CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
JCSP 36 / PCEMI 36

MASTER OF DEFENCE STUDIES

THE NEED FOR A WHOLE-OF-GOVERNMENT APPROACH TO COUNTER-IED OPERATIONS

By/par Maj C.R. Henderson

Word Count: 13673

Compte de mots : 13673

CONTENTS

Table of Contents i

List of Figures ii

Chapter

1. Introduction 1

2. Background – C-IED 101 6

3. Counter-IED as a Sub-Set of COIN 16

4. Gaining the Upper Hand: Whole-of-Government Opportunities In the Defeat the Device and Attack the Network Lines of Operation 33

5. Discussion: If We Build It, Will They Come? 48

6. Conclusion 58

Bibliography

List of Figures

Figure 3.1: Systems Perspective of the Operational Environment
Figure 3.2: Nodes and Links of an Adversary System
Figure 3.3: Unified Action
Figure 3.4: Range of Popular Support
Figure 3.5: IED Defeat Concept of Ops
Figure 3.6: Functional Flow Diagram of a Terrorist Attack
Figure 3.7: IED Lexicon Construct

CHAPTER 1 - INTRODUCTION

Contact, I-E-D. Wait, out.
- Solider under contact

Since the beginning of Canada's deployment to Afghanistan as part of the Global War On Terrorism (GWOT), the type of radio transmission above has been ominously heard countless times over Canadian combat net radio to indicate yet another equipment and/or personnel victim to a seemingly new and pervasive threat - the Improvised Explosive Device (IED). These devices have been responsible for approximately 75% of Canada's combat deaths in Afghanistan[1] and they continue to be a persistent threat. Indeed, IED strikes have been a significant threat in both the Afghanistan and Iraq theatres of operation from the outset of the current coalition campaigns in these countries.[2] With IEDs accounting for such a high proportion of combat casualties, why hasn't Canada, and its allies, found a viable counter-measure and why do IEDs continue to be widely employed throughout Afghanistan, Iraq and other conflict areas around the world.[3]

To date, the United States (US) and its close allies have spent billions of dollars in efforts to provide adequate force protection, countermeasures and intelligence to defeat these weapons.[4] Despite these efforts, coalition forces continue to fall victim to these

---

[1] Department of National Defence, "Fallen Canadians," Department of National Defence, http://www.forces.gc.ca/site/news-nouvelles/fallen-disparus/index-eng.asp (accessed May 19, 2010).

[2] Joint Improvised Explosive Device Defeat Organization, "About JIEDDO," US Department of Defense, https://www.jieddo.dod.mil/about.aspx (accessed April 22, 2010).

[3] Staff, "Israel Finds another IED Along Eqyptian Border," *World Tribune*April 9, 2010, http://www.worldtribune.com/worldtribune/WTARC/2010/me_israel0297_04_09.asp.

[4] US Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: US Department of Defense, 2006), 64.

weapons of choice. The research undertaken in Canada, the US, and other allied countries has led to some technological breakthroughs in mitigating the effects of these devices, but it has also clearly indicated that in order to both understand these weapons and how to counter them, we need to have a solid grasp of not only the nature of these weapons, but also the groups who employ them.[5]

When coalition forces develop an improved personal or equipment armour system, the enemy builds bigger bombs to defeat them. Furthermore, when coalition forces develop a new tactic, technique or procedure to reduce the threat of IEDs, the enemy subsequently changes his own tactics, techniques or procedures to counter those of the coalition. It is this lethal game of cat and mouse that dominates the realities of operating in an IED environment, and which has led Canada and its allies to take a broader view in addressing the threat. While seemingly straight forward in concept, the Counter-IED (C-IED) effort has proven to demand more than a traditional military approach, and more significantly, traditional military solutions. Similar with those lessons learned over time which deal with how to fight an enemy that lives, fights and hides within the same population in which coalition forces are charged to protect and re-build, the C-IED fight also requires the skills and capacities from all applicable agencies of national power.[6]

The current counterinsurgency (COIN) campaigns in Afghanistan and Iraq have brought to the fore the concept of interagency or whole-of-government (WoG) approaches to COIN operations. While not a unique concept to these campaigns,

---

[5] Joint Improvised Explosive Device Defeat Organization, *About JIEDDO*

[6] John A. Nagl, *Learning to Eat Soup with a Knife* (Chicago, IL: University of Chicago Press, 2005), 28-29.

coalition forces have had to re-learn interagency operations lessons learned from earlier COIN campaigns, such as those in Malaya and Vietnam. Like the British and US experiences in those campaigns, coalition forces in Afghanistan and Iraq have identified the need to avoid heavy-handed, traditional and solely military responses to the use of IEDs as a weapon of choice.[7] Like other military operations within an overarching COIN effort, C-IED operations require a nuanced approach that is deliberate, yet subtle and which falls within the scope of an overall strategy or campaign plan.[8]

If the IED threat and C-IED operations are understood within the context of insurgency and counterinsurgency operations, the need for an adaptive, responsive and comprehensive effort can then be understood. This thesis will argue that it is within these C-IED lines of operation that Canada must apply a WoG approach to its C-IED efforts and that Canada must develop and maintain a sustained WoG C-IED capability now and into the future.

In order to fully develop this thesis, the paper will discuss the essence of C-IED in the context of COIN operations in a complex Contemporary Operating Environment (COE) to understand the linkages between C-IED and traditional COIN approaches. Once these linkages are established, the analysis will develop the WoG argument. To establish a baseline understanding of C-IED theory and concepts, chapter 2 of this paper will present doctrinal definitions of relevant C-IED terminology. It will further define key C-IED operational concepts which will set the stage for subsequent discussions of relevant capacities from appropriate government departments that are necessary to produce desired effects on the ground. This will be achieved by using a commonly

---

[7] *Ibid*., 29

[8] *Ibid*., xvi

accepted approach which has been developed by Canadian and allied C-IED research, initiatives, trials and errors. This approach is that the C-IED fight must be along three lines of operation: Attack the Network, Defeat the Device and Prepare the Force.[9]

In Chapter 3 this paper will establish the linkages between C-IED and COIN within the complex COE. That discussion will commence with presenting the COE from a systems theory perspective to assist in describing the multiple and related facets of the COE. COIN operations within the complex COE will then be discussed to highlight the need for non-traditional and comprehensive approaches to COIN given the characteristics of the COE. Finally, C-IED operations will be presented as a sub-set of COIN operations and substantiate the similar need for a comprehensive, or whole-of-government, approach to C-IED as part of COIN operations. With this link established between C-IED and COIN operations, chapter 4 will present examples of areas within the C-IED concept of operations, defined in chapter 2, where there is potential for WoG collaboration in C-IED. Finally, chapter 5 will discuss some options for Canada to consider in order to institutionalize a WoG approach to C-IED and ensure that Canada truly capitalizes from its C-IED efforts in support of operations in Afghanistan.

