---

[125]Department of Defense, *Joint and National Intelligence Support*…, II-25.
[126]Chapter 3 will address methods to improve classified intelligence sharing.
[127]Department of Defense, *Improvised Explosive Device Operations*…, V-10.
[128]Joe Gould, "Electronic warfare is more than jamming IEDs," *Defence News*, 11 October 2011, http://blogs.defensenews.com/ausa/2011/10/11/electronic-warfare-is-more-than-jamming-ieds/.

hurdles in achieving connectivity across the coalition.[129] Within the Five-Eyes community, IED-related intelligence can be easily exchanged using the classified network STONEGHOST.[130] NATO has the Battlefield Information Collection and Exploitation System (BICES), GRIFFIN, and CRONOS, where IED-related intelligence is released.[131] It is not always the case in a broader coalition. As a result, friendly forces need to create mission-specific classified networks to allow other nations to access intelligence, such as in Afghanistan where a mission secret network connects US Central Command, NATO, and non-NATO nations participating in ISAF.[132] However, the ISAF Mission Secret Network is only available in the theatre of operations and a few locations outside the JOA. Since it does not connect to national systems, this network architecture creates intelligence stovepipes. Nations have to manually transfer data from one network to another. To address this problem, nations have to find ways to improve connectivity and maintain the latest common operating picture with regards to the IED threat.

A third major interoperability hurdle is having common databases, particularly biometric and forensic.[133] Having multiple databases based on national systems creates data exchange challenges. Terminology is another issue that causes problems in the C-IED community. The proliferation of terms causes issues in trying to develop sources. Though NATO has a glossary of terms and definitions (AAP-6), it is difficult to maintain

---

[129]Gerald Christman and Mark Postal, "Coalition Interoperability: a Modeled Approach," last accessed 18 February 2013, http://www.dodccrp.org/events/11th_ICCRTS/html/papers/003.pdf, 5.

[130]Department of Defense, *Joint and National Intelligence Support*…, II-26.

[131]*Ibid.*

[132]Gerald Christman and Mark Postal, "Coalition Interoperability…, 3.

[133]NATO Bi-Strategic Commands, *NATO BI-SC Counter-Improvised Explosive Device (C-IED) Campaign Plan* (NATO SHAPE: file SH/OPI/OSP/JOP/12-300265/5000/TXX-0077/TT-8394/Ser/NS, 6 November 2012), 22.

a common terminology database due to the improvised nature of IEDs. In an effort to standardize IED terms, the EOD COE has compiled a database of 538 EOD and IED-related terms.[134] Yet, the nature of the components poses a problem. For instance, the database has defined a vehicle borne IED (VBIED) and a remote control IED (RCIED). However, if threat networks use a remote control to detonate a VBIED, friendly forces may categorize it as one or the other since there is no entry for a RC-VBIED. Though sounding trivial, it creates problems when analyzing patterns and statistics.

An example of this issue is illustrated in Table 1. According to the National Counterterrorism Center (NCTC), there were 3,746 IEDs in 2011.

Table 1 – Terrorist Attacks in 2011 by Weapon Type

Weapon	Attacks	Dead	Wounded
Explosive	3,541	4,732	13,148
Fake device	3	0	4
Firearm	3,712	5,584	5,415
Firebomb/Incendiary	615	338	461
Grenade	358	357	1,300
IED	3,746	6,354	18,537
Landmine	279	484	584
Letter Bomb	9	2	14
Missile/Rocket	392	144	592
Mortar/Artillery	306	910	1,777
Other	48	83	172
Primitive	325	335	768
RPG	128	289	414
Toxic	7	8	149
Unknown	1,165	783	507
Vehicle bomb	351	2,100	6,979
Total	**14,985**	**22,503**	**50,821**

Source: National Counterterrorism Center, *Worldwide Incident Tracking System Database 2011*.

[134]Explosive Ordnance Disposal Centre of Excellence, *EOD and IED Terminology Database* (Trenčín: EOD COE, 2012), https://www.eodcoe.org/data_web/editor_data/file/terminology%20posledne.pdf.

In this table, although surpassing any other type of weapon, IEDs only represent 25% of the total terrorist attacks.[135] However, the table also includes "explosives", "firebombs", "landmine", "letter bomb", and "vehicle bomb". Considering the definition of an IED in Chapter 1, these should be also included under "IEDs", which increases the number of IEDs to 8,541, or 57% of all types of attacks. These statistics are important, especially when trying to gain support from other government agencies, multinational partners, and other key stakeholders. This is why interoperability through common databases must be addressed throughout the coalition.

Prepare does not just involve NATO or coalition forces. In many conflicts, security sector reform (SSR) is a key element to friendly forces' mission since it is an integral part of the "exit strategy". It involves rebuilding and reforming indigenous security forces to be competent, effective, and responsible.[136] Reform national security involves a wide range of forces, such as military, police, national intelligence, and border units. As it will be discussed in Chapter 3, SSR requires a number of foreign national agencies training their local counterparts. Consequently, non-military friendly agencies must also be prepared to operate in a high IED threats environment since threat networks often perceived them to be "soft targets". Such is the case in Afghanistan where the Afghan National Police (ANP) units are the primary target of IEDs.[137]

---

[135]National Counterterrorism Center, *Worldwide Incident Tracking System Database 2011* (Washington, DC: Office of the Director of National Intelligence, 2012), http://wits.nctc.gov/.

[136]Government of Canada, *Canada's Engagement in Afghanistan - Fourteenth and Final Report to Parliament* (Ottawa: Library and Archives Canada, 2012), 8.

[137]United Nations Assistance Mission in Afghanistan, *Afghanistan Annual Report 2010: Protection of Civilians In Armed Conflict* (Kabul: UNAMA, 2011), http://unama.unmissions.org/Portals/UNAMA/human%20rights/March%20PoC%20Annual%20Report%20Final.pdf, 4.

Therefore, while mentoring and training the ANP, friendly police forces must have the same C-IED training competencies as military units. Though each agency could run its own C-IED training, it duplicates efforts, and it increases the risks of setting different standards. To facilitate the most cost effective training, the Comprehensive Approach must be applied to this line of operation. Training is one of the many examples that demonstrate the importance of multinational and interagency support. Addressing interoperability and training enables the next line of operation: *Defeat the Device*.

Defeat the Device

The line of operation DtD is principally a series of proactive and reactive activities to detect and neutralize emplaced IEDs and to mitigate their effects.[138] As per Figure 6, DtD encompasses the key operational activity *Protect*.[139] This activity is perhaps the easiest line of operation to understand, since it involves physical measures such as detection systems, C-IED drills, armoured protection, and jammers. Detection systems include intelligence, reconnaissance and surveillance (ISR) sensors, such as UAVs, ground monitoring stations, and reconnaissance vehicles. They detect IED emplacement as well as other nodes in an IED system, such as smuggling routes and IED caches. IED detection systems are specialized route clearance packages (RCPs), such as the Husky mine detection vehicle, EOD robots, ground-penetrating radar, and metal

---

[138]NATO, *Allied Joint Doctrine For Countering Improvised Explosive Devices*…, 1-8

[139]*Protect* is the new NATO key operational activity (KOA). It incorporates the former KOAs *Mitigate*, *Detect*, and *Neutralize*. Some nations, such as Canada and the United States, still use the former KOAs as part of DtD. For the purpose of this thesis, *Protect* includes *Mitigate*, *Detect*, and *Neutralize*.

detectors.[140] However, not all nations can afford ISR and RCPs. To address this problem, the NATO Secretary-General created the SMART Defence initiative with a goal to "promote multinational cooperation in defense spending".[141] Through this strategy, nations have agreed to a common C-IED Material Road Map where 19 initiatives will undergo joint research and development, trialing, acquisition, and fielding.[142] Since nations share the burden, individual nations will not have to buy the complete inventory of detection systems. One nation could provide RCPs while another provides UAVs. This cost-sharing multinational approach is instrumental to avoid duplication of effort, ensure interoperability, and ultimately, strengthen the Alliance.

Another element of DtD is force protection measures which includes personal protection equipment (PPE), infrastructure fortification, and vehicle armour. The quest to best protect soldiers against IEDs has been the source of many debates. When JIEDDO was stood up in January 2006, it focused primarily on finding technical solutions to defeating IEDs, such as fielding up-armoured vehicles and ECM.[143] The problem associated with being equipment-centric was thoroughly highlighted in a US Joint Forces Staff College paper:

---

[140]RCPs are also called Expedient Route Opening Capability (EROC). EROC incorporates three types of vehicles: a mine-detection vehicle (Husky), a disposal vehicle (Buffalo), and an EOD team carrier (Cougar). For more details, see General Dynamics Land System, "MRAP Family," last accessed on 24 February 2013, http://www.gdls.com/index.php/products/mrap-family.

[141]NATO Multimedia Library, "Countering Improvised Explosive Devices," last accessed 17 February 2013, http://www.nato.int/cps/en/natolive/topics_72809.htm.

[142]*Ibid.*

[143]Vincent Clark, "The Future of JIEDDO – The Global C-IED Synchronizer," (thesis, Naval War College, 2008) http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA494284, 11.

> Additionally, not only is JIEDDO a large bureaucracy, it is still built around a technical solution approach focused on research and development, testing, and fielding the elusive "silver bullet" to defeat IEDs. By doing so, the organization overly relies on technology to defeat an adaptive enemy who quickly learns how to overcome our latest countermeasures.[144]

In its first year alone, JIEDDO spent $1.2 billion for 70 equipment initiatives, mainly on CREW jammers, vehicle armour, and detection devices.[145] Initially, this equipment was successful in reducing the number of IED attacks in Iraq and Afghanistan through an increased detection rate. One particular project that was deemed most successful was working with military dogs. In the first four months of their deployment in Afghanistan, the 170 explosive-sniffing dogs found over 400 IEDs in Sangin Valley.[146] Additional UAVs were also deployed, increasing the number of airborne surveillance patrols from nine, in 2008, to twenty-five, in 2010.[147] Figure 7 illustrates the impact of this new technology in Afghanistan: the number of IEDs found by friendly forces doubled the number of IED attacks (ineffective and effective) in April 2009.

---

[144]Richard Ellis *et al.*, "JIEDDO: Tactical Successes Mired in Organizational Chaos…", 6.

[145]William G. Adamson, "An Asymmetric Threat Invokes Strategic Leader Initiative: the Joint Improvised Explosive Device Defeat Organization," (research project, Industrial College of the Armed Forces, 2007), http://www.scribd.com/doc/26736694/Adamson-Final-Icaf-Research-Paper-Jieddo, 30.

[146]Tony Perry, "Afghanistan's most loyal troops," *Los Angeles Times*, 8 February 2011, http://articles.latimes.com/2011/feb/08/nation/la-na-war-dogs-20110208.

[147]Nolin, *Countering the Afghan Insurgency*…, 14.

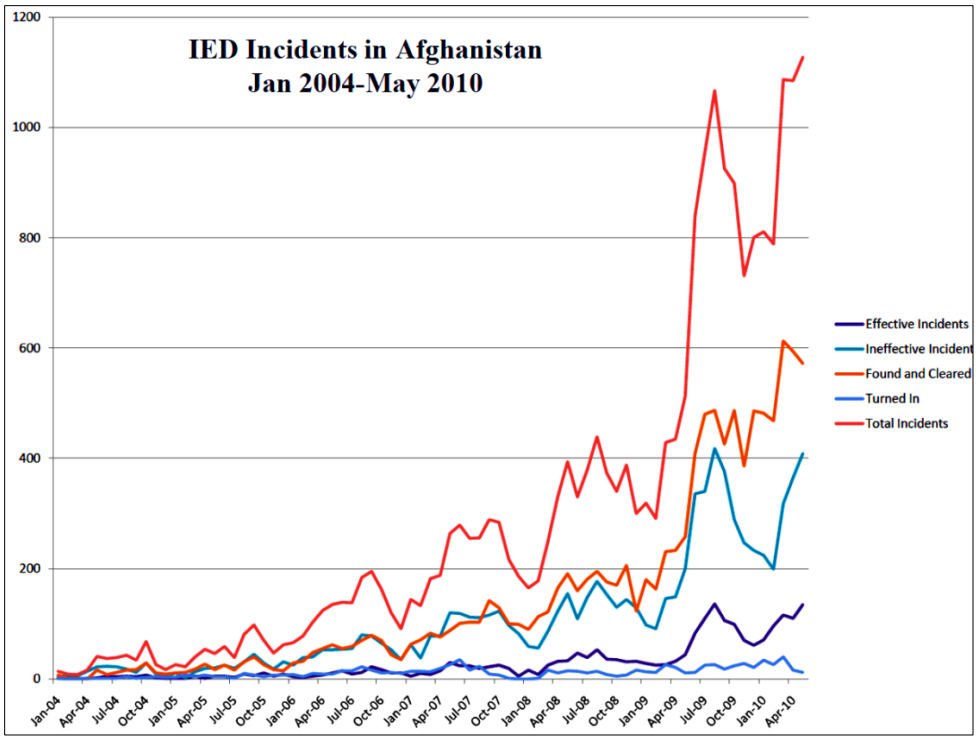


Figure 7 - IED Incidents in Afghanistan (Jan 2004-May 2010)

Source: Cordesman *et al.*, "IED Metrics for Afghanistan," 5.

However, despite spending 80% of its annual budget on equipment acquisition, JIEDDO's initiatives were ineffective at reducing the threat of IEDs in the medium and long-term. [148] As Figure 7 shows, the overall number of IED attacks increased by 500% despite JIEDDO's efforts. This led to criticism from inside the DoD, including the commander of CENTCOM, General Abizaid, who argued that high-technology sensing equipment was not the solution to reduce IED attacks.[149]

One of the reasons of their failure is directly tied to the nature of IEDs. As highlighted in Chapter 1, threat networks can rapidly adapt the device to counter new

---

[148]Ackerman, "Improvised Explosive Devices: A Multifaceted Threat…"

[149]Bryan Bender, "Panel on Iraq bombings grows to $3b effort Critics say it has been ineffective," *The Boston Globe*, 25 June 2006, http://www.boston.com/news/world/middleeast/articles/2006/06/25/panel_on_iraq_bombings_grows_to_3b_effort/.

friendly TTPs. For instance, when friendly forces effectively countered RCIEDs using CREW jammers in Afghanistan, insurgents quickly changed tactics. They used long command wires attached to radio triggers so that the signal would be outside the jammer's protective "bubble".[150] Consequently, jammers no longer worked since the IED receivers were hundreds of meters from the bomb.

Insurgents also increased their use of victim-operated IEDs for which jammers have no effect.[151] Despite $2.3 billion spent on jammers, threat networks still effectively attacked US forces.[152] The threat network's ability to adapt to friendly countermeasures highlights one of the limitations of the DtD line of operation.

Another limitation is instigated from the attempt to protect soldiers using up-armoured vehicles. Since 2003, the US has spent over $47 billion on the acquisition of Mine-Resistant Armoured-Protected (MRAP) vehicles.[153] The heavily-armoured vehicles incorporate a raised v-shaped hull which deflects the explosive blast.[154] Weighing up to 22 tonnes, its sizeable mass also protects its passengers against IEDs.[155] In one academic paper, it was noted that MRAPs are "up to 400% more effective than [other vehicles] and

---

[150]Nolin, *Countering the Afghan Insurgency*…,6.

[151]*Ibid.*

[152]House of Representatives, *The Joint Improvised Explosive Device Defeat Organization*…, 14.

[153]International Institute for Strategic Studies. "IEDs: The Home-Made Bombs that Changed Modern War." *Strategic Comments* 18, no. 24 (August 2012): 2. http://www.iiss.org/publications/strategic-comments/past-issues/volume-18-2012/.

[154]Andrew Krepinevich and Dakota Wood, *Of IEDs and MRAPs: Force Protection in Complex Irregular Operations* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2007), http://www.csbaonline.org/publications/2007/10/of-ieds-and-mraps-force-protection-in-complex-irregular-operations/, 8.