While the Prepare the Force line of operation plays a critically important role in preparing our troops for operations in an IED environment, it is the lessons and knowledge learned within the Attack the Network and Defeat the Device lines of operation that will feed required inputs into force preparation. With no single technological development capable of eliminating the threat of a dedicated, cunning and intelligent insurgent emplacing an IED, the close interrelationship of the Attack the

[9] NATO Joint Warfare Centre, "Joint Opeational Guideline for Counter-IED" (Draft Publication, Stavanger, Norway, 2008), 9.

Network and Defeat the Device lines of operation appear to be the best avenue in which to have any reasonable expectation of mitigating and minimizing the IED threat. With this in mind, the Attack the Network and Defeat the Device lines of operation will be the focus of this paper.

CHAPTER 2 – BACKGROUND – C-IED 101

The intent of this chapter is to provide a common baseline understanding of C-IED operations. IEDs will first be placed in some historical context, followed by doctrinal definitions of key C-IED lexicon terminology. With this established the chapter will then transition into an explanation of key C-IED operational concepts used to address the IED threat. This chapter set the stage for subsequent discussion on C-IED within the context of COIN in a complex COE.

Context

Despite the current focus and attention on the IED threat, these weapons are not something new. Although sometimes referred to by other names such as booby traps, roadside bombs, suicide bombers, pipe bombs, etc, these are all types of improvised explosives, or IEDs. Indeed, even the hijacked planes of September 11, 2001 could be viewed as IEDs in a general sense of the term. While the label IED may be a new term in the security threat lexicon, improvised explosives have been a constant threat to military forces and civilian populations for years. However, what has changed is the nature of conflict environments.

The Contemporary Operating Environment (COE) and the projected Future Security Environment (FSE) are characterised by failed and failing states, state and non-state actors, and predominantly intrastate, vice interstate, conflict.[10] These security environments are, and are likely to remain for the foreseeable future, arenas where conflict is played out on the global stage due to the global reach of media. These factors

[10] Department of National Defence, *Canada First Defence Strategy* (Ottawa, ON: Government of Canada,[2008]), 6, http://www.forces.gc.ca/site/focus/first-premier/June18_0910_CFDS_english_low-res.pdf (accessed January 8, 2010).

play a direct role in the resultant preference for the use of IEDs by belligerent forces.[11] To better understand why this is so, the nature and types of IEDs will be discussed.

Definitions

The Canadian Forces (CF) define IEDs as "a device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract."[12] This definition is consistent with that articulated by the North Atlantic Treaty Organization (NATO)[13], and both organizations further stipulate that IEDs can be based around military munitions, but they are normally based around commercial or household components.[14] In addition, IEDs have common design components that include some form of initiation system or fuse, a detonator, an explosive charge, a power supply, and some form of container for the device.[15] Although IEDs share common design characteristics, they can be employed in various ways.

Coalition operations in Afghanistan and Iraq have experienced numerous types of IED employment methods, or means of delivery. However, IEDs can be generally grouped into the following, but not exhaustive, list of categories:[16]

Suicide operated IED: These IEDs are borne on the IED operator and are

---

[11] Joint Improvised Explosive Device Defeat Organization, *About JIEDDO*

[12] Department of National Defence, "Canadian Forces Joint Doctrine Note: Canadian Forces Improvised Explosive Device (IED) Lexicon - DRAFT" (Joint Doctrine Note, Ottawa, 2007), 3.

[13] NATO Joint Warfare Centre, *Joint Opeational Guideline for Counter-IED*, 4.

[14] Department of National Defence, *Canadian Forces Joint Doctrine Note: Canadian Forces Improvised Explosive Device (IED) Lexicon - DRAFT*, 3.

[15] NATO Joint Warfare Centre, *Joint Opeational Guideline for Counter-IED*, 5.

[16] *Ibid*.

detonated at the place and time of the bomber's choosing. It is the most discriminate type of IED as the bomber directly controls when and where the device is initiated.

Command operated IED: Similar to a suicide IED, command operated IEDs are initiated at the time and place of the bomber's choosing. However, the bomber is located away from the device. The bomber can initiate the device by way of a command wire leading from the bomber to the device, a simple wire system, or some form of remote control system such as a radio signal or cellular phone signal.

Victim operated IED: These IEDs are initiated by the victim and are the most indiscriminate form of IED as they are generally left unattended once emplaced, and their initiation is not controlled. These IEDs can be initiated by pressure (a soldier or civilian stepping on the initiator), pressure release, tension release, passive or active infrared sensors, trip wire, light sensitive initiation systems, tilt, proximity fuses, etc.

Time controlled IED: These IEDs are initiated by way of some form of timed initiation mechanism. These mechanisms can be mechanical, electronic, chemical or igniferous. Some time controlled IEDs found in Afghanistan, for example, have been based on simple wind-up alarm clock initiation systems.

Projected IED: These IEDs usually take the form of an improvised mortar or rocket and will have some form of initiation system like a command wire or time controlled mechanism.

With no real limits placed on the exact scope and nature of IED employment, other than the imagination and ingenuity of those who employ them, IEDs are a very simple and extremely effective weapon. Indeed, IEDs can be referred to as a tactical weapon with strategic consequences.[17] Insurgents in Afghanistan and Iraq have access to the internet and are able to follow the internal politics of countries contributing troops to the coalitions in those countries. One common thread within the coalitions is a national sensitivity to large numbers of deaths due to operations. With this in mind, IEDs are an extremely effective way not only to strike fear and anxiety among coalition combat troops, but also among parent country populations and, therefore, their parent governments. Due to this nature or second order effect of IEDs, coalition experience in Afghanistan and Iraq has shown that the vast majority of IEDs are emplaced and employed by organized networks and cells of insurgents, more so than by disgruntled individual local nationals.[18]

Typically, these networks stretch from the strategic to tactical levels with key functions being carried out at each level. The networks are generally non-linear in nature with several key nodes each supporting the overall network. At the strategic level of a well-organized IED network, typical functions performed at this level could include funding, planning, training, logistics support and overall resource allocation. At the tactical level, typical functions could include the provision of local leadership and direction on specific IED employment plans, bomb making, delivery of the completed IEDs or its components, IED emplacement, IED initiation and IED event exploitation.[19]

---

[17] Joint Improvised Explosive Device Defeat Organization, *About JIEDDO*

[18] *Ibid*.

Of note at the strategic level of IED networks, the key components at this level generally operate in a decentralized organization bound together by a common ideology. Like seen in other insurgent or terrorist networks, this tends to lend greater security to the network, more efficient planning and greater flexibility.[20]

The strategic through tactical levels of an IED network combine to make an IED system. Within these systems, there are some common elements that exist in most structured and organized IED networks:[21]

> Leadership: A person or group that provides overall direction and purpose for the group. This leadership can be at the international, national, regional, and/or local level. As applicable, these leadership nodes will coordinate the operations of other network nodes and conduct planning.
>
> Recruiting: Some form of recruiting effort will be performed to maintain the overall network. This can range from convincing or intimidating local nationals to emplace IEDs, to grooming individuals to conduct suicide IED missions.
>
> Training: This element provides appropriate education to personnel to perform a specific skill within the network, whether building the device or coordinating network financing, etc.
>
> Target Selection and Planning: This key element relates to the selection of targets and subsequent mission planning. It is here that IED organizations will review enemy (coalition) tactics, techniques and procedures, and conduct appropriate

---

[19] NATO Joint Warfare Centre, *Joint Opeational Guideline for Counter-IED*, 6.

[20] *Ibid*.

[21] *Ibid*.

reconnaissance on the target and associated vulnerabilities, approach and escape routes, etc.

Surveillance: Closely associated with target selection and planning, organized IED networks will often conduct covert target surveillance to gather essential information on the planned target, ideal emplacement methods and locations, viable vantage points to observe the target or target area, as well as viable escape routes for triggermen, etc.

Rehearse attack: Much like coalition forces will rehearse deliberate operations, organized IED networks can rehearse IED attacks to test and evaluate their plan.

Movement: This is the planned movement of device components, supplies, complete devices and personnel into and, as appropriate, out of the target area of operations. It includes the initial movement of components from international or other regional areas into the specific area of operations. It also includes the insertion and extraction of IED cell personnel involved in an IED attack to/from the incident site.

Funding: This includes the sourcing and distribution of financial resources required to finance IED operations. It includes everything from international donor financing, covert international government financing, to tactical level financing from illegal activities like drug trafficking or intimidation.

Supplies: This element describes the materials required to conduct IED operations and includes resources ranging from IED components, vehicles and weapons.

Support: This is the international, regional and local support to assist in the conduct of IED operations and can include funding, training, organization, recruiting, publicity, planning assistance, and possibly leadership. At the local level, support can be active in the form of willing participants joining or otherwise assisting the IED cells, or it can be passive in the form of the provision of information on coalition movements, or the refusal of local nationals to cooperate with coalition forces. Of note, local support can sometimes be more the result of fear of the insurgents than of true support of the insurgents' actions and objectives or a rejection of coalition actions or objectives.

Coordination group: This small, but essential, group at the local or regional level will coordinate the IED effort in a specific area of operations.

Exploitation: This element of the IED network has the function of maximizing the success of any IED attack through the refinement and revision of insurgent tactics, techniques and procedures, or through media exploitation of the attack to influence local and international populations, with particular emphasis on the populations of coalition countries.

Emplacement: This is the act of positioning an IED for an attack. It may be hasty or deliberate and may be conducted by a member of the network or by a local national who willingly assists the insurgents, or who has been coerced into doing so.

Monitor and Detonate: This activity involves watching the target area for the purpose of command detonating an IED or exploiting an IED attack.

Infrastructure: This element includes the physical infrastructure required to conduct IED operations such as safe houses and storage locations.

Information Operations: In conjunction with insurgent exploitation efforts, insurgent information operations will seek to have an effect on both the local national population and that of foreign nations, specifically the populations of coalition countries.

C-IED Operational Concepts

To combat the devices described above and the networks or systems of insurgents that employ them, C-IED doctrine aligns C-IED operations along three lines of operation: Attack the Network; Defeat the Device; and Prepare the Force.[22] Within these overarching lines of operation are six operational functions to achieve desired effects within the lines of operation: Predict; Prevent; Detect; Neutralize; Mitigate; and Exploit.[23] Each of these concepts will be briefly described in turn as described within current NATO doctrine.[24]

The first C-IED line of operation is Attack the Network. Activities within this line of operation target the insurgent political, social and cultural systems. They also include all simultaneous actions at the strategic, operational and tactical levels intended to disrupt the IED network or system. The aim of these efforts is to undermine the ability and will of insurgents to construct and employ IEDs. Attack the Network may include, but are not limited to, such things as deterrence, information operations, law enforcement,

---

[22] Department of National Defence, *Canadian Forces Joint Doctrine Note: Canadian Forces Improvised Explosive Device (IED) Lexicon - DRAFT*, 1-18.

[23] NATO Joint Warfare Centre, *Joint Opeational Guideline for Counter-IED*, 9.

[24] *Ibid*.

and disrupting insurgent re-supply operations and capacity. In Chapter 4 of this paper the Attack the Network areas of network financing, signals intelligence, and criminal intelligence activities of biometric analysis, behavioural analysis and geographic profiling will be examined from a WoG perspective to demonstrate their potential contributions to C-IED operations.

The second C-IED line of operation is Defeat the Device. Activities in this line of operation aim to prevent the emplacement of IEDs, detect IEDs, neutralizing IEDs, and mitigating the effects of these devices. Defeat the Device activities may include the identification of effective tactics, techniques and procedures, the protection of friendly forces, and the development of technologies to detect, identify, classify, mark and disrupt IEDs. In Chapter 4 of this paper the Defeat the Device activities of electronic analysis, explosive analysis and radio frequency propagation analysis will be examined from a WoG perspective to demonstrate their potential contributions to C-IED operations.

The third C-IED line of operation is Prepare the Force. This line of operation aims to integrate C-IED knowledge into pre-deployment training and ensure that friendly forces are conversant with procedures and tactics to successfully conduct operations in an IED threat environment. As already stated this paper will not focus on this line of operation, rather it will focus on the Attack the Network and Defeat the Device lines of operation from a WoG perspective.

C-IED Operational Functions

Predict: The aim of the Predict function within C-IED is to be able to identify the critical elements and nodes of an IED network or system, and where, when and how an IED may be employed. The Predict function includes all activities, technologies and mechanisms

to identify and understand the IED network, its equipment, infrastructure, procedures and support mechanisms.

Prevent: The Prevent function aims to undermine or counter the ability of insurgents to build and employ IEDs.