[155]*Ibid.*

can cut casualties by two-thirds."[156] The deployment of MRAPs had an impact on the effectiveness of IEDs in Afghanistan, particularly in the US surge in 2009. Figure 7 illustrates the reduction in the successful IEDs between July 2009 and January 2010 (dark blue line).

A number of DoD sources have argued that the arrival of MRAPs significantly contributed to this success rate. For instance, US Deputy Secretary of Defence, Ashton Carter, and the DoD Director of Operational Test and Evaluation, Michael Gilmore, argued that MRAPs helped saved thousands of lives by reducing the effectiveness of IEDs in 2009 to 2010.[157] Dr Chris Rohlfs and Dr Ryan Sullivan disagree with these findings. In their *Foreign Affairs* article they stated:

> The Defense Department says that its $45 billion MRAP program saved the lives of 40,000 troops in Iraq and Afghanistan. But according to a study of restricted Pentagon data, that number is a miscalculation, and much less expensive equipment would be just as effective.[158]

Though this debate continues in a number of articles and academic papers, one fact remains. Figure 7 shows that in July 2010, in spite of the deployment of MRAPs in Afghanistan, the number of successful IED attacks reached the same level of July 2009.

Though it is clear that MRAPs mitigate the IED blast and save lives, they are not a "silver bullet" to defeat IEDs. They do provide considerable force protection, but they also have their limitations. Firstly, as highlighted in the epigraph of this chapter, threat

---

[156]Christopher J. Lamb, Matthew J. Schmidt, and Berit G. Fitzsimmons, "MRAPs, Irregular Warfare, and Pentagon Reform," Institute for National Strategic Studies, National Defense University, 2009, http://usacac.army.mil/cac2/cgsc/sams/media/MRAPs.pdf, 14.

[157]Ashton B. Carter and J. Michael Gilmore, "Running the Numbers on MRAPs: Reliable Data Proves the Vehicles are Worth the Money," *Foreign Affairs*, 9 October 2012, http://www.foreignaffairs.com/articles/138172/ashton-b-carter-and-j-michael-gilmore/running-the-numbers-on-mraps?page=show.

[158]Chris Rohlfs and Ryan Sullivan, "The MRAP Boondoggle: Why the $600,000 Vehicles Aren't Worth the Money," *Foreign Affairs*, 26 July 2012, http://www.foreignaffairs.com/ articles/137800/chris-rohlfs-and-ryan-sullivan/the-mrap-boondoggle.

networks can always build a bigger IED to defeat armoured protection. While deploying an IED with enough explosive force to destroy a MRAP limits the number of IEDs that can be built, destroying one of these vehicles scores considerable points for the enemy.

Secondly, since threat networks can easily adapt to new friendly forces TTPs, they can shift their focus to other "softer" targets. By doing so, they maintain the initiative. In Afghanistan, when the US and other nations employed MRAPs, insurgents shifted their efforts from targeting military convoys on main supply routes to dismounted ISAF and Afghan National Security Forces (ANSF) personnel in urban and rural areas.[159] As seen in both figures 1 and 7, the overall number of IED incidents continued to increase despite the arrival of MRAPs.

Thirdly, operating from highly armoured and physically imposing vehicles can have negative consequences, particularly in a COIN environment. Dr Andrew Krepinevich and Dakota Wood highlight a number of these consequences:

> Successful counterinsurgency (COIN) operations, in particular, require close contact with the local population to provide them with security and to develop a working knowledge of the local environment that, together, produces the intelligence necessary to defeat an insurgent enemy force. This approach is similar to law enforcement techniques that emphasize policemen "walking the beat" in a neighborhood as opposed to merely driving through it in a squad car. Simply put, commanders may have to risk some casualties in the near term, by having their troops dismount, in order to develop the secure environment that yields the intelligence that will reduce the insurgent threat—and US casualties—over the longer term. Given this approach, which is consistent with the military's new COIN doctrine, the MRAP—at least in this situation—may send the wrong message to troops in the field.[160]

---

[159]Gareth Evans, "Going to War Against the IED," *Army Technology*, 7 May 2010, http://www.army-technology.com/features/feature84291.

[160]Krepinevich and Wood, *Of IEDs and MRAPs*…, x.

Though this paper agrees with this assessment, MRAPs remain important to C-IED operations since they are instrumental in high-risk missions, such as protecting convoys, supporting EOD forces, opening routes, and clearing high risk areas. A large number of MRAPs must be available to coalition forces since they provide the greatest level of protection, particularly to transport OGD personnel. Therefore, MRAPs provide the best platform to protect unity of effort in a multinational and interagency approach.

However, MRAPs are not the most appropriate platform for all friendly forces, particularly in stability operations. The paper *Fixing Intel* reinforces this argument by noting that American units in Afghanistan became successful in gaining ground against the Taliban when "they began sweeping across the district *on foot* [emphasis added] establishing nearly two dozen patrol bases in villages and cornfields along the way."[161] This could not have been done if US forces had simply rolled across Afghanistan in large armored vehicles that cannot circulate in most villages due to their size. Therefore, an effective C-IED strategy in a COIN environment requires troops operating amongst the population and gaining their trust. Once this trust is established, locals will be more inclined to provide valuable intelligence on the IED system operating in their areas. This strategy leads to the third and last line of operation: *Attack the Network*.

Attack the Network

According to NATO AJP 3.15, "AtN consists of largely offensive and proactive activities, driven by intelligence that may go beyond the theatre of operations, designed

---

[161]Flynn *et al.*, "Fixing Intel…", 13.

to disrupt the networks of the adversary's IED System."[162] The Comprehensive Approach is instrumental to this line of operation since it involves two key operational activities: *Pursue* and *Prevent*.[163] These actions rely heavily on non-military effects, in particular, intelligence and law enforcement. In addition, this line of operation is considered the most effective pillar in the overall C-IED strategy since it focuses on "Left of Boom" by directly targeting the critical vulnerabilities of an IED system.[164]

Prevent encompasses activities designed to deter involvement from elements that support an IED system[165] It includes reducing local population support to threat networks and mitigating the IEDs' strategic effects by incorporating two main actions: predict and mitigate. The first is linked to the basis of the C-IED strategy as illustrated in Figure 6, *Understanding* and *Intelligence*. By understanding the IED system, friendly forces are able to predict how the system operates. For example, through intelligence and analysis, it is possible to anticipate an IED support structure and identify their critical capabilities (CCs), which leads to critical requirements (CRs). Figure 8 provides a list of CCs (top line of boxes in this figure) and CRs (subsequent boxes). Through prediction, friendly forces can task ISR assets to detect and confirm the source of these requirements.

---

[162]NATO, *Allied Joint Doctrine For Countering Improvised Explosive Devices* …, 1-7.

[163]*Prevent* is the new NATO key operational activity (KOA). It incorporates the former KOAs *Predict* and *Mitigate*. Some nations, such as Canada and the United States, still use the former KOAs as part of AtN. For the purpose of this thesis, *Prevent* includes *Predict* and *Mitigate*.

[164]NATO, *Allied Joint Doctrine For Countering Improvised Explosive Devices* …, 1-7.

[165]Allied Command Transformation, *Commanders' and Staff Handbook*…, 10.

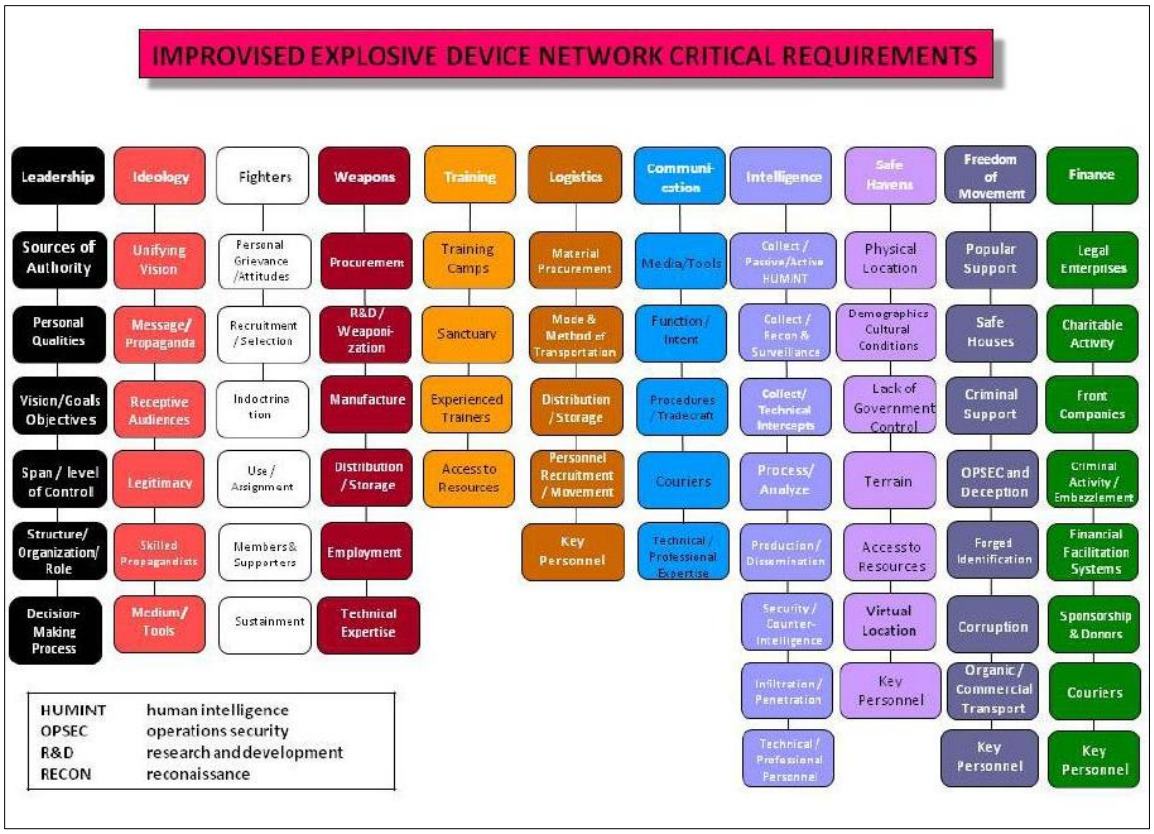


Figure 8 – IED Critical Capabilities and Critical Requirements

Source: Department of Defence, Commander's Handbook to Attack the Network Operations, II-6.

Once friendly forces detect these CRs, they can identify the ones that are vulnerable to targeting. These are the critical vulnerabilities (CVs) of an IED system. To attack CVs, many agencies and OGDs must be involved. For instance, the source of IED financing (front companies, charitable organizations, and donors) could be operating outside the jurisdiction of Western national agencies. To disrupt the money trail, national financial intelligence units (FIU) and law enforcement agencies need to cooperate with other national agencies to counter money laundering.

Prevent also means interrupting the supply of IED components, which are commonly available from normal commercial sources. Whereas it is difficult to track every component bought through legitimate companies, law enforcement and intelligence

agencies can trace large volume acquisitions of a particular component that could be used in IEDs, such as the purchase of thousands of remote-control devices by a dubious organization. A parallel can be drawn with the production of methamphetamine. In 1996 the Methamphetamine Control Act controlled the selling of over-the-counter ephedrine which is used in the product of methamphetamine.[166] As a result, no one can procure or import large quantities of cold-medicine such as Sudafed without attracting attention. A similar approach could be applied if C-IED organizations provide border and law enforcement agencies with a list of potential IED components, such as circuit boards and cell phones. If large quantities are found, the police and border services can further investigate and seize the material if doubts exist to their intended use.

Prevent also predicts how IEDs will evolve throughout the campaign once friendly forces deploy countermeasures. Since threat networks distribute IED-building techniques through the Internet, they share "best practices" to defeat friendly countermeasures. Consequently, friendly forces must be proactive to shut down these websites using Computer Network Activities (CNA) by using national SIGINT agencies or cyber task forces. Friendly forces must also develop new TTPs to meet the emerging threat. Linked to PtF, this requires sharing technical intelligence across the coalition among military and non-military elements. It is understood that friendly forces will not be able to completely disrupt the IED system and some IEDs will still be deployed. Therefore, friendly forces have to mitigate the effects of IEDs, particularly in the information realm. This prevention measure involves a number of activities, principally

---

[166]Carlos Dobkin and Nancy Nicosia, "The War on Drugs: Methamphetamine, Public Health and Crime", *American Economic Review* 99, no. 1 (March 2009): 324-349, http://www.aeaweb.org/articles.php?doi=10.1257/aer.99.1.324

using Information Operations. According to AJP 3.15(A), Information Operations includes a range of disciplines useful to AtN.[167]

One of these disciplines is "Posture, Presence, and Profile", which is tied to force protection measures. If the posture and profile is aggressive, robust, and focused on armoured protection, then the locals will perceive the situation is deteriorating. Hence, to gain the support of the local population, friendly forces should strive to adjust their posture, presence and profile to "create a powerful perception of improving normality or a determination to carry-on which, in turn, reduces the threat."[168] By gaining local support, friendly forces deny the threat networks many critical requirements, such as a base for recruitment, safe houses, and legitimacy.

Another discipline of Information Operations that gains local support is proactive communications through media and psychological operations. NATO C-IED doctrine stresses the need to "be first in the news to pre-empt adversary propaganda."[169] An example of the importance of getting the friendly force message out early occurred in Afghanistan in 2008 when a suicide car bomb killed 14 primary school children.[170] The Taliban claimed responsibility, stating that they targeted a tribal meeting. However, ISAF immediately released photos showing that the suicide bomber was clearly able to see children near the vehicle. An ISAF spokesperson stated "[it was proof that] the Afghan

---

[167]NATO, *Allied Joint Doctrine For Countering Improvised Explosive Devices* …, 3-6
[168]*Ibid.*, 3-7.
[169]*Ibid.*, 3-6.
[170]Cable News Network, "Afghan car bomb kills 14 children," *CNN*, December 28, 2008, last accessed 7 January 2013, http://www.cnn.com/2008/WORLD/asiapcf/12/28/afghan.carbomb/index.html.

militants are not interested in the welfare nor benefit of the Afghan people."[171] This example highlights the importance of Information Operations in reducing local support to threat networks. Information Operations should also be used to inform the population back home to mitigate the strategic effects of IEDs and prevent the loss of public support. By communicating friendly successes on the three lines of operations, the home front develops a better understanding of the long-term strategy in defeating IEDs. Recently, JIEDDO and other C-IED task forces have actively publicized their efforts through media articles, academic papers, and government publications.

The military cannot be the only element publicizing the C-IED strategy. National governments must also understand and own this process. However, it seems that politicians are primarily focused on announcing force protection equipment acquisition, perhaps because it is tangible and easily understood by the electorate. Nonetheless, politicians must understand the importance of all three lines of operations, particularly the need to disrupt an IED system using the final activity: *Pursue*.

One action that is well understood by national governments is killing insurgents. The media frequently report the death of insurgents, particularly those planting IEDs.[172] Yet, *Pursue* is not just a strategy of "whack-a-mole" where insurgents are killed using armed UAVs and airstrikes. In fact, this approach can be counter-productive for a number of reasons. Chapter 1 has demonstrated that triggermen and emplacers are often people with no real ties to threat network, either recruited locally through financial gain or coercion. Therefore, eliminating the lower levels of an IED system does not create long-

[171]Saeed Shah, "Suicide car bomb in Afghanistan kills 14 primary school children," *The Guardian,* 28 December 2008, http://www.guardian.co.uk/world/2008/dec/28/suicide-car-bomb-attack-afghanistan.