Detect: Activities within the Detect function include the identification and location of explosive devices, components, related personnel and infrastructure. Detection activities will normally take place if Predict and Prevent activities have failed.

Neutralize: The Neutralize function incorporates both proactive and reactive activities and technologies to disrupt, disarm, render safe, dispose or destroy IEDs and their components.

Mitigate: Mitigation efforts are aimed at mitigating IED effects against personnel and equipment. This is achieved through technology, standardized and realistic training and education.

Exploitation: The Exploitation function spans across the entire C-IED spectrum and spans all three lines of operation in C-IED. It is intelligence driven and uses technical, tactical and forensic means to exploit IEDs and IED events. IED incident exploitation is the process which captures, preserves and analyzes evidence from an IED event in order to enable interdiction operations against IED networks, and to enhance force protection through the development of procedures and new technologies.

With a common baseline understanding of C-IED terminology and operational concepts established, the next chapter will build from this to place C-IED within the broader spectrum of COIN operations in a complex COE.

CHAPTER 3 – COUNTER-IED AS A SUB-SET OF COIN

C-IED operations are not conducted in isolation and without consideration for collateral effects to overall campaign objectives. This chapter will situate C-IED operations within the larger context of COIN within a complex COE to gain better insight to C-IED linkages to COIN, and how the nature and scope of C-IED necessitate a comprehensive or WoG effort to ensure success. To do so, the discussion in this chapter will commence with a brief description of the COE using basic ideas from systems theory. COIN operations within the COE will then be examined with a view to demonstrating that successful COIN operations require comprehensive solutions to address the multitude of diverse factors in the COE. Finally, linkages will be established between the nature of COIN in the COE to the concepts of C-IED operations in order to demonstrate the need for a complimentary WoG approach to C-IED as a sub-set of COIN operations.

The COE

Whether or not Canada was truly prepared to fight a counterinsurgency (COIN) campaign when it transitioned its focus and forces to southern Afghanistan in mid-2005 and early 2006 may be the subject of further reflection in the future. What seems clear, however, is that the Canadian government and the CF have gone through, and continue to go through, a period of new or perhaps renewed emphasis on interagency operations; what is commonly referred to as a whole of government approach.[25] Although Canada certainly employed interagency efforts on previous missions, such as those in the Balkans, Canada's involvement in the COIN campaign in Afghanistan has highlighted

[25] Phil Orchard, "Canada and the Changing Strategic Environment: The Canada First Defence Strategy and Beyond" (UBC, 2008), 26-27.

the need for such operations to harness both military and civil capabilities from across all applicable government agencies. This renewed focus is not unique to Canada; it is the same reality facing its closest allies. Even the United States finds itself re-learning old lessons for the need for interagency cooperation in COIN operations[26] and in a more complex world order that demands non-traditional (not Cold War) approaches to address security challenges that arise within the Contemporary Operating Environment (COE).[27] An examination of the nature of interagency COIN operations will shed some light on how C-IED operations can, and need to be, viewed as part of this integrated effort.

The COE is characterized as being a dynamic system comprising multiple actors, both state and non-state, who operate and interact within adaptive and networked systems that extend beyond geographic boundaries.[28] The actual operating environment, specific to a campaign, can be further defined as the "air, land, sea, space, and associated adversary, friendly, and neutral systems (political, military, economic, social, infrastructure, informational, and others) which are relevant to a specific joint operation, regardless of geographic boundaries."[29] The interplay of these systems demands more than purely military solutions to contemporary problems and they challenge more traditional approaches which are more prescriptive in nature. The COE, as a system of systems, demands approaches that can consider and address the various components or dimensions of the overall system framework and, therefore, this demands capabilities

---

[26] Wiiliam B. Caldwell and Steven M. Leonard, "Field Manual 3-07, Stability Operations: Upshifting the Engine of Change," *Military Review* LXXXVIII, no. 4 (July-August, 2008), 58-59, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20080831_art001.pdf.

[27] US Department of Defense, *Quadrennial Defense Review Report*, 83-86.

[28] US Department of Defense, *Commander's Handbook for an Effects-Based Approach to Joint Operations* (US Joint Forces Command, 2006), I-2.

[29] *Ibid*., I-2

beyond the military. Figure 3.1 below is one example of this interrelationship among systems within the COE.[30]

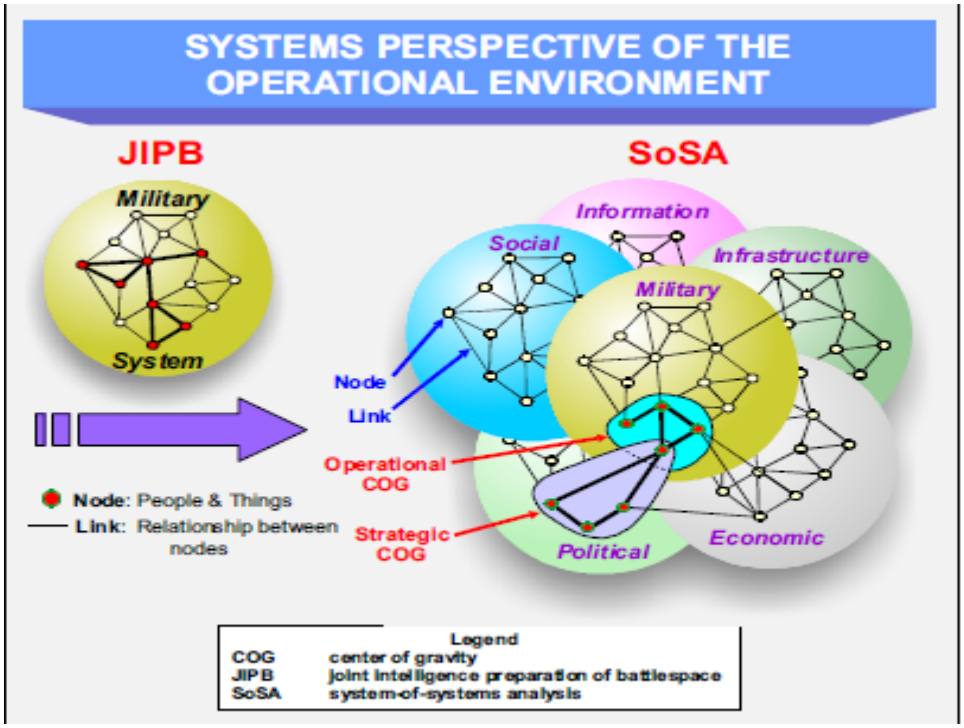

Figure 3.1 – Systems Perspective of the Operational Environment

Source: US DoD, *EBA Handbook*, II-2.

The Systems-of-Systems Analysis (SoSA) on the right hand side of Figure 3.1 highlights the interplay and connectivity between the multiple components, or systems, that comprise the COE. Each of the systems within the system has potential impacts on one or any number of the others in the overall system. For example, any effort to affect the military system set could have a positive or negative affect within any one or combination of the political, economic, information, infrastructure or social systems as well. With this in mind, many nations are acknowledging the need for a comprehensive or integrated approach to the COE where efforts from applicable agents of national power

[30] *Ibid*., II-2

are engaged, but coordinated, to achieve a coherent and unified approach to a given problem set or system.[31] Another depiction of the system approach to describing the COE is presented in Figure 3.2 below.[32] This example illustrates the same approach in the specific example of a terrorist organization with the ultimate objective of employing a weapon of mass effect (WME) against a target in another country. Like the SoSA depiction, this example demonstrates the various potential systems and nodes that could form part of a system, in this case a terrorist system, within the COE. Each of the nodes is connected in a system and each will be or could be impacted by any action taken against any one or group of nodes within the system. It also illustrates that options exist as to how, where, and when any of the nodes may be attacked or otherwise influenced to produce an effect. For example, if it was desired to influence the system node responsible for constructing the WME, it could be possible to do so by targeting other nodes, such as the financing or transport nodes, to produce that effect or the node could be targeted directly.

[31] CACI International Inc and National Defense University, "Dealing with Today's Asymmetric Threat to U.S. and Global Security" (Arlington, VA, 2008), 3-5.

[32] EBO Handbook II-6

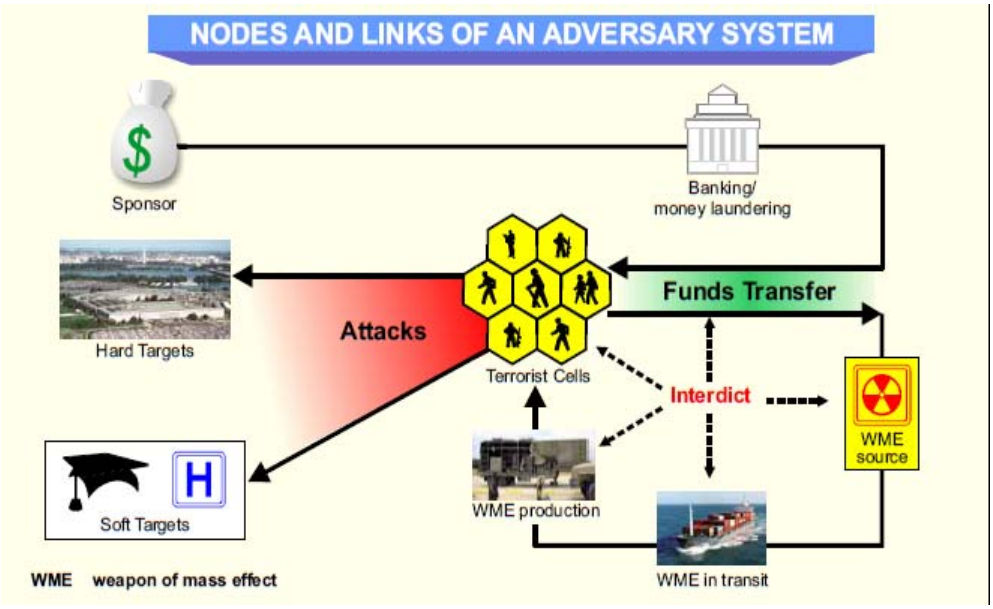

Figure 3.2 – Nodes and Links of an Adversary System

Source: US DoD, *EBA Handbook*, II-6.

The latest United States joint doctrine publication on COIN, JP 3-24 released in 2009, underscores and promotes the requirement for unified effort and action as "the synchronization, coordination, and/or integration of military operations with the activities

of governmental and nongovernmental entities to achieve unity of effort."[33]

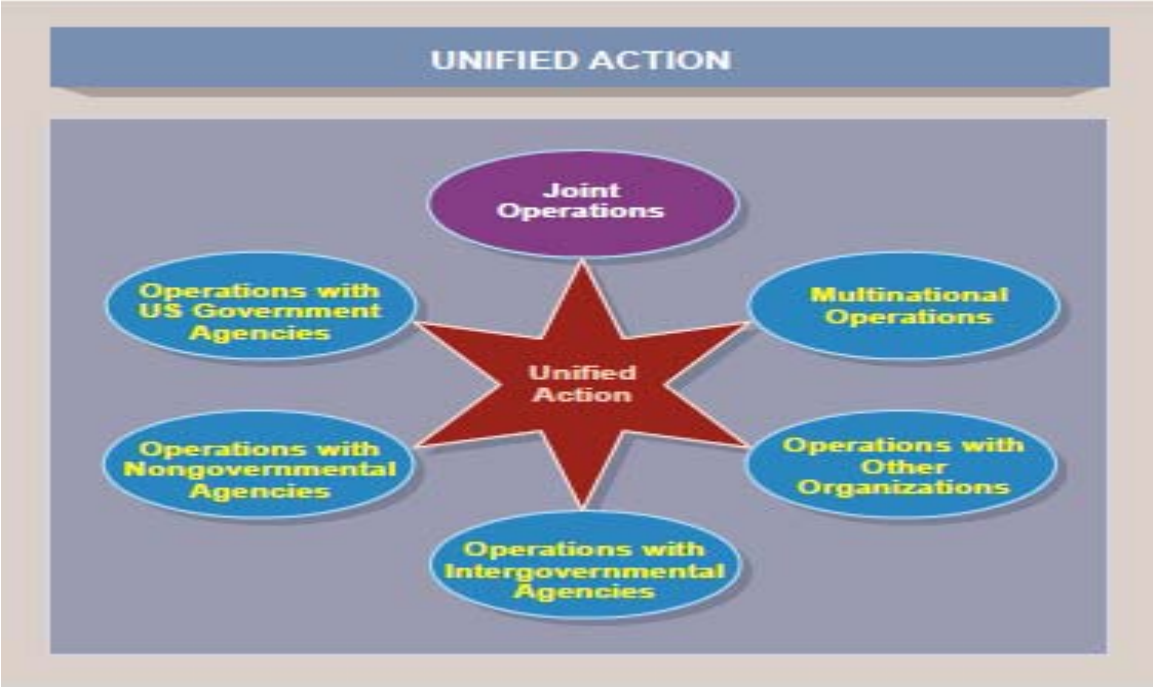

Figure 3.3 – Unified Action

Source: US DoD, *Joint Publication 3-24*, IV-I.