[172]Nolin, *Countering the Afghan Insurgency*…, 14.

term effects. In addition, there is an inherent risk that the suspected IED emplacement team could be a group of civilians, such as farmers digging irrigation ditches near roads. It occasionally happened in Afghanistan, which significantly eroded Afghan support to ISAF.[173]

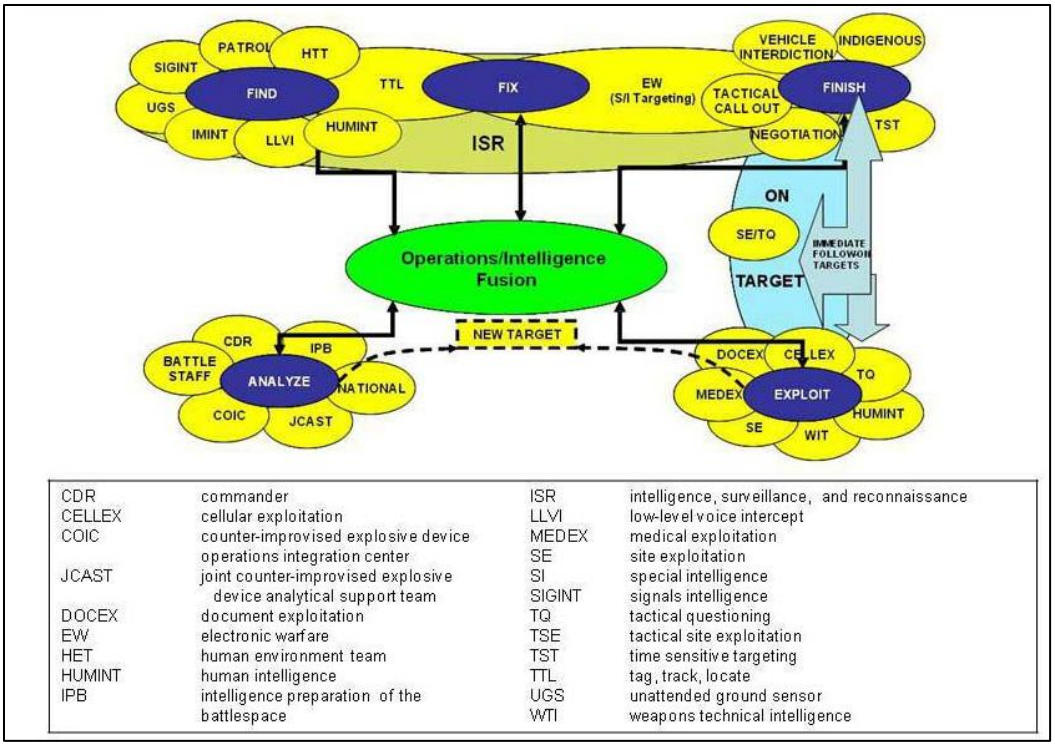
To effectively disrupt an IED system, the *Pursue* strategy must focus on middle and top-level IED facilitators, such as financiers, suppliers, and builders. This involves a process called *Find, Fix, Finish, Exploitation, Analyze* and *Disseminate* (F3EAD).[174] F3EAD is a term used by most NATO nations for time-sensitive targeting, involving both kinetic and non-kinetic means.[175] Accomplishing F3EAD requires more than military forces, especially since many facilitators operate outside the JOA. Directly targeting the IED systems requires a number of intelligence, law enforcement, diplomatic, and judicial organizations to play their part in the F3EAD process. Figure 9 shows this cycle and how national agencies contribute to it.

---

[173]Joshua Foust, *Five Lessons We Should Have Learned in Afghanistan* (Washington, D.C: American Security Project, 2012), http://americansecurityproject.org/ASP%20Reports/Ref%200066%20-%20Five%20Lessons%20We%20Should%20Have%20Learnt%20In%20Afghanistan.pdf, 5.

[174]Department of Defense, *Counter-Improvised Explosive Device Operations*…, IV-9.

[175]F3EAD is a term used by Canada and the US in their C-IED publications. NATO C-IED doctrine 3.15(A) uses the term F3EA where *Disseminate* is part of the *Exploitation* phase.



CDR	commander	ISR	intelligence, surveillance, and reconnaissance
CELLEX	cellular exploitation	LLVI	low-level voice intercept
COIC	counter-improvised explosive device operations integration center	MEDEX	medical exploitation
		SE	site exploitation
JCAST	joint counter-improvised explosive device analytical support team	SI	special intelligence
		SIGINT	signals intelligence
DOCEX	document exploitation	TQ	tactical questioning
EW	electronic warfare	TSE	tactical site exploitation
HET	human environment team	TST	time sensitive targeting
HUMINT	human intelligence	TTL	tag, track, locate
IPB	intelligence preparation of the battlespace	UGS	unattended ground sensor
		WTI	weapons technical intelligence

Figure 9 - *Find-Fix-Finish-Exploit-Analyze-Disseminate* Cycle

Source: Department of Defence, Commander's Handbook to Attack the Network Operations, III-13.

The F3EAD process requires a series of actions. The first step to find an IED facilitator requires some form of evidence that proves that a particular target is involved in the IED system. The key to this evidence is the exploitation of IED components. Exploitation is defined by NATO as: "the systematic collection and processing of information and dissemination of intelligence obtained as a result of tactical questioning, interrogation and the extraction of data from recovered materiel."[176] There are three levels of exploitation: field (Level 1), theatre (Level 2), and out-of-theatre / national (Level 3).[177]

[176]NATO, *Allied Joint Doctrine For Countering Improvised Explosive Devices*…, 2-9.
[177]NATO, *Allied Joint Doctrine For Countering Improvised Explosive Devices*…, 2-14.

Level 1 exploitation is typically performed by weapon intelligence teams (WITs) or other troops collecting IED parts in a forensic method. Level 2 is normally conducted at a Combined Explosive eXploitation Centre (CEXC) manned by joint and multinational EOD and law enforcement agencies, such as the FBI, the Royal Canadian Mounted Police (RCMP), and/or the British Metropolitan Police.[178] Level 3 is performed by national explosive forensic laboratories, such as the FBI's Terrorist Explosive Device Analytical Center (TEDAC), RCMP's Canadian Bomb Data Centre (CBDC), or the UK Forensic Explosives Laboratory (FEL). Chapter 3 will examine how these various levels of exploitation must cooperate under the Comprehensive Approach in order to maximize efficiency and support the overall C-IED strategy.

By being able to recover bomb parts, WITs develop forensic and biometric intelligence (FABINT), and technical intelligence (TECHINT).[179] FABINT includes DNA, fingerprints, and other forensic data found on IED components. DNA and fingerprints could be from a number of IED facilitators, like suppliers, builders, and emplacers. TECHINT provides information on the device's technical characteristic that can provide a *Modus Operandi* (MO) specific to a bomb maker. By merging FABINT and TECHINT into a database, friendly forces can identify patterns and supply sources. However, since threat networks operate inside and outside the JOA, military, law enforcement, and intelligence agencies need to have one single database if they are to effectively track IED builders and other facilitators.

---

[178]Department of Defense, *Counter-Improvised Explosive Device Operations*…, V-6.
[179]NATO, *Allied Joint Doctrine For Countering Improvised Explosive Devices* …, 2-10.

The second step of *Find* is to identify the IED facilitator's location. It requires national intelligence agencies that provide SIGINT, HUMINT, and GEOINT capabilities. Once threat nodes are detected, these agencies must coordinate with operational and tactical units to positively identify IED facilitators. To accomplish the *Fix*, ISR assets ensure constant coverage to avoid targets disappearing. It also determines collateral damage reducing the risk of civilian casualties. If the target is outside the JOA, then diplomatic and law enforcement agencies liaise with their local counterparts, unless covert action is envisaged.

Once the target's location is confirmed and collateral damage is acceptable, friendly forces can launch direct action to *Finish* the target. This can involve a range of forces, such as conventional military units, Special Forces, or law enforcement agencies. Depending on the situation, it could be a combined effort involving Western and host nation forces. Ideally, the target is captured and questioned. This may lead to other facilitators which is instrumental to disrupt the IED system. In some cases, this is not possible and the target is killed in the process.

Whether the target is captured or killed, *Exploitation* is conducted at the site to gather intelligence. Exploitation yields information on other nodes of the IED system. For instance, the target could have a list of contacts, such as emplacers, suppliers, and planners. The *Analyze* step provides intelligence on new IED designs, TTPs, and sources of components. It also provides evidence to prosecute the target in a court of law. Some targets could be tried back in the Western national court while others are put on trial in the country where the incident took place, such as Afghanistan. Chapter 3 will examine

how friendly nations need to support justice and penal reform in the host nation country to ensure successful prosecution and incarceration.

In addition, the *Exploit-Analyze* stage provides evidence that a particular nation-state is involved in the IED system. This was the case in Iraq where the US and British forces exploited an IED site and found remnants of an explosively formed penetrator (EFP). Their analysis determined that the EFP was built in Iran.[180] Through a diplomatic note, the US accused Iran of supplying Iraqi Shiite insurgents with EFPs, leading to diplomatic and economic sanctions.[181] Additionally, to counter the emerging EFP threat, US forces developed improved armor protection, such as the "Frag Kit Six" added to MRAPs.[182] The *Exploit-Analyze* process also develops TECHINT identifying how the device works. This enables new friendly countermeasures and TTPs, such as jamming new remote control frequencies.[183]

Another aspect of *Exploit-Analyze* involves open-source and media exploitation. Since threat networks use the internet to publicize IED attacks, websites provide valuable intelligence on enemy TTPs. In addition, identifying the Internet Service Provider can pinpoint the location of a support network. Analyzing internet usage and traffic produces a list of members and supporters of the IED system. These websites can be shut down if

---

[180]Michael R. Gordon and Scott Shane, "The Struggle for Iraq; Behind U.S. Pressure on Iran, Long-Held Worry Over a Deadly Device in Iraq," *The New York Times*, 27 March 2007, http://query.nytimes.com/gst/ fullpage.html?res=F40C1EF639540C748EDDAA0894DF404482.

[181]*Ibid*.

[182]Christopher J. Lamb, Matthew J. Schmidt, and Berit G. Fitzsimmons, "MRAPs, Irregular Warfare, and Pentagon Reform," Institute for National Strategic Studies, National Defense University, 2009 http://usacac.army.mil/cac2/cgsc/sams/media/MRAPs.pdf, 24.

[183]NATO, *Allied Joint Doctrine For Countering Improvised Explosive Devices* …, 2-13.

deemed useful to C-IED operations. Yet, all these actions require Cyber assets from national SIGINT capabilities.

The final step in F3EAD is *Disseminate*. The goal of the entire process is to share intelligence between all key stakeholders to enable the C-IED lines of operations. For instance, identifying new enemy TTPs through exploitation allows friendly forces to adapt their TTPs, hence supporting *Prepare the Force* and *Defeat the Device*. Dissemination also involves creating C-IED Flash Reports and BOLO Reports[184] to provide new intelligence on an IED system. To work successfully, all nations must want to share intelligence to mitigate the IED threat. It must also be supplied to NGOs and IOs to reduce the risk to their personnel, therefore strengthening cooperation.

Conclusion

This chapter has examined the C-IED strategy with regards to the three lines of operations. It has shown how those lines are interrelated with the foundation being *Understanding and Intelligence*. Developing the comprehensive intelligence picture requires interagency support such as national law enforcement, GEOINT, SIGINT, and HUMINT agencies. As an IED system may operate in a number of countries, multinational support is also necessary to enable intelligence.

Prepare the Force involves the key operational activity *Prepare* which protects friendly forces through TTPs and training. Sharing with OGDs, IOs, and allied partners achieves a common understanding, reduces interoperability issues and avoids duplication

[184]BOLO stands for "Be On the Look Out". Though a Law Enforcement term, it is used in the C-IED field to designate threat network personnel implicated or suspected to be part of the IED system.

of effort. Undergoing common training and education reduces the risk to "soft targets" certain groups, such as OGDs and civilian actors, therefore strengthening unity of effort. *Defeat the Device* incorporates a number of activities to detect and neutralize IEDs. Under the key operational activity *Protect*, friendly forces reduce the effectiveness of IEDs through force protection measures and Information Operations. Viewing protection of soldiers as a top priority, national governments increased the number of UAVs, RCPs, and MRAPs to enable this line of operation. To avoid duplication of effort and strengthen the Alliance, NATO developed the SMART Defence initiative enabling multinational C-IED equipment acquisition.

Though these two lines of operations are instrumental in the overall C-IED strategy, they are also "stop-gap" measures that have limited success in reducing IEDs. Threat networks rapidly adapt to new friendly technology and shift their attacks to "softer" targets when countermeasures are introduced. Therefore, the C-IED strategy must focus on "Left of Boom" through *Attack the Networks*. AtN performs two major actions: *Prevent* and *Pursue*. Firstly, *Prevent* deters support to the IED system through Information Operations and other activities, therefore attacking its critical vulnerabilities. AtN also prevents an IED system from being effective by predicting where and how insurgents will use IEDs against friendly forces. Through *Pursue*, friendly forces target the IED system using the F3EAD cycle, reducing their effectiveness by directly neutralizing key nodes. However, *Prevent* and *Pursue* cannot be done by military forces alone. The F3EAD involves a wide range of agencies and departments to exploit all four instruments of national power. This is why the Comprehensive Approach is critical to C-IED strategies.

While we are never going to stop all IEDs, a holistic, decisive, Whole of Government approach will significantly impact the effect the IED has in future operations and to our domestic security.

- Lieutenant-General Michael Barbero, *JIEDDO C-IED Strategic Plan*

CHAPTER 3 - OWNING THE COMPREHENSIVE APPROACH

Introduction

In American, British, Canadian, and NATO doctrines, interagency and multinational support are key considerations to enable C-IED operations, as noted in the epigraph above. For instance, NATO doctrine states that "the C-IED approach will require co-operation between nations and within governments, it is a comprehensive approach that is joint, inter-agency and multinational."[185] If one considers the emphasis on this strategy in current doctrine, one would believe that there are no issues with the Comprehensive Approach. Yet, there are major challenges in implementing this strategy. The problem is not the military's appreciation of the Comprehensive Approach, but how national governments empower it.

This chapter will demonstrate why governments must achieve unity of effort by championing the Comprehensive Approach to overcome the limitations of the C-IED strategy. To succeed in realizing unity of effort, a nation's government must address joint and interagency cooperation before it tackles the larger multinational and public approach. This chapter will also consider how instruments of national power effectively disrupt the asymmetric characteristics of the IED system. Lastly, it will examine the

---

[185]NATO, *Allied Joint Doctrine For Countering Improvised Explosive Devices*…, xiii.

obstacles to implement the Comprehensive Approach and measures to overcome them. To begin this analysis, one must consider the overall concepts of the Comprehensive Approach.

Conceptual Foundations

The concepts of the Comprehensive Approach, Whole of Government, and Joint, Interagency, Multinational, and Public concepts have been the subject of many doctrinal publications, government reports, and academic papers. In all cases, they consider these terms to be complementary or synonymous. This paper will not debate the differences between the various concepts. Rather, it will focus on the utility of Comprehensive Approach to C-IED operations. The US Field Manual 3-07 *Stability Operations* provides a suitable definition:

> *Comprehensive approach* is an approach that integrates the cooperative efforts of the departments and agencies of the United States Government, intergovernmental and nongovernmental organizations, multinational partners, and private sector entities to achieve unity of effort toward a shared goal.[186]

Considering this definition, the Whole of Government integrates interagency support from OGDs to military operations (or vice versa). The Whole of Government nests within the larger Comprehensive Approach which incorporates multinational partners and the public sector.[187] Figure 10 illustrates the relationship between the joint,

---

[186]Department of the Army, *Stabilization Operations*…, 1-4.

[187]For the purpose of this paper, the public sector is defined as NGOs, IOs, private corporations, academic institutions, think tanks, and research and development organizations.

Whole of Government, and Comprehensive Approach. It also indicates the departments, agencies, and institutions supporting this strategy.[188]

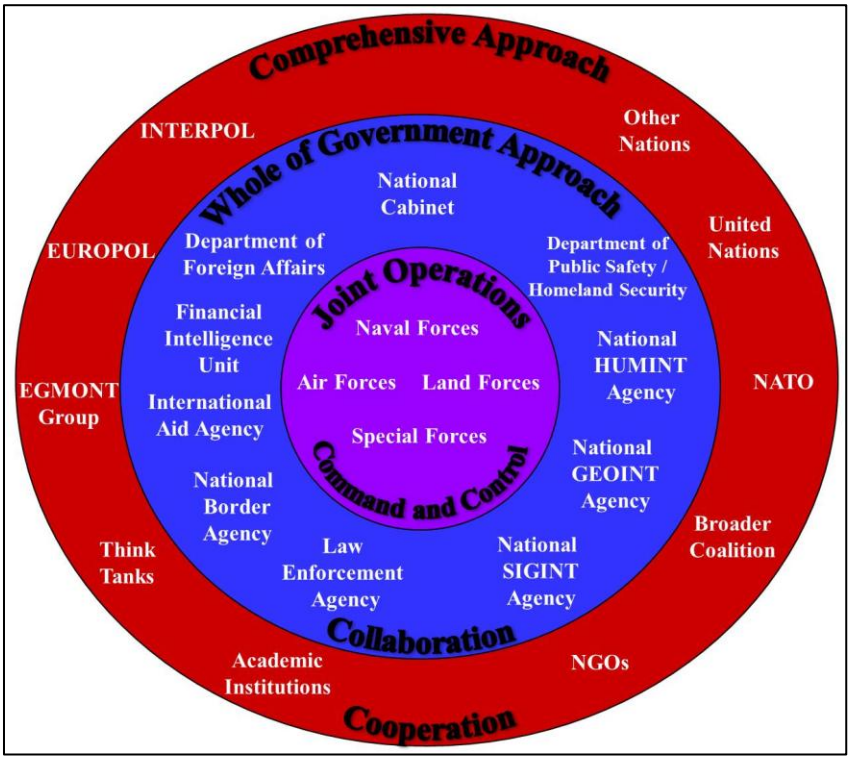


Figure 10 – The Comprehensive Approach

Source: Department of Defence, FM 3-07, *Stabilization Operations*, 1-6.

Furthermore, the definition of the Comprehensive Approach addresses two essential elements to C-IED. The first is the need for cooperation of various organizations as the joint, interagency, multinational, and public levels. As Dr Cécile Wendling argues in her analysis of the Comprehensive Approach, its purpose is to achieve "a common strategy, common mission statement, common understanding of the strategy, and

[188]The original diagram in the source document does not include the various agencies (in white). This was added by the author to illustrate where each department and institution falls under.

common modus operandi".[189] The second crucial element is unity of effort. As it will be demonstrated later, achieving unity of effort is the greatest advantage, but also the greatest challenge, of the Comprehensive Approach.

Enabling Joint Power

Joint power involves all military services: Army, Air Force, Navy, and Special Forces. Since the vast majority of IEDs target ground forces, one could consider that C-IED only applies to the Land Component and Special Forces. However, the attack on the USS Cole in Yemen in 2000 demonstrated that the Maritime Component is also at risk from water-borne IEDs.[190] Surface-to-air and airborne IEDs are also significant threats to the Air Component.[191]

The nature of the threat is not the only reason why each service must be involved in countering IEDs. Each element contributes to the overall C-IED strategy through their specific capabilities. For instance, Special Forces provide time-sensitive targeting and reconnaissance capabilities to the F3EAD cycle.[192] The Air Component provides ISR, air mobility, and precision strike capabilities. [193] By conducting Maritime Security Operations, naval forces can interdict IED support structures, such as piracy financing

---

[189]Cécile Wendling, *The Comprehensive Approach to Civil-Military Crisis Management: A Critical Analysis and Perspective* (Paris: Institut de recherche stratégique de l'École militaire, 2010), http://www.humansecuritygateway.com/documents/IRSEM_TheComprehensiveApproachtoCivilMilitaryCrisisManagement.pdf, 27.

[190]Headquarters of Department of the Army, *Improvised Explosive Device Defeat*, v.

[191]Department of Defense, *Counter-Improvised Explosive Device Operations*…, I-1.

[192]NATO, *Allied Joint Doctrine For Countering Improvised Explosive Devices*…, 1-19.

[193]*Ibid.*

IEDs or smuggling components by sea.[194] When contributing to the C-IED fight, each component must share intelligence and maintain interoperability across the force.

Although western militaries strive to conduct joint operations, there are a number of obstacles that hamper joint efforts. The first hurdle is the competition for resources between each service and the lack of a common strategy on how to tackle a particular issue, such as defeating IEDs.[195] For instance, though important to the US Army, spending $47 billion on MRAPs does not address the US Navy's IED threat. In a world of finite financial resources, it may cause dissention among the services. Without a common strategy, each service develops its own C-IED initiatives causing duplication of effort and interoperability issues.[196]

Due to the lack of cooperation, many nations have created dedicated joint C-IED organizations or task forces. For instance, DoD Directive 2000.19E created JIEDDO, whose mission is "to focus (lead, advocate, coordinate) all DoD actions in support of the Combatant Commanders' and their respective Joint Task Forces' efforts to defeat IEDs as weapons of strategic influence."[197] Although JIEDDO is supposed to be the single point of coordination for C-IED initiatives, it has faced issues in synchronizing the efforts of the US DoD Services and Combatant Commands. In their academic paper on the

---

[194]NATO, *Allied Joint Doctrine For Countering Improvised Explosive Devices* …, 1-22.
[195]Richard Ellis *et al.*, "JIEDDO: Tactical Successes Mired in Organizational Chaos…", 3.
[196]*Ibid.*
[197]Department of Defense, *Joint Improvised Explosive Device Defeat Organization (JIEDDO)*, DoD Directive: 2000.19E, 14 February 2006, http://www.dtic.mil/whs/directives/corres/pdf/200019p.pdf, 2.

challenges facing JIEDDO, the authors made strong recommendations on how to address them, such as realigning the organization under the US Joint Forces Command.[198]

The House of Representatives also examined JIEDDO's efforts in 2008, and found similar issues, particularly that the organization was not leading all DoD C-IED efforts.[199] Reports from the Government Accountability Office (GAO) in 2012 presented the same findings. Stating that JIEDDO still did not have "full visibility of all C-IED initiatives within DoD", GAO recommended that JIEDDO establish a comprehensive database of C-IED initiatives.[200] It also recommended that DoD provide JIEDDO with additional authorities for the oversight of all C-IED efforts. [201] These challenges highlight the need to address joint C-IED command and control. In 2012, JIEDDO developed a Strategic Plan to address these issues over a four year period. The plan emphasizes the need for JIEDDO to enable all C-IED initiatives through effective oversight, proper authority, and a streamlined acquisition process.[202]

In Canada, the CF encountered similar issues in implementing joint C-IED strategy. Facing an increasing threat of IEDs in Afghanistan, the Chief of Defence Staff created the CF C-IED Task Force (CF C-IED TF) in 2006, becoming "the strategic focal point for C-IED issues within the CF."[203] Before 2006, acquisition of C-IED equipment was left to each service. The CF C-IED TF rapidly assumed oversight for all acquisition

---

[198]For more, see Ellis *et al.*, "JIEDDO: Tactical Successes Mired in Organizational Chaos…"

[199]House of Representatives Subcommittee, *JIEDDO DoD's Fight Against IEDs …*, 9.

[200]Adam Smith, Roscoe Bartlett and Silvestre Reyes, *Counter-Improvised Explosive Devices: Multiple DoD Organizations are Developing Numerous Initiatives* (United States Government Accountability Office: GAO-12-861R, 1 August 2012), http://www.gao.gov/products/GAO-12-861R, 2.

[201]Smith *et al.*, *Counter-Improvised Explosive Devices…*, 2.

[202]Department of Defense, *Counter Improvised Explosive Device Strategic Plan …*, 7.

[203]Department of National Defence, *Counter Improvised Explosive Devices Operations …*, 3-2.

of EOD, force protection, and countermeasures. It also drafted the joint C-IED doctrine 3.15 which clearly delineates the roles and responsibilities of each service as well as strategic, operational, and tactical commands.[204] In addition, CFJP 3.15 lists all the government and multinational agencies supporting C-IED. The result was an integrated joint plan for all C-IED initiatives and efforts.

Both the American and Canadian examples highlight the need for a strategic solution to solve the joint problem. In both cases, it was the government through the department of defense that empowered the joint C-IED organization with the proper levels of authority and oversight. This underlines the need for a "top-down" approach to the C-IED fight. Although each service may have its own ideas on countering the IED threat, the government must regroup these initiatives to achieve a common strategy. A unified approach ensures interoperability, common understanding, and synchronizes each service's capabilities. Once a nation addresses the joint aspect, it can start focusing on the next step: interagency support.

Gaining Interagency Support

Chapters 1 and 2 have stressed the need for interagency support to disrupt the IED system and facilitate the C-IED strategy. Threat networks operate throughout the world, involving loose networks from criminal to terrorist groups. Therefore, military forces cannot adequately disrupt an IED system without involving a number of government departments and agencies. In addition, not all operations will be military-led. Friendly

---

[204]Department of National Defence, *Counter Improvised Explosive Devices Operations …,* 3-2.

forces may be called to support domestic or international operations where another national agency is in the lead, such as Foreign Affairs or law enforcement.[205] JIEDDO has recognized this fact in its mission statement:

> Lead DoD actions to rapidly provide C-IED capabilities and solutions in support of Combatant Commanders, the Services, and *as authorized, other federal agencies to enable the defeat of the IED as a weapon of strategic influence* [emphasis added].[206]

Consequently, all agencies and departments must collaborate to ensure they also achieve common strategy, understanding, and *modus operandi*.[207] As highlighted in the epigraph of this chapter, the JIEDDO Strategic Plan also emphasizes the Whole of Government approach.[208] As a result, JIEDDO launched two key initiatives that accelerated interagency support. The first was the establishment of the Counter-IED Operations Integration Center (COIC) in 2006.[209] COIC is a fusion centre supporting *Attack the Network* operations by analyzing intelligence from national agencies, such as NSA, NGA, and CIA.[210] The second initiative was the establishment of the Law Enforcement Program (LEP). Recognizing that threat networks operate like criminal groups, LEP

---

[205]For an example of military C-IED support to domestic operations, see Geoffrey D. Stevens, *Whole Of Government Approach to Countering Domestic IEDS: Leveraging Military Capabilities* (Syracuse: Institute for National Security and Counterterrorism, 2012), http://insct.syr.edu/uploadedFiles/insct/about/in_the_news/Whole%20of%20Government%20Approach.pdf.

[206]Department of Defense, *Counter Improvised Explosive Device Strategic Plan…,* 1.

[207]Wendling, *The Comprehensive Approach…,* 27.

[208]According to the JIEDDO Strategic Plan, the definition of Whole of Government is "is the ability to rapidly synchronize counter-threat network capabilities and actions among joint, interagency, intergovernmental, international, and other federal agencies' C-IED stakeholders." Therefore, it is synonymous with the US Stability Operation definition of the Comprehensive Approach.

[209]Department of Defense, *Joint Improvised Explosive Device Defeat Organization 2006 Annual Report* (Norfolk: Joint Improvised Explosive Device Defeat Organization, 2006), https://www.jieddo.mil/content/docs/2006_JIEDDO_Annual_Report_(U).pdf, 1.

[210]House of Representatives Subcommittee, *JIEDDO: DoD's Fight Against IEDs…,* 20.

integrates professionals from the Drug Enforcement Agency (DEA), the FBI, and other police departments that support AtN by providing *Pursue* subject matter expertise.[211]

Interagency collaboration also facilitates *Prevent*, particularly in affecting the IED system's critical vulnerabilities. For instance, by improving a host nation's government control and the social conditions of its local population, it reduces safe havens. Corruption, popular support, and criminal support are necessary for freedom of movement. To affect these vulnerabilities, friendly nations need to improve the local conditions, specifically governance and development.

In Western countries, this is called Stabilization Operations. Highlighted in a number of doctrinal publications and academic papers, these operations are considered a critical military task in today's complex operational environment.[212] The United States defines Stabilization Operations as follows:

> An overarching term encompassing various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or re-establish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief.[213]

This definition addresses two major concepts that apply to C-IED operations. The first is the importance of harnessing the instruments of national power. The second focuses on the maintenance or re-establishment of three key areas: security, governance, and

---

[211]House of Representatives Subcommittee, *JIEDDO: DoD's Fight Against IEDs…,* 24.

[212]For examples of papers addressing the importance of Stabilization Operations, see Andrew Leslie, P. Gizewski, and M. Rostek, "Developing a Comprehensive Approach to Canadian Forces Operations," *Canadian Military Journal* 9, No. 1 (Spring 2008); Patrick Travers and T. Owen, "Peacebuilding While Peacemaking: The Merits of a 3D Approach in Afghanistan," *UBC Center for International Relations Security and Defense Forum Working Paper #3 (*Vancouver: University of British Columbia, 2007), http://cicam.ruhosting.nl/teksten/ act.07.grotenhuis.owen%20paper.pdf.

[213]Department of Defense, JP 3-0, *Joint Operations* (Washington, DC: Department of Defense 2008), GL-26.

economic development. In western democracies, each federal department is primarily responsible for one area of national power. Consequently, the military cannot efficiently conduct Stabilization Operations without the participation of OGDs listed in Figure 10.

To stabilize failed and failing states, Canada, the UK, and the US developed "Defense, Diplomacy, and Development (3D)" concept.[214] Based on activities performed by Whole of Government, it nests within the greater Comprehensive Approach.[215] 3D enables military operations through security sector reform (SSR), economic development, and local governance. For C-IED operations, 3D effectively reduces local support to threat networks by "winning hearts and minds".[216] The Canadian Independent Report on Afghanistan (Manley Report) describes the importance of security in setting the conditions for the other dimensions:

> Each dimension, of course, affects the others in dynamic interaction. Security enables development; effective governance enhances security; development creates opportunities, and multiplies the rewards, of improved security and good governance. In this virtuous circle of cause and effect, security is an essential condition of good governance and lasting development.[217]

This statement addresses the interdependence between defence, development, and diplomacy. As Lieutenant-General Leslie *et al.* argue: "…military operations are likely to

---

[214]Andrew Leslie, P. Gizewski, and M. Rostek, "Developing a Comprehensive Approach to Canadian Forces Operations," *Canadian Military Journal* 9, No. 1 (Spring 2008): 12.

[215]For the history of the development of the concepts and relationships between 3D, Whole of Government, and the Comprehensive Approach, see Patrick Travers and T. Owen, "Peacebuilding While Peacemaking: The Merits of a 3D Approach in Afghanistan," *UBC Center for International Relations Security and Defense Forum Working Paper #3 (*Vancouver: University of British Columbia, 2007), http://cicam.ruhosting.nl/teksten/ act.07.grotenhuis.owen%20paper.pdf.

[216]This term was introduced by Sir Gerald Templer during the Malayan Emergency. For more details see: Austin Long, *On "Other War' 'Lessons from Five Decades of RAND Counterinsurgency Research* (Santa Monica, CA: RAND Corporation, 2006), 23.

[217]John Manley, *et al.*, *Independent Panel on Canada's Future Role in Afghanistan* (Ottawa: Public Works and Government Services, 2008), 11.

be as much about 'winning hearts and minds' … as they are about engaging in armed combat and destroying adversaries."[218] This view is also shared by Dr David Kilcullen when discussing counter insurgency:

> Governments seek to defeat insurgents primarily through 'winning the hearts and minds' of the broader population, a process that by necessity often involves compromise and negotiation…. In this paradigm, insurgency is a Whole of Government problem rather than a military or law-enforcement issue.[219]

To "win hearts and minds", the instruments of national power must be harnessed to influence the three elements of society, or as Carl von Clausewitz calls them "the trinity": government, military, and people.[220] By exploiting these instruments of power, friendly nations can improve security, the economy, and governance.