US military COIN doctrine acknowledges that the military cannot and will not act unilaterally in a COIN campaign and that its efforts must be aligned and coordinated with "the activities of USG [United States Government] interagency partners, IGOs, NGOs, regional organizations, the operations of multinational forces, and activities of various HN [Host Nation] agencies to be successful."[34] This is graphically represented in Figure 3.3 above.[35] It also recognizes the significant role the military component plays in such a comprehensive or integrated approach through the military's inherent ability provide unity of command and a reliable and functional command and control architecture and

[33] US Department of Defense, *Joint Publication 3-24: Counterinsurgency Operations* (US COIN Center, 2009), IV-1.

[34] *Ibid*., IV-1

[35] *Ibid*., IV-1

infrastructure that is able to integrate strategic, operational and tactical level COIN operations.[36] Some specific natures or aspects of COIN that necessitate such an approach will now be reviewed to better understand what is about COIN that causes C-IED efforts to be seen as a sub-set of the broader COIN campaign.

Arguably, the principal difference between conventional or traditional military operations and COIN is that the former focuses on terrain and COIN is focused on the population.[37] If it is accepted that an insurgency "aims to gain power and influence"[38] the importance of the population can be understood. Regardless of the exact nature of the insurgency's grievance(s) against the state or its government, an insurgency relies on this power and influence among the population to further its agenda and allow itself freedom of action within the population.[39] Figure 3.4 below illustrates the potential range of support for an insurgency, or for a government, among a population from active support to indifference, and what these means to each side of the insurgency.[40]

---

[36] *Ibid*., IV-1

[37] Gompert, David, Gordon, John, *War by Other Means: Building Complete and Balanced Capabilities for Counterinsurgency* (Santa Monica, CA: RAND Corporation, 2008), xxxiii.

[38] US Department of Defense, *Joint Publication 3-24: Counterinsurgency Operations*, II-1.

[39] Gompert, David, Gordon, John, *War by Other Means: Building Complete and Balanced Capabilities for Counterinsurgency*, xxv-xxxiii.

[40] US Department of Defense, *Joint Publication 3-24: Counterinsurgency Operations*, II-13.

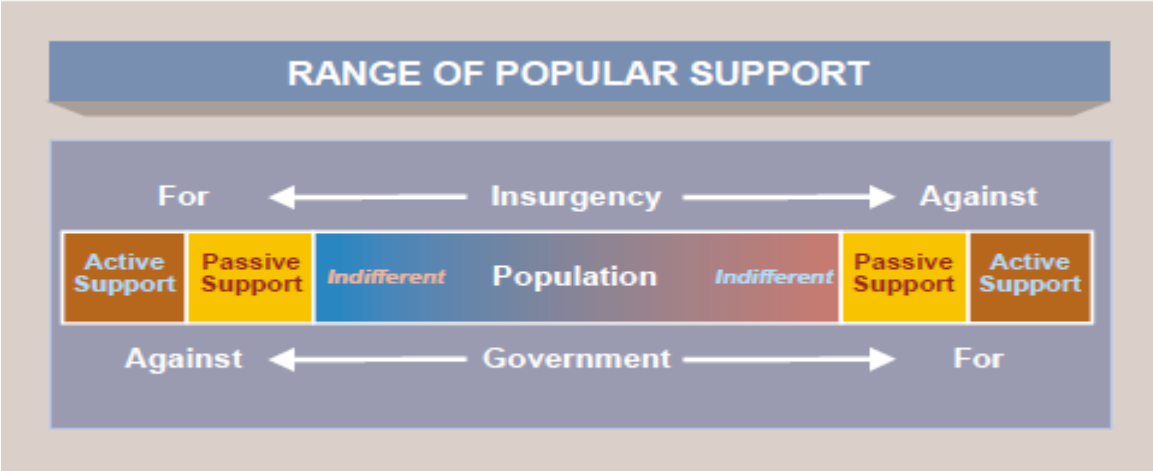

Figure 3.4 – Range of Popular Support

Source: US DoD, *Joint Publication 3-24*, II-13.

It is within the range of active, passive and indifferent support that insurgencies thrive and maintain their freedom of action. To do so they often organize themselves within networks to allow for local action and leadership and also to best influence their support at the tactical level. It is this local, tactical level of support which allows for a broader support base from which insurgencies can conduct higher level activities to keep fuelling the insurgency. These activities include financing (both national and transnational sources), illegal activities such as drug trafficking, political activities, weapons proliferation and the spreading of their particular political and/or religious ideology. All of these activities, if combined to overshadow the activities of the local and national governments will lend legitimacy to the insurgency and propel it even further forward.[41] It is on this perception of legitimacy of the insurgency by the population that the counter-insurgent must focus. To do so, COIN operations must separate or dislocate

[41] *Ibid*., Chap 2

the population from the insurgency while having the concurrent effect of attacking the insurgent networks.[42]

Western militaries have, as part of this recognition to dislocate insurgents from their support base among the population, recognized the need to approach this task from more than just a military/security perspective. In the Canadian context of its campaign in Afghanistan, three lines of operation are used: governance (diplomacy), development (reconstruction) and security (defence).[43] This approach to COIN operations embraces the need to legitimize the local government in the eyes of the local population. To do so, Canada has engaged other government departments beyond the Department of National Defence, and its exclusive tasks to provide security and build capacity within the Afghan army, to achieve this approach. Some of the more prominent or more actively engaged departments include the Department of Foreign Affairs and International Trade (DFAIT) to assist with building and improving Afghan government and political infrastructure, the Canadian International Development Agency (CIDA) to assist with reconstruction, Public Safety Canada (PSC) embodied in the representatives of Corrections Services Canada (CSC) who assist with Afghan security forces capacity building in the area of corrections, and PSC is also represented by the various federal (RCMP) and other Canadian police forces who are deployed as part of PSC's efforts to build Afghan police capacity.[44] All of these integrated efforts are part of a larger comprehensive approach to legitimize the

---

[42] *Ibid*., Chap 3

[43] Independent Panel on Canada's Future Role in Afghanistan, *Independent Panel on Canada's Future Role in Afghanistan: Final Report* (Ottawa: Public Works and Government Services, 2008), 10-29, (accessed August 26, 2008).

[44] *Ibid*.

Afghan government at all levels with a view to it gaining the support of the Afghan people, all the while increasingly dislocating the insurgents from the same population.