In Afghanistan, the Government of Canada used 3D to strengthen these three areas.[221] The Canadian Forces' Task Force Kandahar (TFK) used the "clear, hold, and develop" approach.[222] During "clearing", the TFK Battle Group (BG) conducted offensive operations to rout out insurgent groups. TFK's Observer Mentor Liaison Team (OMLT) developed the ANSF who performed the "hold" function by safeguarding villages and preventing the Taliban from returning.[223] Once the area was secure, development started under TFK's Provincial Reconstruction Team (PRT) and CIDA. Developing "Quick Impact Projects", the PRT and CIDA provided essential services to

---

[218]Leslie, *et al.*, "Developing a Comprehensive Approach*…",* 1.

[219]David Kilcullen, "Countering Global Insurgency," *Journal of Strategic Studies* 28, no. 4 (August 2005): 605.

[220]Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 7.89.

[221]Government of Canada, *Canada's Engagement in Afghanistan…,* 8.

[222]Manley, *et al.*, *Independent Panel on Canada's Future Role in Afghanistan…,* 13.

[223]Lee Windsor, D. Charters and B. Wilson, *Kandahar Tour: The Turning Point In Canada's Afghan Mission* (Mississauga: John Wiley & Sons, 2008), 92.

Afghan villages.[224] This approach allowed the local population to feel secure and improved their quality of life.[225] A greater sense of security helped in reducing local support to the IED system, contributing to the *Prevent* activity of the C-IED strategy.

In addition, DFAIT and the CF's Strategic Advisory Team (SAT) worked with the Government of the Islamic Republic of Afghanistan (GoIRA) and the Kandahar provincial government to improve its national institutions.[226] Reducing corruption and improving the ministries' efficiency also increased Afghan acceptance of the Canadian military in Afghanistan. By winning over the Afghans, TFK could rely on them to assist in developing intelligence in the area.[227] Local intelligence is essential to C-IED as argued in *Fixing Intel*:

> Local people … are far better than outsiders at spotting insurgents and their bombs and providing indications and warnings "left of boom" (before IEDs blow up). The second inescapable truth asserts that merely killing insurgents usually serves to multiply enemies rather than subtract them.[228]

Therefore, by focusing on the population instead of destroying the enemy, the security situation was improved. These arguments show why development and governance support C-IED operations. By improving basic services, friendly forces gain the confidence of the local population, which in turn, provide intelligence on the IED threat.

Interagency support also enables the *Pursue* activity, particularly the F3EAD process. As demonstrated in Chapter 2, national law enforcement agencies contribute personnel to the Level 2 exploitation centre (CEXC). National laboratories also provide

---

[224]Windsor *et al.*, *Kandahar Tour…,* 46.
[225]Government of Canada, *Canada's Engagement in Afghanistan…,*8.
[226]*Ibid.*
[227]Windsor *et al.*, *Kandahar Tour…,* 48-49.
[228]Flynn *et al.*, "Fixing Intel…",8.

reachback support for out-of-theatre Level 3 exploitation, which allows for "in-depth technical and forensic examination and analysis utilising scientific and counter criminal capabilities."[229] Friendly forces need this forensic and biometric data to adequately conduct F3EAD, especially to initiate the process.

Pursue also involves improving law enforcement and judicial processes to ensure IED facilitators are properly arrested, convicted, and imprisoned. In Afghanistan, Canada sent RCMP, Correctional Services Canada (CSC), and Department of Justice Canada (DJC) personnel to improve institutional capacities.[230] Without a functioning correctional system in Afghanistan, there is little benefit in arresting IED facilitators. A corrupt and inefficient prison system has caused some nations to question the whole C-IED strategy, particularly the exploitation process. For instance, in the wake of a number of EOD operators killed while neutralizing and exploiting IEDs, British commanders have reportedly changed their policy with regards to IED exploitation. As journalist Sean Raymond has reported:

> Rather than removing bombs from the ground without blowing them up, so that they can be forensically analysed, more devices will now be simply destroyed in situ. Senior officers believe the new tactic will be quicker and safer.[231]

Pierre Nolin has argued that the policy change is a result of the inefficiencies in the Afghan justice system.[232] By believing that IED facilitators will not be adequately convicted, or will easily escape from prison, some military commander will not risk EOD

---

[229]NATO, *Allied Joint Doctrine For Countering Improvised Explosive Devices…,* 2-14.
[230]Government of Canada, *Canada's Engagement in Afghanistan…,*13.
[231]Sean Rayment, "Commanders to Change Bomb Disposal Tactics," *The Telegragh*, 12 February 2011. http://www.telegraph.co.uk/news/uknews/defence/8320560/Commanders-to-change-bomb-disposal-tactics.html.
[232]Nolin, *Countering the Afghan Insurgency*…, 8.

operators' lives to conduct IED exploitation, which considerably affects C-IED strategy, particularly *Attack the Network*. This example highlights how each nation will have different views of C-IED operations, which leads to the requirement of addressing the multinational approach to achieve unity of effort.

Achieving Multinational Support

The importance of multinational cooperation is highlighted in a number of doctrinal publications, particularly in the US Joint Publication 3-15.1 where "Developing Multinational and HN C-IED Capability" is a line of operation.[233] Since not all nations can afford the full spectrum of C-IED resources, lead nations may have to provide partners with a variety of C-IED support.[234] Ensuring common training is another goal of multinational C-IED operations. Specifically, not all nations have the ability to run C-IED pre-deployment or in-theatre training. To overcome this issue, NATO has implemented a C-IED Action Plan that includes COEs taking on the responsibility for a number of training activities.[235] This avoids duplication of work, strengthens common understanding, and ensures standards across nations.

Combined training also develops communities of interest through networking, which contributes to unity of effort. For NATO, unity of effort is critical since cohesion is considered the Alliance's Centre of Gravity.[236] The NATO C-IED Campaign Plan

---

[233]Department of Defense, *Counter-Improvised Explosive Device Operations…,* III-6.
[234]*Ibid.*, xiv.
[235]NATO C-IED.org, "Counter Improvised Explosive Device (C-IED) Courses / Training," last accessed on 26 February 2013, https://www.c-ied.org/Training/Courses.aspx.
[236]NATO, *BI-SC Counter-Improvised Explosive Device (C-IED) Campaign Plan*…, 22.

stresses the significance of the protecting the Centre of Gravity, particularly in an environment where IEDs pose a considerable risk to friendly forces:

> Continued unacceptable levels of casualties caused by IEDs in future NATO operations that, if not addressed, undermine international willingness to continue the effort, reduce support from nations, undermine the Alliance Centre of Gravity (cohesion among the Alliance), restrict NATO freedom of action, and ultimately reduce NATO credibility and relevance.[237]

Thus, by reducing the strategic effects of IEDs, nations are more likely to contribute forces to an operation. Therefore, enabling nations to collaborate in C-IED operations protects the Alliance Centre of Gravity.

The multinational approach will also support joint capabilities since each nation provides a portion of the Combined Joint Statement of Requirement (CJSOR) within the coalition. For instance, a number of nations contribute specific capabilities to Crisis Response Operations through the NATO Response Force (NRF). Yet, the NATO C-IED Working Group identified that NRF did not have dedicated C-IED capabilities.[238] As a result, NATO issued a request to nations to provide a range of C-IED equipment and personnel to the NRF.[239] Through multinational collaboration, NATO is enabling C-IED by having nations provide their expertise in specific fields.

In addition to the military alliance collaboration, the Comprehensive Approach includes partnerships across all departments and agencies. As demonstrated in Chapter 1, contemporary threat network are based on informal ties of like-minded individuals. The

---

[237]NATO, *BI-SC Counter-Improvised Explosive Device (C-IED) Campaign Plan*…, 22.
[238]*Ibid.*
[239]Peter Kowalski, *Counter – Improvised Explosive Device (C-IED) Capability Package to the NATO Response Force* (NATO Consultation, Command, and Control Agency: file NC3A-BE/ACQ/ASG/ 12/ 0492, 4 June 2012), http://www.defensa.gob.es/Galerias/info/servicios/concursos/ 2012/06/MS-13500-NRF.pdf.

loose network is hard to target since it can be anywhere in the world. Consequently, law enforcement and intelligence agencies must work together to disrupt their activities. One method to accomplish this level of collaboration during C-IED operations, particularly between law enforcement agencies, is to involve international organizations.

Incorporating IO, Public, and Private Institutions

As illustrated in Figure 10, the Comprehensive Approach can be supported by a number of private corporations, academic institutions, and international organizations. They all bring their own specific expertise and complement interagency and multinational support. Ensuring their cooperation can be accomplished through mutual benefit, trust, and a willingness to defeat the IED threat.

Private corporations contribute to C-IED operations through their research and development of equipment (R&D) or development of C-IED training, mainly of the *Defeat the Device* and *Prepare the Force* line of operation. Obviously, they benefit from this process through government acquisition of equipment and training. Yet, it provides the military with commercial-off-the-shelf equipment, which can reduce the time to field new military capabilities. JIEDDO states that "private R&D accelerates the most promising C-IED solutions to combat the ever-evolving threat."[240] With regards to C-IED training, a number of private companies facilitate *Prepare the Force*, such as Allen Vanguard, the Saab Group, and MKDS. They provide courses in C-IED equipment

[240]Department of Defense, *Counter Improvised Explosive Device Strategic Plan*…, 2.

operation, WIT exploitation, IEDD, and C-IED TTPs. Outsourcing this training releases military and other OGD personnel to focus on operations.

Other elements that contribute to the Comprehensive Approach are academic and private institutions. Since completing JIPOE requires knowledge of the social and cultural dynamics, it involves "human terrain", which is defined as "social science research about the local population to provide situational awareness to the military."[241] Yet, friendly forces rarely have in-house sociology experts. Consequently, JIEDDO developed a proof of concept project called the Human Terrain System (HTS).

Now fully integrated in the US Army, the HTS includes sociologists, psychologists, and anthropologists who provide social-cultural information to the US Army, the US Marines, and nine other coalition countries in Afghanistan.[242] Determining the attitude of the local population is crucial to the C-IED strategy since friendly forces will be better positioned to influence their beliefs.[243] For instance, by improving the population's perceptions, the public is more likely to report IEDs and facilitators to friendly or local security forces.[244]

The HTS provides additional benefits to C-IED operations, specifically by bringing in new perspectives than those of military forces. Dr Montgomery McFate and Dr Steve Fondacaro note the utility of civilian staff supporting JIPOE:

---

[241]Montgomery McFate and Steve Fondacaro, "Reflections on the Human Terrain System During the First 4 Years," *Prism* 2, no. 4 (September 2011): 63, http://www.ndu.edu/press/lib/images/prism2-4/Prism_63-82_McFate-Fondacaro.pdf.

[242]Christopher A. King, Robert Bienvenu, and T. Howard Stone, "HTS Training and Regulatory Compliance for Conducting Ethically-Based Social Science Research," *Military Intelligence Professional Bulletin* 37, no. 4 (October-December 2011): 16, http://www.fas.org/irp/agency/army/mipb/2011_04.pdf.

[243]NATO, *Allied Joint Doctrine For Countering Improvised Explosive Devices* …, 3-13.

[244]*Ibid.*

> Civilian members of [Human Terrain Teams (HTT)] (or Counter-insurgency Advisory and Assistance Teams, or any other entity that uses scholarly labor in a military context) contribute something valuable to the commander and staff of deployed units—namely, a unique *nonmilitary* perspective derived from years of education and research. Civilian social scientists who work *for* the military but are not *in* the military bring a level of objectivity and an out-of-the-box perspective that promotes increased understanding of the civilian population and helps identify more effective courses of action. Because civilian members of an HTT are not beholden to the performance pressures created by the need to obtain a favorable Officer Evaluation Report rating, they can articulate views not necessarily in conjunction with the dominant perspective.[245]

This statement highlights two advantages of having civilians contributing to C-IED operations: a non-military perspective and a certain level of independence.

These advantages also apply to think tanks, academic institutions, and other private organizations that support C-IED operations through academic R&D. For instance, the RAND Corporation, the Centre for a New American Security, and the International Institute for Strategic Studies have published a number of articles and papers contributing to the overall understanding of the IED threat, counter-insurgency, and counter-terrorism.[246] Through these papers, the C-IED community has developed a greater appreciation of the larger context, reinforcing *Understanding and Intelligence*.

Yet, incorporating public institutions under the Comprehensive Approach requires a certain willingness to cooperate. One method to improve cooperate that is widely used in the C-IED community is to invite these organizations to attend conferences and working groups and have them share their expertise. For instance, INTERPOL and EUROPOL participated in a number of conferences hosted by the C-IED COE, which led

---

[245]Montgomery McFate And Steve Fondacaro, "Reflections on the Human Terrain System During the First 4 Years," *Prism* 2, no. 4 (September 2011): 76, http://www.ndu.edu/press/lib/images/prism2-4/Prism_63-82_McFate-Fondacaro.pdf.

[246]For specific papers on these topics, see Marla C. Haims *et al*., 2008; Michael Flynn *et al.*, 2010.

to both intergovernmental law enforcements organizations in providing *Pursue* education and training.[247] Through mutual support, INTERPOL is also assisting in the *Prevent* activity through the creation of a dedicated C-IED unit called the Chemical and Explosives Terrorism Prevention (ChemEx).[248] Furthermore, INTERPOL provides the collaboration mechanism between different law enforcement agencies, thus improving multinational information exchange on the IED system.

Another organization that contributes to *Prevent* is the Egmont Group, an informal network of Financial Intelligence Units (FIUs). Through Egmont, "FIUs cooperate in the fight against money laundering and financing of terrorism and to foster the implementation of domestic programs in this field,"[249] which mitigates a threat network's critical capability of sourcing financial support to an IED system. Similar arrangements exist with other international organizations such as the United Nations and World Customs Organization (WCO) that support C-IED operations. For instance, the United Nations Office on Drugs and Crime (UNODC) created the Global Project strategy that strengthens counter-terrorism legislation, including IED-related terrorism.[250] From this strategy, UNODC established working groups that led to another international organization initiative, Project Global Shield. WCO's final report on the project

---

[247]INTERPOL, "INTERPOL supports international training course on countering homemade explosives," last accessed on 4 March 2013, http://www.interpol.int/News-and-media/News-media-releases/2012/N20121024Bis.

[248]INTERPOL, "New unit to assist INTERPOL member countries combat chemical and explosives terrorism," last accessed on 4 March 2013, http://www.interpol.int/News-and-media/News-media-releases/2012/N20120918ter.

[249]Egmont Group, "About the Egmont Group," last accessed on 7 January 2013, http://www.egmontgroup.org/.

[250]United Nations Office of Drugs and Crime, "The Global Project on Strengthening the Legal Regime Against Terrorism," last accessed on 4 March 2013, http://www.unodc.org/unodc/en/terrorism/UNODC_Role/Global_Project.html.

addresses its purpose in supporting *Attack the Network* operations, specifically *Prevent* activities:

> To combat the threat that IEDs pose to the international community, the World Customs Organization, in conjunction with the International Police Organization (INTERPOL), the United Nations Office on Drugs and Crime (UNODC), and its Member countries administrations, launched Project Global Shield. Project Global Shield was a six-month multilateral law enforcement operation that sought to monitor the licit movements of explosive precursor chemical shipments to identify and combat the illicit cross-border diversion and trafficking of those chemicals used to manufacture IEDs.

UNODC also supports the reduction of HME production in Pakistan and Afghanistan, where approximately 80% of IEDs are built using HME, primarily from calcium ammonium nitrate (CAN).[251] Although GoIRA banned CAN in 2010, smugglers easily move it into Afghanistan due to the porous nature of the Pakistan-Afghanistan border.[252] As a result, the US created a C-IED Working Group (C-IED WG) chaired by the US State Department, with representatives from the departments of Homeland Security (DHS), Defence (DoD), Justice (DOJ), and Agriculture (DOA), as well as the US Agency for International Development (USAID), the British High Commission, and UNODC.[253]

The C-IED WG works with their Pakistani and Afghan counterparts to improve border control to suppress smuggling of IED precursors, finding alternatives of CAN for legitimate use in farming, and enable both countries improve their intelligence exploitation efforts.[254] This example highlights the value of using the Comprehensive

---

[251]Johnson, *U.S. Agencies Face Challenges…*, 1.
[252]Ibid., 5.
[253]Ibid., 2.
[254]Ibid.

Approach to disrupt the IED system: ISAF forces could not have done this since they do not have either the mandate or the capabilities to affect these areas in Pakistan, particularly in finding a solution to the use of fertilizers. The reduction of HME production required unity of effort which was championed by the highest level of federal governments, and supported by international and intergovernmental organizations that provided diplomatic solutions.

CHAMPIONING C-IED

The Comprehensive Approach can only succeed if all government departments and other key stakeholders are working towards a common goal. However, achieving unity of effort can be very challenging. Interagency support is often characterized by "turf wars", bureaucratic hurdles, and resources shortfalls.[255] Clearly defined political objectives from national governments can be also challenging.[256]Dr Patrick Travers and Dr Taylor Owen note:

> Diplomats, humanitarians, and defence experts may view the same issues in strikingly different terms, reflecting varying institutional cultures and divergent objectives…. Without sufficient common ground, setting joint goals and developing a shared strategy may well be impossible. This task is also made more challenging within an integrated policy framework.[257]

---

[255]Christopher Schnaubelt, "The Challenges to Operationalizing a Comprehensive Approach," In *Operationalizing a Comprehensive Approach in Semi-Permissive Environments,* edited by Christopher Schnaubelt (Rome: NATO Defense College, 2009), 36.

[256]*Ibid.*

[257]Patrick Travers and T. Owen, "Peacebuilding While Peacemaking: The Merits of a 3D Approach in Afghanistan," *UBC Center for International Relations Security and Defense Forum Working Paper #3 (*Vancouver: University of British Columbia, 2007), http://cicam.ruhosting.nl/teksten/act.07.grotenhuis.owen%20paper.pdf.8.

In addition to the problems of finding common ground between different departments in one country, there must be a common strategy, a common mission statement, and a common understanding in the coalition.[258] However, since each friendly nation may have its own reason to participate in conflict stabilization, this common approach can be difficult to achieve. National laws may also preclude from sharing intelligence with other nations, mainly due to privacy concerns.[259] Yet, these obstacles must be overcome to address the limitations of the C-IED strategy, mainly those effecting *Attack the Network* operations. Addressing these challenges can involve two approaches: formal authority and informal relationships.

Formal Authority

Formal authority requires the involvement of the highest level of government. In the United States, it must be the President who enables interagency and multinational support. Recently, the White House has issued a number of strategies that overcome the significant issues regarding countering IEDs. These included DoD Directive 2000.19E which created JIEDDO in 2006, the National Strategy for Terrorism-Related Information Sharing published in 2007, the Comprehensive National Cybersecurity Initiative of 2010, and the 2011 National Strategy for Counterterrorism. These publications clearly outlined the roles, responsibilities, and authorities to improve information sharing, cyber activities,

---

[258]Wendling, *The Comprehensive Approach…,* 27.

[259]White House, *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (Washington, DC: White House, 2007), http://www.fas.org/sgp/library/infoshare.pdf, 25-26.

and overall global counterterrorism activities across a Whole of Government, and multinational approach.

Yet, it was the White House's Strategy for Countering Improvised Explosive Devices that most comprehensively addressed the limitations to effective C-IED. Signed by President Barack Obama on 26 February 2013, it strengthened US policy with regards to countering IEDs and translates that policy into clearly defined actions.[260] These actions include the following:

> Increasing domestic and international engagement, advancing intelligence and information analysis, exploiting IED materials, stemming the flow of explosive precursors, maintaining deployable C-IED resources, and standardizing training and equipment. [261]

Therefore, the US approach addresses the three C-IED pillars, with the primary focus on *Attack the Network* operations. The document also recognizes the importance of the Comprehensive Approach to counter this global and enduring threat. [262] This high-level strategy is a clear example of how C-IED must be championed by a "top-down" approach.

In the UK, the primary document indicating the government's commitment to implementing the Comprehensive Approach is CONTEST, the counter-terrorism (CT) strategy. This strategic document addresses the need for "the police and Security

---

[260]White House, *Countering Improvised Explosive Devices* (Washington, DC: White House, 2013) http://www.whitehouse.gov/sites/default/files/docs/cied_1.pdf, 1.

[261]*Ibid.*, 1-3.

[262]*Ibid.*, 4.

Service … to improve their ability to work locally, nationally and with our international partners to counter the threat."[263] It also highlights that IEDs are the main threat to UK interests and the need to counter IED support structures, such as financing and communications technology.[264] Interestingly, CT strategy is based on four major activities: *Prepare*, *Prevent*, *Protect*, and *Pursue*. Therefore, one can easily draw conclusions on the relationship between CT and C-IED strategies.

The Canadian CT strategy, *Building Resilience Against Terrorism*, also has similar key operational activities: *Prevent*, *Detect*, *Deny*, and *Respond*.[265] When examining their definitions, they correspond to the definitions of the four C-IED activities. The concepts of the Whole of Government and 3D are clearly emphasized in this strategy:

> Canada also partners with the international community to promote security in other states, including fragile states under its whole-of-government approach, which involves defence, development and diplomacy.[266]

The document delineates the roles and responsibilities of each Canadian government department and agency under the Whole of Government approach and how they contribute to the key operational activities. The strategy also focuses on the involvement of IOs and multinational partners, such as the UN, NATO, INTERPOL, WCO, and the Egmont Group.[267]

---

[263]Home Department, *CONTEST: The United Kingdom's Strategy for Countering Terrorism* (London: The Stationary Office Limited, 2011), 52.

[264]*Ibid.*

[265]Government of Canada, *Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy* (Ottawa: Library and Archives Canada, 2011), 13.

[266]*Ibid.*, 19.

[267]*Ibid.*

When considering the CT and C-IED strategies in the US, the UK, and Canada, one would believe that the Comprehensive Approach is always implemented since these documents undoubtedly stress its importance. However, writing a policy and enforcing it are two different things. As demonstrated, despite having all the formal authorities, JIEDDO is still facing problems in synchronizing C-IED efforts in the US. Therefore, improving C-IED coordination also requires the second approach: informal relationships.

Informal Relationship

This approach is developed through a series of activities such as C-IED working groups, conferences, and exercises. This forms communities of interest based on personal and organizational relationships between the military, OGDs, allied partners, and public institutions. For instance the NATO Community of Interest includes all relevant COEs, training establishments, fusion centers, and NATO strategic, operational, and tactical headquarters. It also includes member-nation C-IED organizations, law enforcement, and international organizations, such as INTERPOL and the European Defence Agency.[268] To improve working relationships, NATO Allied Command Transformation and Allied Command Operations have developed a C-IED Campaign Plan. This plan includes institutionalizing NATO and national training plans, conducting experimentation exercises, enhancing practical cooperation with across the Alliance, intergovernmental

[268]NATO C-IED.org, "Community Partners," last accessed on 10 March 2013, NATO C-IED.org, "Community Partners," last accessed on 26 February 2013, https://www.c-ied.org/en-us/community.aspx.

law enforcement, international organisations, NGOs and local actors in the planning and conduct of operations.[269]

The major advantage of both formal and informal approaches is the cost. Specifically, these actions require minimum investment from federal governments. Sending a number of personnel on training activities and as liaison officers in joint interagency task forces is not a significant amount when compared to the billions of dollars invested in force protection and countermeasures. Yet, developing interagency and multinational cooperation considerably improves the ability to conduct C-IED operations. As demonstrated throughout this paper, the Comprehensive Approach harnesses the expertise of each department and agency, therefore mitigating their own limitations. Fundamentally, the governments' ultimate objective is achieving success while reducing costs.

Conclusion

American, British, Canadian, and NATO C-IED doctrines have extensive references to the Comprehensive Approach, highlighting why it enables friendly forces in defeating an IED system. Doctrine demonstrates the utility of joint command and control to affect all three lines of operations. Naval forces contribute to interdicting IED system support networks, whereas the Air Component provides ISR and precision strike capabilities. Special Forces have their unique exploitation, reconnaissance, and targeting roles in the F3EAD process. Performing the majority of C-IED activities, land forces

---

[269]NATO, *BI-SC Counter-Improvised Explosive Device (C-IED) Campaign Plan*…, 7.

contribute to all three lines of operations through “clear and hold operations”. These are primarily short-term activities.

For medium and long-term effects on an IED system, friendly forces require interagency collaboration. Law enforcement, corrections, and justice departments must modernize host nation institutions where threat networks operate to ensure that IED facilitators will be successfully sentenced and imprisoned. Development agencies and diplomatic corps have to improve the local economic and governance conditions to reinforce “winning hearts and minds”.

When working in a coalition, the multinational approach enables other nations to cooperate. Working with allies reduces duplication of effort and increases interoperability and exchange of information. Ultimately, it achieves unity of effort, which is crucial to an alliance centre of gravity, where cohesion provides freedom of action to friendly forces. By incorporating the public sector and international organizations, C-IED organizations benefit from an external perspective. Sociology academics assist with knowledge development of the local situation, which is instrumental to population-centric intelligence. Private R&D and training also support C-IED organizations by reducing the amount of personnel dedicated to fielding equipment and to C-IED education and training.

Yet, the greatest long-term solution rests with the commitment of the national government. As demonstrated, the major challenge of the Comprehensive Approach is its implementation. Since there are a number of obstacles to the application of this strategy, it must be the federal government that champions it by establishing formal policies for information sharing and synchronizing C-IED efforts. In addition, improving informal

relationships helps alleviate some of the issues in implanting the Comprehensive Approach, such as turf wars, bureaucratic hurdles, and resource competition. Exchanging liaison officers and attending training and conferences enhances common understanding and common strategy, and ultimately, unity of effort. The overall cost of improving formal and informal relationship is significantly lower to the billions spent on C-IED equipment.

CONCLUSION

Though the IED is not a 21st century invention, it has not been used in the past as significantly as it is today. IEDs are now present in almost every country in world, affecting every sphere of society. In Afghanistan and Iraq alone, there have been over 100,000 IEDs in the last ten years. These attacks have killed and injured thousands of soldiers and civilians, which is more than by any other weapon system.

IEDs have become the weapon of choice for all sorts of threat networks since they are easy to build, easy to use, easy to adapt, and very cheap. They provide stand-off capability and, if sufficiently large, can defeat any armour, which circumvents friendly strategies employed by militaries to protect their forces. These asymmetric weapons also provide to those employing IEDs the advantage of avoiding decisive engagements. IEDs are weapons of strategic influence which are used to target military, economic, and diplomatic targets, and threat networks used them effectively to attack their enemy's centre of gravity: national will.

To mitigate their effects, western nations have developed a common C-IED strategy based on three lines of operations. *Prepare the Force* and *Defeat the Device* are mainly tactical actions aimed at mitigating the effects of IEDs in the physical realm using training and equipment. These activities are costly and have their limitations since they are reactive in nature. Threat networks can easily shift their attacks to "softer targets" or change their TTPs to counter friendly ones. Alternatively, *Attack the Network* is a proactive line of operation that focuses on "Left of Boom". It disrupts the IED system through Information Operations and other targeting activities that neutralize key nodes.

The nature of the IED system limits the military's abilities to effectively perform all three lines of C-IED operations. Therefore, to protect and exploit all four instruments of national power, military forces require support from a wide range of agencies and departments. *Understanding and Intelligence* requires national intelligence assets, academic research, and local social-cultural knowledge. *Prepare* needs law enforcement training so forces can adequately develop exploitation skills. *Protect* requires interoperability and common TTPs, especially when working in a coalition. *Prevent* involves law enforcement and intelligence agencies affecting the IED system's critical vulnerabilities, such as finances and leadership. *Prevent* also reduces local support to threat networks by improving local economic and governance conditions, which is the responsibility of foreign affairs and development agencies. *Pursue* means finding, fixing, and finishing the targets. Yet, since IED systems are loose networks, targets can be anywhere in the world, which demands interagency support to identify, arrest, and imprison IED facilitators.

Accomplishing all these tasks requires a common understanding and willingness to cooperate. Common national strategy is instrumental in harnessing joint power. A Whole of Government approach allows a country to synchronize its instruments of national power, improving security, development, and governance. A 3D approach reduces threat networks critical capabilities, particularly local support. Working with allied partners reduces duplication of effort and interoperability issues. Ultimately, multinational cooperation supports unity of effort, an alliance's centre of gravity.

Involving the public sector and international organizations brings unique capabilities such as expert knowledge and networking. These are all key elements to the Comprehensive Approach, which is instrumental to countering the IED threat.

Yet, implementing this strategy is not without its challenges. It can be daunting even within one nation, where different military services, government departments, and agencies are in competition for resources or have difficulties negotiating bureaucratic hurdles. To effectively overcome these challenges, Western governments must establish formal policies for information sharing and synchronizing C-IED efforts. There must also be a fundamental willingness to cooperate between the various key stakeholders. An effective way to improve cooperation is to develop relationships, through liaison officers, training, and other venues to enhance common understanding and strategy. The cost of this approach is minimal compared to the billions spent in MRAPs, UAVs, and other C-IED equipment.

In the end, threat networks know too well how much IEDs impact their enemy's resolve. Therefore, these weapons of strategic influence will remain the greatest threat in stabilization operations. Defeating the IED system requires all agencies to step up and be prepared to support each other. As it takes a network to fight a network, the Comprehensive Approach is the "silver bullet".

BIBLIOGRAPHY

Ackerman, Robert. "Improvised Explosive Devices: A Multifaceted Threat." *Signal Online* 7 (July 2008). https://afceaeurope.org/content/?q=node/1638

Adamson, William G. "An Asymmetric Threat Invokes Strategic Leader Initiative: the Joint Improvised Explosive Device Defeat Organization." Research Project, Washington, D.C.: Industrial College of the Armed Forces, 2007. http://www.scribd.com/doc/26736694/Adamson-Final-Icaf-Research-Paper-Jieddo.

Atkinson, Rick. "The Single Most Effective Weapon Against Our Deployed Forces." *Washington Post*, 30 September 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/09/29/AR2007092900750.html.

Atkinson, Rick. "Left of Boom: The Struggle to Defeat Roadside Bombs." *Washington Post Special Report*, 30 September 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/09/29/AR2007092900750.html.

Bellamy, Chris. *Absolute War: Soviet Russia in the Second World War*. New York: First Vintage Books Edition, 2008.

Bender, Bryan. "Panel on Iraq bombings grows to $3b effort Critics say it has been ineffective." *The Boston Globe*, 25 June 2006, http://www.boston.com/news/world/middleeast/articles/2006/06/25/panel_on_iraq_bombings_grows_to_3b_effort/.

Berkeley, Alfred, Wesley Bush, Philip Heasley, James Nicholson, James Reid, and Michael Wallace. *Intelligence Information Sharing: Final Report and Recommendations*. National Infrastructure Advisory Council, 10 January 2012. http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf.

Berthiaume, Lee. **"**Over 2,000 Canadians were wounded in Afghan mission: report." *National Post*, 1 February 2012. http://news.nationalpost.com/2012/02/01/over-2000-canadians-were-wounded-in-afghan-mission/.

Boston, William. "Norway Attacks: The Worrying Rise of the Lone-Wolf Terrorist." *Time*, 28 July 2011. http://www.time.com/time/world/article/0,8599,2085658,00.html.

Boston, William. "A Killer in Paradise: Inside the Norway Attacks." *Time*, 23 July 2011. http://www.time.com/time/world/article/0,8599,2084835,00.html#ixzz2JJwPxcL7.