Concurrent with these efforts, however, insurgents are adapting and evolving their tactics to counter the efforts of the local (Afghan in the Canadian context) government and its foreign supporters (a coalition). Like other insurgencies of years past, the current insurgencies in Afghanistan and Iraq both avoid large, direct, sustained or conventional engagements with coalition and local forces. Where possible, insurgents will employ irregular tactics and asymmetric attacks against the stronger forces of the coalition, and at the time and place of their choosing. Their ability to do so in an environment where they enjoy the active or passive support of the population improves their ability to strike against the coalition and melt away back into the population, in the complete knowledge that coalition forces will avoid collateral damage and employ target discrimination in order to maintain or gain the support of the same population.[45] The relatively low-cost and simple nature of the IED make it an extremely desirable weapon with which to strike coalition forces with minimal risk to insurgent forces and the high potential for strategic impact on the coalition forces (high volume of casualties).

However, the insurgents' choice to attack coalition forces kinetically, via the IED, provides coalition forces with an opportunity to attack the insurgents. Although the insurgent network can build, transport and emplace the IED within plain sight, the device can provide a technical and tactical signature from which coalition forces can learn, define and target insurgent networks.

C-IED as a Sub-Set of WoG COIN Operations

---

[45] Gompert, David, Gordon, John, *War by Other Means: Building Complete and Balanced Capabilities for Counterinsurgency*, xxxii-xxxiii.

The commander of the Canadian Forces C-IED Task Force, Colonel Omer Lavoie, recently underscored this link between COIN and the C-IED fight. In promoting a better understanding of C-IED operations he asserted that "IEDs are merely a sub-set of a number of kinetic forms of asymmetric kinetic attack used by insurgents."[46] To Lavoie, asymmetric attack is but one form of attack or selected line of operation in guerrilla warfare; therefore C-IED efforts are part of COIN operations. Further, Lavoie highlights that C-IED operations must divide those insurgents who specialize in IEDs from those more generalist insurgents who emplace them, "It is a tactical battle against people not against devices. And, as such, the 'human dimension' by insurgents to use IEDs provides the opportunity to attack the enemy."[47] How the C-IED community approaches this fight 'against people not devices' will be outlined to set the foundation for further discussions on the need to approach C-IED operations within the greater COIN context and how, like COIN operations in general, C-IED demands the skills, expertise and capabilities of other agencies of national power to be truly effective.

As set out at the outset of this paper, C-IED operations are structured along three lines of operation: Defeat the Device; Attack the Network; and Prepare the Force. However, it is not because there is a need to view and conduct C-IED operations within a broader COIN construct that it (C-IED) requires a comprehensive, whole of government approach. Rather, it is the similarities that exist in the approach to these two complex problems (COIN and C-IED) that lend themselves to demanding a more detailed and comprehensive solution to eliminate, or at least mitigate, the threat posed by IEDs. As

---

[46] Army Lessons Learned Centre, "The Dispatches," Department of National Defence, http://armyapp.dnd.ca/allc-clra/Downloads/dispatches_e.asp (accessed April 14, 2010).

[47] *Ibid*.

detailed earlier in this paper, the focus of this paper will remain on the Defeat the Device and Attack the Network lines of operation, and will take as a given the fact that lessons learned from defeating devices and attacking IED networks make their way back into a continuously evolving cycle of tactical and technical improvements for personnel and equipment. Before engaging in a discussion on possible areas for whole-of-government collaboration in C-IED operations, this paper will first examine what activities are implied along the Defeat the Device and Attack the Network lines of operation.

C-IED in 2010 – Defeat the Device and Attack the Network

The cycle of C-IED operations is similar to most other COIN operations in that it is designed to be a 'system of systems' that pulls information from multiple sources that are conducting a multitude of activities against the various key nodes of an IED system. The concept of an IED system is commonly held among those nations involved in C-IED operations and stems from lessons learned that indicated that successful C-IED operations must not solely focus on the devices themselves. Rather, C-IED operations must take a more holistic approach and spread the focus on what can be gleaned from devices and also from the human network (insurgent network in the case of COIN) that decides to employ them as a weapon of choice. It is also commonly held among Canada and its closest allies that attacking the IED network is the most likely avenue to realize any success as counter-insurgents must find a way to prevent insurgents from emplacing the IEDs in the first place.[48] However, the C-IED lines of operation are not mutually exclusive and the figure below is a typical depiction of an IED system and the emphasis being placed on the network that finances, builds, transports and emplaces IEDs. This

[48] Joint Improvised Explosive Device Defeat Organization, "Attack the Network," US Department of Defense, https://www.jieddo.dod.mil/attack.aspx (accessed April 22, 2010).

aspect of an IED system is referred to as 'left of boom' as it entails all the relevant insurgent activities leading up to an IED emplacement and/or event (detonation, find, or turn-in). Figure 3.5 below was produced by the United States Marine Corps Warfighting Laboratory, but it closely mirrors similar depictions of 'left of boom' from Canada and NATO.[49]