Brook, Tom Vanden. "IEDs kill more civilian Afghans in 2010." *USA Today*, 5 August 2010. http://usatoday30.usatoday.com/news/world/afghanistan/2010-08-05-1A casualties05_ST_N.htm.

Brook, Tom Vanden. "IEDs kill 21,000 Iraqi civilians 2005-2010." *USA Today*, 1 December 2011. http://usatoday30.usatoday.com/news/world/iraq/2011-01-12-1Aied12_ST_N.htm

Cadewell, John. *Understanding the Basic of Improvised Explosive Devices*. Enschede: Civil-Military Fusion Centre, 2011.

Carter, Ashton B, and J. Michael Gilmore. "Running the Numbers on MRAPs: Reliable Data Proves the Vehicles are Worth the Money." *Foreign Affairs*, 9 October 2012. http://www.foreignaffairs.com/articles/138172/ ashton-b-carter-and-j-michael-gilmore/running-the-numbers-on-mraps?page=show.

Capehart, Bruce. "Managing Posttraumatic Stress Disorder In Combat Veterans With Comorbid Traumatic Brain Injury." *Journal of Rehabilitation Research & Development* 49, no. 5 (May 2012): 789-812. http://www.rehab.research.va.gov/ jour/2012/495/pdf/capehart495.pdf.

Casciani, Dominic. "Car bomb: The Race for Evidence." *BBC News*, 29 June 2007. http://news.bbc.co.uk/2/hi/uk_news/6253274.stm

Cazzanicca, Gianluca. "IED Defeat: A NATO-Wide Approach." *Military Technology* 34, no. 10 (October 2010):47-52.

Christman Gerald, and Mark Postal. "Coalition Interoperability: a Modeled Approach." Last Accessed 18 February 2013. http://www.dodccrp.org/events/11th_ICCRTS/ html/papers/003.pdf.

Clark, Vincent. "The Future of JIEDDO – The Global C-IED Synchronizer." Naval War College, 31 October 2008. http://www.dtic.mil/cgibin/GetTRDoc? AD=ADA494284.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Prince-ton: Princeton University Press, 1976.

Cordesman, Anthony H. Charles Loi, and Vivek Kocharlakota. "IED Metrics for Afghanistan January 2004 - September 2010." *Centre for Strategic Studies*, November 11, 2010. Last accessed 23 December 2012. http://csis.org/files/publication/101110_ied_metrics_combined.pdf.

Curry, Peter. "Small Wars are Local: Questioning Assumptions about Armed Groups." In *Pirates, Terrorists and Warlords,* edited by Jeffery H. Norwitz, 156-165. New York: Skyhorse Publishing, 2009.

D'Agostino, Davi M. *DOD Should Apply Lessons Learned Concerning the Need for Security over Conventional Munitions Storage Sites to Future Operations Planning*. United States Government Accountability Office: GAO-07-639T, 22 March 2007. http://www.gao.gov/assets/120/115974.pdf.

Dannenbaum, Tom. "Bombs, Ballots, and Coercion: The Madrid Bombings, Electoral Politics, and Terrorist Strategy." *Security Studies* 20, no. 3 (July 2011): 303–349.

Dauber, Cori. "Youtube War: Fighting in a World of Cameras in Every Cell Phone and Photoshop on Every Computer." Monograph, Strategic Studies Institute, 2009.

Day, Adam. "Left Of The Boom." *Legion Magazine*, January 19, 2009. http://www.legionmagazine.com/en/index.php/2009/01/left-of-the-boom/.

Deen, Talif. "UN Pullout from Baghdad Threatens to Undermine U.S." *Inter Press Service*, 31 October 2003. http://www.ipsnews.net/2003/10/politics-un-pullout-from-baghdad-threatens-to-undermine-us/.

Dobkin, Carlos, and Nancy Nicosia, "The War on Drugs: Methamphetamine, Public Health and Crime", *American Economic Review* 99, no. 1 (March 2009): 324-349. http://www.aeaweb.org/articles.php?doi=10.1257/aer.99.1.324

Eisler, David. "Counter IED in Modern War." *Military Review* 9, no. 1 (January-February 2012): 9-15.

Ellis, Richard, Richard Rogers, and Bryan Cochran. "Joint Improvised Explosive Device Defeat Organization (JIEDDO): Tactical Successes Mired in Organizational Chaos; Roadblock in the Counter-IED Fight." Joint Forces Staff College, 13 March 2007. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA473109.

Evans, Gareth "Going to War Against the IED." *Army Technology*, 7 May 2010. http://www.army-technology.com/features/feature84291.

Flynn, Michael T. Matt Pottinger, and Paul Batchelor. "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan." *Voices from the Field*. Washington: Centre for a New American Security, 2010. http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf.

Foust, Joshua. *Five Lessons We Should Have Learned in Afghanistan*. Washington, D.C: American Security Project, 2012. http://americansecurityproject.org/ASP%20Reports/Ref%200066%20-%20Five%20Lessons%20We%20Should%20Have%20Learnt%20In%20Afghanistan.pdf

Gallego, Pablo Esteban Parra. "IEDs: A Major Threat for a Struggling Society." *Journal of ERW and Mine Action* 13, no. 3 (Winter 2009). http://maic.jmu.edu/journal/13.3/specialreport/gallego/gallego.htm.

Gates, Robert. Speech, NATO Headquarters, Brussels, Belgium, March 11, 2011. http://www.defense.gov/speeches/speech.aspx?speechid=1547.

Gelpi, Christopher, Jason Reifler, and Peter Feaver. "Success Matters: Casualty Sensitivity and the War in Iraq." *International Security* 30, no. 3 (Winter 2005/06): 7-46. http://www.mitpressjournals.org/toc/isec/30/3.

Gordon, Michael, and Scott Shane. "The Struggle for Iraq; Behind U.S. Pressure on Iran, Long-Held Worry Over a Deadly Device in Iraq." *The New York Times*, 27 March 2007. http://query.nytimes.com/gst/fullpage.html?res= F40C1EF639540C748EDDAA0894DF404482.

Gould, Joe. "Electronic warfare is more than jamming IEDs." *Defence News*, 11 October 2011. http://blogs.defensenews.com/ausa/2011/10/11/electronic-warfare-is-more-than-jamming-ieds/.

Graham, William H. "Learning From The Enemy – Offensively, What IEDs Should Teach The U.S.," Civilian Research Paper, U.S. Army War College, 2010. http://www.dtic.mil/dtic/tr/fulltext/u2/a545052.pdf.

Grandia, Mirjam, Jan van der Meulen, and Sergio Catigani. "The 3D Approach and Counterinsurgency – A Mix of Defence, Diplomacy And Development: the Case of Uruzgan," Master's Thesis, University of Leiden, 2009. http://www.cimic-coe.org/download/3dandcoin.pdf.

Haims, Marla C., David C. Gompert, Gregory F. Treverton, and Brooke K. Stearns. *Breaking the Failed-State Cycle*. Santa Monica, CA: RAND Corporation, 2008.

Higgins, Michael, Jonathan Rivait, and Andrew Barr. "Blood and Treasure." *National Post*, 22 June 2011. http://afghanistan.nationalpost.com/graphic-blood-treasure/.

Hillier, Rick. *A Soldier First: Bullets, Bureaucrats and the Politics of War*. Toronto: HarperCollins Publishers, 2009.

Hilton, Craig. "Shaping Commitment: Resolving Canada's Strategy Gap in Afghanistan and Beyond." *Strategic Studies Institute Paper*. Carlisle: U.S. Army War College, 2007. http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubid=799.

Hope, Ian. *Dancing with the Dushman: Command Imperatives for the Counter-Insurgency Fight in Afghanistan*. Kingston: Canadian Defence Academy Press, 2008.

Hsu, Spencer and Mary Beth Sheridan. "IEDs Seen As Rising Threat in The U.S." *Washington Post*, 20 October 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/10/19/AR2007101902703.html?hpid=topnews

Johnson, Andrew. "Taliban make 'undetectable' bombs out of wood." *The Independent*, 10 January 2010. http://www.independent.co.uk/news/world/asia/taliban-make-undetectable-bombs-out-of-wood-1863353.html.

Johnson, Charles. *U.S. Agencies Face Challenges Countering the Use of Improvised Explosive Devices in the Afghanistan/Pakistan Region*. United States Government Accountability Office: GAO-12-907T, 12 July 2012. http://www.gao.gov/products/GAO-12-907T.

Kalsoom, Lakhani. "Indoctrinating Children: The Making of Pakistan's Suicide Bombers." *CTC Sentinel* 3, no. 6 : 11-13. http://www.ctc.usma.edu/wp-content/uploads/2010/08/CTCSentinel-Vol3Iss6-art4.pdf.

Kem, Jack. "Understanding the operational environment: the expansion of the DIME." *Military Intelligence Professional Bulletin* 32, no. 2 (April-June 2007): 49-53. http://www.fas.org/irp/agency/army/mipb/2007_02.pdf

Kilcullen, David. "Countering Global Insurgency." *Journal of Strategic Studies* 28, no. 4 (August 2005): 597-617.

Kilcullen, David J. "Twenty-Eight Articles: Fundamentals of Company-Level Counterinsurgency." *Marine Corps Gazette* (October 2007): 59–61.

King, Christopher A., Robert Bienvenu, and T. Howard Stone. "HTS Training and Regulatory Compliance for Conducting Ethically-Based Social Science Research." *Military Intelligence Professional Bulletin* 37, no. 4 (October-December 2011): 16-20. http://www.fas.org/irp/agency/army/mipb/2011_04.pdf.

Kowalski, Peter. *Counter – Improvised Explosive Device (C-IED) Capability Package to the NATO Response Force*. NATO Consultation, Command, and Control Agency: file NC3A-BE/ACQ/ASG/12/ 0492, 4 June 2012. http://www.defensa.gob.es/Galerias/info/servicios/concursos/ 2012/06/MS-13500-NRF.pdf.

Krepinevich, Andrew and Dakota Wood. *Of IEDs and MRAPs: Force Protection in Complex Irregular Operations*. Washington, D.C.: Center for Strategic and Budgetary Assessments, 2007. http://www.csbaonline.org/publications/2007/10/of-ieds-and-mraps-force-protection-in-complex-irregular-operations/.

Lamb, Christopher J., and Sally Scudder, "Why the MRAP Is Worth the Money: Dispelling the Flawed Logic of One Battlefield Study." *Foreign Affairs*, 23 August 2012, http://www.foreignaffairs.com/articles/138049/christopher-j-lamb-and-sally-scudder/why-the-mrap-is-worth-the-money?page=show.

Lamb, Christopher J., Matthew J. Schmidt, and Berit G. Fitzsimmons. "MRAPs, Irregular Warfare, and Pentagon Reform." Institute for National Strategic Studies, National Defense University, 2009. http://usacac.army.mil/cac2/cgsc/sams/media/MRAPs.pdf.

Larence, Eileen. *Progress Made and Challenges Remaining in Sharing Terrorism-Related Information*. United States Government Accountability Office: GAO-12-144T, 12 October 2012. http://www.gao.gov/products/GAO-12-144T.

Lawrence, Thomas E. *Seven Pillars of Wisdom: A Triumph*. Oxford: Alden Press, 1952.

Leslie, Andrew, Peter Gizewski, and Michael Rostek. "Developing a Comprehensive Approach to Canadian Forces Operations." *Canadian Military Journal* 9, No. 1 (Spring 2008): 11-20.

Long, Austin. *On "Other War" Lessons from Five Decades of RAND Counterinsurgency Research.* Santa Monica, CA: RAND Corporation, 2006.

Mackinlay, John. *Globalization and Insurgency*. New York: Oxford University Press, 2002.

Manley, John, D. Burney, J. Epp, P. Tellier, P. Wallin. *Independent Panel on Canada's Future Role in Afghanistan*. Ottawa: Public Works and Government Services, 2008.

Martin, Rachel. "The IED: The $30-Bombs That Cost The U.S. Billions." *NPR*, 17 December 2011. http://www.npr.org/2011/12/18/143902421/in-iraq-fighting-an-improvised-war.

McBride, Robert. "Improvised Explosive Devices: Why They Are Used And Our Failure To Defeat Them." Master's Thesis, Canadian Forces College, 2010.

McChrystal, Stanley. "It Takes a Network." *Foreign Policy*, 21 February 2011. http://www.foreignpolicy.com/articles/2011/02/22/it_takes_a_network.

McFate, Montgomery, and Steve Fondacaro. "Reflections on the Human Terrain System During the First 4 Years." *Prism* 2, no. 4 (September 2011): 63-82. http://www.ndu.edu/press/lib/images/prism2-4/Prism_63-82_McFate-Fondacaro.pdf.

Moores, Lawrence W. “T.E. Lawrence: Theorist and Campaign Planner,” Monograph, US Army Command and General Staff College, 1992.

Murphy, David. *Lawrence of Arabia: Leadership, Strategy and Conflict*. Oxford: Osprey Publishing, 2011.

Murphy, David. *The Arab Revolt 1916-1918: Lawrence Sets Arabia Ablaze*. Oxford: Osprey Publishing, 2008.

Nolin, Pierre Claude. *Countering the Afghan Insurgency: Low-Tech Threats, High-Tech Solutions*. NATO Parliamentary Assembly Special Report: 189 STC 11 E Bis Final, October 2011. http://www.nato-pa.int/default.asp?SHORTCUT=2551.

Nordeste, Bruno and D. Carment. “Trends in Terrorism Series: A Framework for Understanding Terrorist Use of the Internet.” *ITAC* 2 (2006): 1-21. http://www.carleton.ca/cifp/app/serve.php/1121.pdf.

Osborn, Kris. “Firms work to stay a step ahead of EFP threat.” *Army Times*, 18 May 2008. http://www.armytimes.com/news/2008/05/army_beating_efp_051908w/.

Perry, Tony. “Afghanistan's most loyal troops.” *Los Angeles Times*, 8 February 2011. http://articles.latimes.com/2011/feb/08/nation/la-na-war-dogs-20110208.

Pugliese, David. “34 Canadian Forces Vehicles Destroyed, 359 Damaged During Afghan War.” *Ottawa Citizen*, 19 July 2012. http://blogs.ottawacitizen.com/2012/07/19/34-canadian-forces-vehicles-destroyed-359-damaged-during-afghan-war-list-includes-3-leopard-tanks-destroyed/.

Pugliese, David. “More Counter-IED Equipment and Protected Vehicles Being Sent to British Forces in Afghanistan.” *Ottawa Citizen*, 23 December 2011. http://blogs.ottawacitizen.com/2011/12/23/more-counter-ied-equipment-and-protected-vehicles-being-sent-to-british-forces-in-afghanistan/.

Rayment, Sean. “Commanders to Change Bomb Disposal Tactics.” *The Telegragh*, 12 February 2011. http://www.telegraph.co.uk/news/uknews/defence/8320560/Commanders-to-change-bomb-disposal-tactics.html

Rayment, Sean. *Bomb Hunters.* London: Harper Collins, 2011.

Rohlfs, Chris, and Ryan Sullivan. “The MRAP Boondoggle: Why the $600,000 Vehicles Aren't Worth the Money.” *Foreign Affairs*, 26 July 2012. http://www.foreignaffairs.com/articles/137800/chris-rohlfs-and-ryan-sullivan/the-mrap-boondoggle.

Roosevelt, Ann. “IEDs Are Strategic Weapons, General Says.” *Defense Daily* 238, no. 58 (June 2008).

Sageman, Marc. *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press, 2004.

Schnaubelt, Christopher M. "The Challenges to Operationalizing a Comprehensive Approach." In *Operationalizing a Comprehensive Approach in Semi-Permissive Environments*, edited by Christopher M. Schnaubelt. Rome: NATO Defense College, 2009.

Shah, Saeed. "Suicide car bomb in Afghanistan kills 14 primary school children." *The Guardian*, 28 December 2008. http://www.guardian.co.uk/world/2008/dec/28/suicide-car-bomb-attack-afghanistan.

Shalizi, Hamid. "Coordinated Kabul suicide attack targets government building." *Reuters*, 21 January 2013. http://www.reuters.com/article/2013/01/21/us-afghanistan-blast-idUSBRE90K03120130121.

Singer, Peter. "The Evolution of Improvised Explosive Devices (IEDs)." *Armed Forces Journal*, February 2012. http://www.brookings.edu/research/articles/2012/02/improvised-explosive-devices-singer.

Smith, Adam, Roscoe Bartlett and Silvestre Reyes. *Counter-Improvised Explosive Devices: Multiple DOD Organizations are Developing Numerous Initiatives*. United States Government Accountability Office: GAO-12-861R, 1 August 2012. http://www.gao.gov/products/GAO-12-861R.

Travers, Patrick, and Taylor Owen. "Peacebuilding While Peacemaking: The Merits of a 3D Approach in Afghanistan." UBC Center for International Relations Security and Defense Forum Working Paper #3, University of British Columbia, 2007. http://cicam.ruhosting.nl/teksten/act.07.grotenhuis.owen%20paper.pdf.

Wendling, Cécile. *The Comprehensive Approach to Civil-Military Crisis Management: A Critical Analysis and Perspective*. Paris: Institut de recherche stratégique de l'École militaire, 2010. http://www.humansecuritygateway.com/documents/IRSEM_TheComprehensiveApproachtoCivilMilitaryCrisisManagement.pdf.

Whitlock, Craig. "Number of U.S. Casualties from Roadside Bombs in Afghanistan Skyrocketed from 2009 to 2010." *Washington Post*, 25 January 2011. http://www.washingtonpost.com/wp-dyn/content/article/2011/01/25/AR2011012506691.html.

Windsor, Lee, David Charters, and Brett Wilson. *Kandahar Tour: The Turning Point in Canada's Afghan Mission.* Mississauga: John Wiley & Sons, 2008.

Winter, Phil, Alex Meiliunas, and Steve Bliss. "Countering the Improvised Explosive Devices Threat." *United Service Journal* 59**,** no. 3 (September 2008): 9-11.

Zorpette, Glenn. “Countering IEDs.” *IEEE Spectrum* 45, no. 9 (September 2008): 26-35. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04607910.

Angus-Reid. “Britons and Canadians Oppose Afghan War; Americans Evenly Divided.” Last accessed 7 January 2013. http://www.angus-reid.com/polls/43776/britons-and-canadians-oppose-afghan-war-americans-evenly-divided/.

Canadian Broadcasting Corporation. “Canada's Military Mission in Afghanistan: Training Role to Replace Combat Mission in 2011.” *CBC News*, 10 February 2009. Last accessed 23 December 2012.http://www.cbc.ca/news/canada/story/2009/02/10/f-afghanistan.html.

Canadian Broadcasting Corporation. “Fewer Canadians 'strongly approve' of Afghan mission: survey.” *CBC News*, 9 November 2006. Last accessed 29 January 2013. http://www.cbc.ca/news/canada/story/2006/11/08/afghanistan-survey.html.

Cable News Network. “CNN/ORC Poll – March 24-25 – Afghanistan.” *CNN*, March 30, 2012. Last accessed 7 January 2013. http://i2.cdn.turner.com/cnn/2012/images/03/29/rel3f.pdf.

Cable News Network. “Afghan car bomb kills 14 children.” *CNN*, December 28, 2008. Last accessed 7 January 2013. http://www.cnn.com/2008/WORLD/asiapcf/12/28/afghan.carbomb/index.html.

Egmont Group. “About the Egmont Group.” Last accessed 7 January 2013. http://www.egmontgroup.org/

General Dynamics Land System. “MRAP Family.” Last accessed on 24 February 2013. http://www.gdls.com/index.php/products/mrap-family.

Icasualties.org. *Operation Enduring Freedom* (2013). Last accessed 7 January 2013. http://icasualties.org/OEF/index.aspx.

International Institute for Strategic Studies. “IEDs: The Home-Made Bombs that Changed Modern War.” *Strategic Comments* 18, no. 24 (August 2012): 1-4. http://www.iiss.org/publications/strategic-comments/past-issues/volume-18-2012/.

INTERPOL. “INTERPOL supports international training course on countering homemade explosives.” Last accessed on 4 March 2013. http://www.interpol.int/News-and-media/News-media-releases/2012/N20121024Bis.

INTERPOL. “New unit to assist INTERPOL member countries combat chemical and explosives terrorism.” Last accessed on 4 March 2013. http://www.interpol.int/News-and-media/News-media-releases/2012/N20120918ter.

Military Technology. "We Will Defeat the IED." *Military Technology* 32, no. 10 (October 2008): 20-27.

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

The Canadian Press. "One Bomb, Many Lives: the Destruction of Call Sign 4-2 Charlie." Last accessed 23 December 2012, http://www.cbc.ca/news/background/afghanistan/cp-one-bomb.html.

University of Waterloo. "Engineering Under Fire." Last Accessed 23 December 2012. https://info.uwaterloo.ca/www/profiles/profile.php?id=103.

Canada. Department of National Defence. Canadian Forces Joint Publication 3.15, *Counter Improvised Explosive Devices Operations.* Ottawa: DND Canada, 2012.

Canada. Department of National Defence. B-GL-300-003/FP-001, *Command in Land Operations.* Ottawa: DND Canada, 2007.

Canada. Department of National Defence. *Canada First Defence Strategy.* Ottawa: DND Canada, 2008.

Canada. Financial Transactions and Reports Analysis Centre of Canada. "Who We Are." Last accessed 23 December 2012. http://www.fintrac.gc.ca/fintrac-canafe/1-eng.asp.

Canada. Royal Canadian Mounted Police. "Explosives Disposal and Technology Section." Last accessed 23 December 2012. http://www.rcmp-grc.gc.ca/fs-fd/edts-sete-eng.htm.

Canada. Government of Canada. *Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy*. Ottawa: Library and Archives Canada, 2011.

Canada. Government of Canada. *Canada's Engagement in Afghanistan - Fourteenth and Final Report to Parliament*. Ottawa: Library and Archives Canada, 2012.

Canada. Government of Canada. *Canada's International Policy Statement: A Role of Pride and Influence in the World, Overview*. Ottawa: Department of Foreign Affairs and International Trade, 2005.

Canada. Government of Canada. "Cost of the Afghanistan Mission 2001-2011." Last accessed 7 January 2013. http://www.afghanistan.gc.ca/canada-afghanistan/news-nouvelles/2010/2010_07_09.aspx?view=d.

North Atlantic Treaty Organization. Allied Command Transformation C-IED Integrated Project Team. "(NU) ACT C-IED IPT Briefing to COE C-IED, 18 Jan 2011." NATO Joint Operational Planning Group Campaign Plan, 2012.

North Atlantic Treaty Organization. Allied Command Transformation. *(NU) Commanders' and Staff Handbook for Countering Improvised Explosive Devices*. Norfolk: NATO, 2011.

North Atlantic Treaty Organization. NATO C-IED.org. "Community Partners." Last accessed on 26 February 2013. https://www.c-ied.org/en-us/community.aspx.

North Atlantic Treaty Organization. NATO C-IED.org. "Counter Improvised Explosive Device (C-IED) Courses / Training." Last accessed on 26 February 2013. https://www.c-ied.org/Training/Courses.aspx.

North Atlantic Treaty Organization. Explosive Ordnance Disposal Centre of Excellence. *EOD and IED Terminology Database*. Trenčín: EOD COE, 2012. https://www.eodcoe.org/data_web/editor_data/file/terminology%20posledne.pdf.

North Atlantic Treaty Organization. NATO Multimedia Library. "Countering Improvised Explosive Devices." Last Accessed 17 February 2013. http://www.nato.int/cps/en/natolive/topics_72809.htm.

North Atlantic Treaty Organization. NATO Multimedia Library. "NATO Centres of Excellence." Last accessed 10 February 2013. http://www.nato.int/cps/en/natolive/topics_68372.htm.

North Atlantic Treaty Organization. NATO Multimedia Library. "NATO Response Force." Last accessed 1 March 2013. http://www.nato.int/cps/en/natolive/topics_49755.htm.

North Atlantic Treaty Organization. NATO Standardization Agency. Allied Joint Publication (AJP)-01(D). *(NU) Allied Joint Doctrine*. Brussels: NATO, 2010.

North Atlantic Treaty Organization. NATO Standardization Agency. Allied Joint Publication (AJP)-3.15(A). *(NU) Allied Joint Doctrine For Countering Improvised Explosive Devices*. Brussels: NATO, 2011.

United Kingdom. Home Department, *CONTEST: The United Kingdom's Strategy for Countering Terrorism*. London: The Stationary Office Limited, 2011.

United Kingdom. Ministry of Defence. *Joint Doctrine Note 4/05: The Comprehensive Approach*. Shrivenham: Joint Doctrine & Concepts Centre, 2006.

United Kingdom. Ministry of Defence. "UK Forces: Operations in Afghanistan." Last accessed 7 January 2013. https://www.gov.uk/uk-forces-operations-in-afghanistan.

United Nations. United Nations Assistance Mission in Afghanistan. *Afghanistan Annual Report 2011: Protection of Civilians in Armed Conflict*. Kabul: UNAMA, 2012. http://unama.unmissions.org/Portals/UNAMA/Documents/UNAMA%20POC%202011%20Report_Final_Feb%202012.pdf.

United Nations. United Nations Office of Drugs and Crime. "The Global Project on Strengthening the Legal Regime Against Terrorism." Last accessed on 4 March 2013. http://www.unodc.org/unodc/en/terrorism/UNODC_Role/Global_Project.html.

United Nations. UN Secretary-General. *The Situation in Afghanistan and its Implications for International Peace and Security.* Report of the Secretary-General: A/65/873-S/2011/381, 23 June 2011. http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Afgh%20S%202011%20381.pdf.

United States. Central Intelligence Agency. "CIA World Factbook: Afghanistan." Last accessed on 7 March 2013. https://www.cia.gov/library/publications/the-world-factbook/geos/af.html.

United States. Department of Defense. *Al-Shabaab's Exploitation of Alternative Remittance Systems (ARS) in Kenya*. Norfolk: Joint Improvised Explosive Device Defeat Organization, 2009. http://info.publicintelligence.net/JIEDDO-AlShabaabARS.pdf.

United States. Department of Defense. *Attack the Network: An Innovation Project*. Norfolk: Joint Improvised Explosive Device Defeat Organization, 2010. https://transnet.act.nato.int/WISE/JKnIFE/IEDDRefere/IEDDRefere.

United States. Department of Defense. *Commander's Handbook to Attack the Network Operations*. Suffolk: Joint Force Command coalition Warfare Centre, 2011. https://transnet.act.nato.int/WISE/JKnIFE/IEDDRefere/IEDDRefere.

United States. Department of Defense. *Counter Improvised Explosive Device Strategic Plan 2012-2016*. Norfolk: Joint Improvised Explosive Device Defeat Organization, 2012. https://www.jieddo.mil/content/docs/20120116_JIEDDOCIEDStrategicPlan_MEDprint.pdf.

United States. Department of Defence. *JIEDDO Global IED Monthly Summary Report* Norfolk: Joint Improvised Explosive Device Defeat Organization, 2012. http://publicintelligence.net/jieddo-global-ieds-aug-2012/.

United States. Department of Defense. *Joint Improvised Explosive Device Defeat Organization (JIEDDO)*. DoD Directive: 2000.19E, 14 February 2006. http://www.dtic.mil/whs/directives/corres/pdf/200019p.pdf.

United States. Department of Defense. *Joint Improvised Explosive Device Defeat Organization 2010 Annual Report.* Norfolk: Joint Improvised Explosive Device Defeat Organization, 2011. https://www.jieddo.mil/content/docs/JIEDDO_2010_Annual_Report_U.pdf.

United States. Department of Defense. Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*. Washington, D.C: Joint Chiefs of Staff, 2012.

United States. Department of Defense. Joint Publication 2-01.3, *Joint Intelligence Preparation of the Operational Environment*. Washington, D.C: Joint Chiefs of Staff, 2009.

United States. Department of Defense. Joint Publication 3-15.1, *Counter-Improvised Explosive Device Operations*. Washington, D.C: Joint Chiefs of Staff, 2012.

United States. Department of Defense. *Victim Operated Improvised Explosive Devices (VOIED) Recognition Guide – Afghanistan.* Norfolk: Joint Improvised Explosive Device Defeat Organization, 2011. http://info.publicintelligence.net/JIEDDO-VOIED.pdf.

United States. Department of Homeland Security. *IED Attack: Improvised Explosive Devices.* Washington, DC: The National Academies Press, 2007. http://www.dhs.gov/xlibrary/assets/prep_ied_fact_sheet.pdf.

United States. Department of State. *Country Reports on Terrorism 2011*. CRT12, July 2012. http://www.state.gov/j/ct/rls/crt/2011/.

United States. Federal Bureau of Investigation. "Terrorist Explosive Device Analytical Center (TEDAC)." Last accessed 23 December 2012. http://www.fbi.gov/about-us/lab/tedac.

United States. Headquarters of Department of the Army. FM 3-07, *Stabilization Operations*. Washington: US Department of the Army, 2008.

United States. Headquarters of Department of the Army. FMI 3-34.119/MCIP 3-17.01, *Improvised Explosive Device Defeat*. Washington: US Department of the Army, 2008.

United States. House of Representatives Committee on International Relations. *Hezbollah's Global Reach*. Washington, DC: U.S. Government Printing Office, 2006. www.democrats.foreignaffairs.house.gov/archives/109/30143.pdf.

United States. House of Representatives Subcommittee on Oversight & Investigations. *The Joint Improvised Explosive Device Defeat Organization: DOD's Fight Against IEDs Today and Tomorrow*. Washington, DC: U.S. Government Printing Office, 2008. http://www.fas.org/irp/congress/2008_rpt/jieddo.pdf.

United States. National Counterterrorism Center. *Report on Terrorism 2011*. Washington, DC: Office of the Director of National Intelligence, 2012. http://www.nctc.gov/docs/2011_NCTC_Annual_Report_Final.pdf.

United States. National Counterterrorism Center. *Worldwide Incident Tracking System Database 2011*. Washington, DC: Office of the Director of National Intelligence, 2012. http://wits.nctc.gov/.

United States. National Geospatial-Intelligence Agency. *NGA Strategy 2013-2017*. Springfield: National Geospatial Intelligence Agency, 2012. https://www1.nga.mil/About/NGAStrategy/Documents/19639_NGA%20Strat%20Pub_Public_Web.pdf.

United States. National System Geospatial for Intelligence. Directive NSGD FM 1100, *Roles and Responsibilities of the Department of Defense (DoD) Geospatial Intelligence (GEOINT) Manager and Intelligence Community (IC) Functional Manager (FM) for GEOINT*. Fort Belvoir: National Geospatial-Intelligence Agency, 2011. http://www.gwg.nga.mil/documents/fm1100.pdf.

United States. White House. *Countering Improvised Explosive Devices*. Washington, DC: White House, 2013.http://www.whitehouse.gov/sites/default/files/docs/cied_1.pdf.

United States. White House. *National Strategy for Counterterrorism*. Washington, DC: White House, 2011. http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf.

United States. White House. *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*. Washington, DC: White House, 2007. http://www.fas.org/sgp/library/infoshare.pdf.

United States. White House. *The Comprehensive National Cybersecurity Initiative*. Washington, DC: White House, 2010. http://www.fas.org/irp/eprint/cnci.pdf.

World Customs Organization. United States Immigration and Customs Enforcement. *Project Global Shield Final Report*. Brussels: WCO Secretariat, 2011. https://www.c-ied.org/Portals/0/Documents/projects/MaritimeInitiative/MCIEDCoIConference/Sept-2011-Report-GlobalShield.pdf.