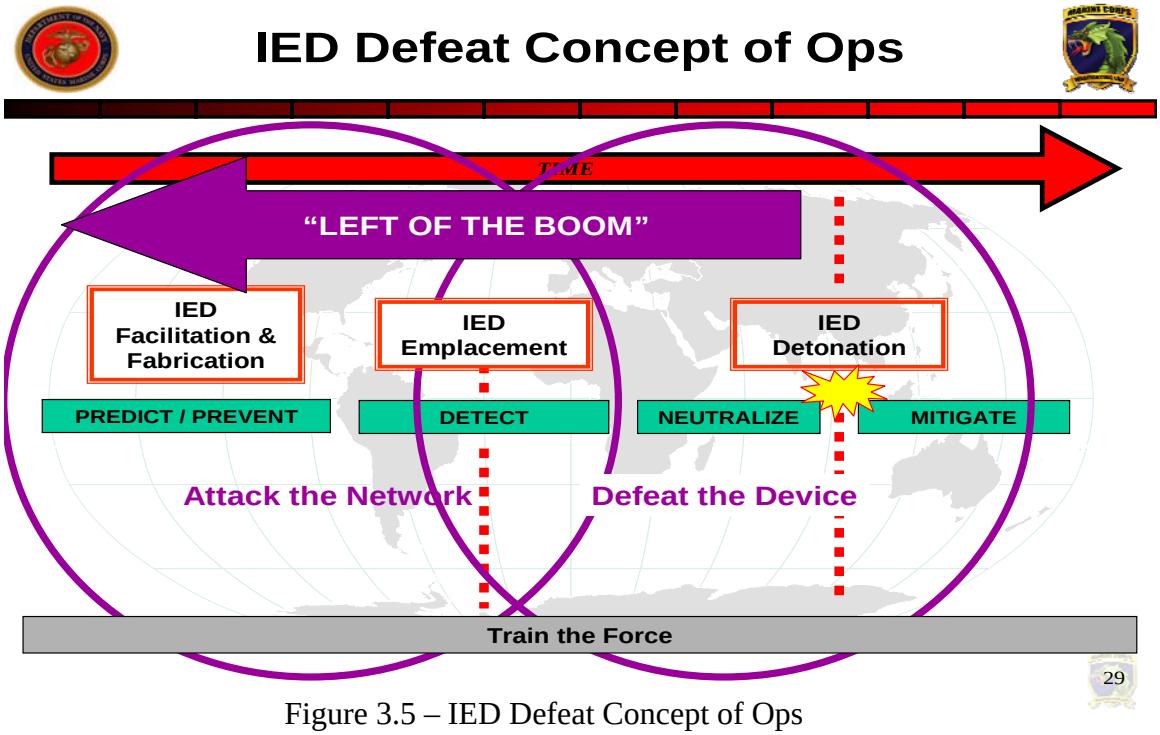

Figure 3.5 – IED Defeat Concept of Ops

Source: Haig, *AO Integration Brief*, 29.

In this 'left of boom' approach to C-IED, all C-IED activities can be placed along a horizontal axis of time in relation to an IED event. In the figure above, as in most 'left of boom' depictions, the IED event is a detonation. What this type of depiction provides is a snapshot of major areas of C-IED operations that can take place before and after an IED event and where the three lines of C-IED operation fit along this horizontal axis. As noted above, the 'Train the Force' ('Prepare the Force' in Canadian parlance) spans the

[49] NATO Joint Warfare Centre, *Joint Opeational Guideline for Counter-IED*, 8.

entire ‘left of boom’ concept as it absorbs lessons learned from all relevant events, actions and analysis throughout C-IED operations. More importantly to this discussion, the figure above gives a relevant delineation of Defeat the Device and Attack the Network areas of focus in C-IED operations.

What can be seen by this depiction is that Defeat the Device activities are principally focused on everything that happens with a device once it has been discovered. This concept includes instances where a device has been detected by whatever means before it has been detonated, to instances where a device has detonated and C-IED operations are then focused on post-blast analysis. As shown above, the three principal areas within the Defeat the Device line of operation are Detect, Neutralize and Mitigate. Similarly, the major C-IED activity areas within the Attack the Network line of operation are Predict, Prevent, and Detect. These are the three areas of focus in the concept of ‘left of boom’: everything that takes place before an IED gets emplaced and/or detonated. It is within these concept areas that C-IED operations focus there efforts on defining and/or targeting those network nodes that conceive IED employment, finance IED construction, build devices, transport devices and emplace devices. To illustrate in more detail beyond that presented in ‘left of boom’ concept diagrams, Figure 3. 6 below illustrates the types of insurgent activities that may take place in the lead up to an IED event, and those insurgent activities following an event.[50] This will allow a better potential understanding of the scope of Defeat the Device and Attack the Network activities conducted by the counter-insurgent.

[50] Shannon Whiteman, "Improving Situational Awareness in the Counter-IED Fight with the Utilization of Unmanned Sensor Systems" (Master's Thesis, Naval Postgraduate School), 33.

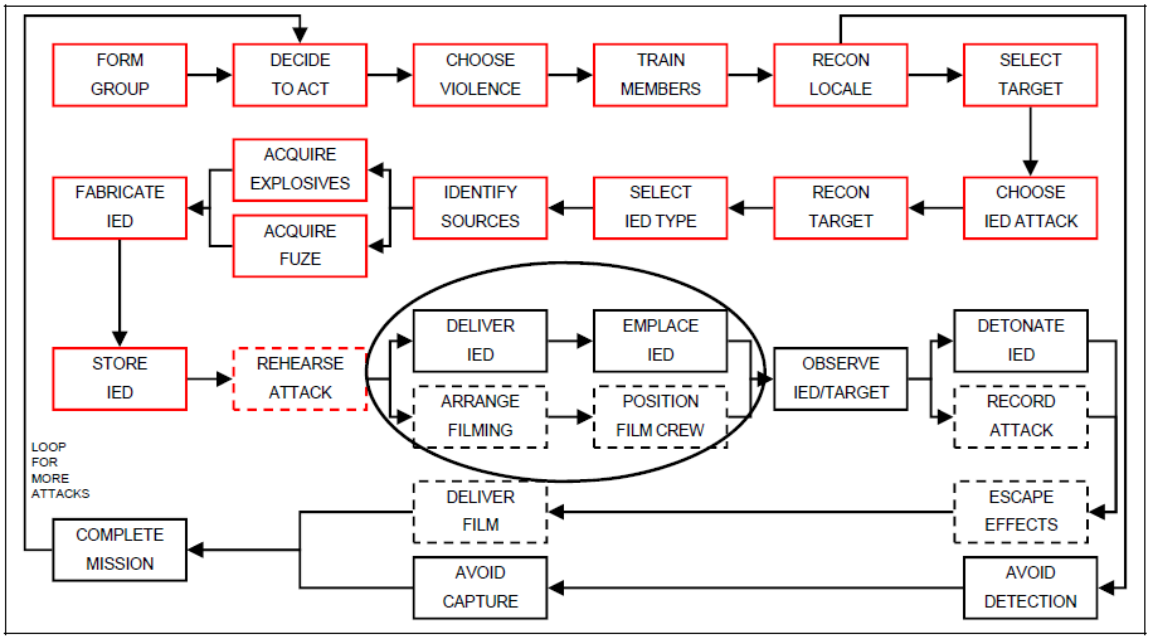

Figure 3.6 – Functional Flow Diagram of a Terrorist Attack

Source: Whiteman, *Improving SA in the CIED Fight*, 33.

What this flow diagram provides is an idea of the various insurgent activities that the counter-insurgent can target to disrupt the IED system. How the counter-insurgent may choose to disrupt the IED system will, as previously discussed, be determined as part of the broader COIN campaign, but when broken down to these types of identifiable nodes and activities, the IED system can be defined in some detail. However, traditional and conventional military capabilities are not necessarily optimized for such activities as nodal definition and targeting. Through the experiences of C-IED operations in Iraq and Afghanistan military forces have been able to develop a framework within which the tactical and technical exploitation of IED events can be conducted with a view to providing detailed analysis of devices and associated networks that be fed back into the

Predict, Prevent, Detect and Mitigate IED system areas. The framework used by Canada is presented in Figure 3.7 below.[51]

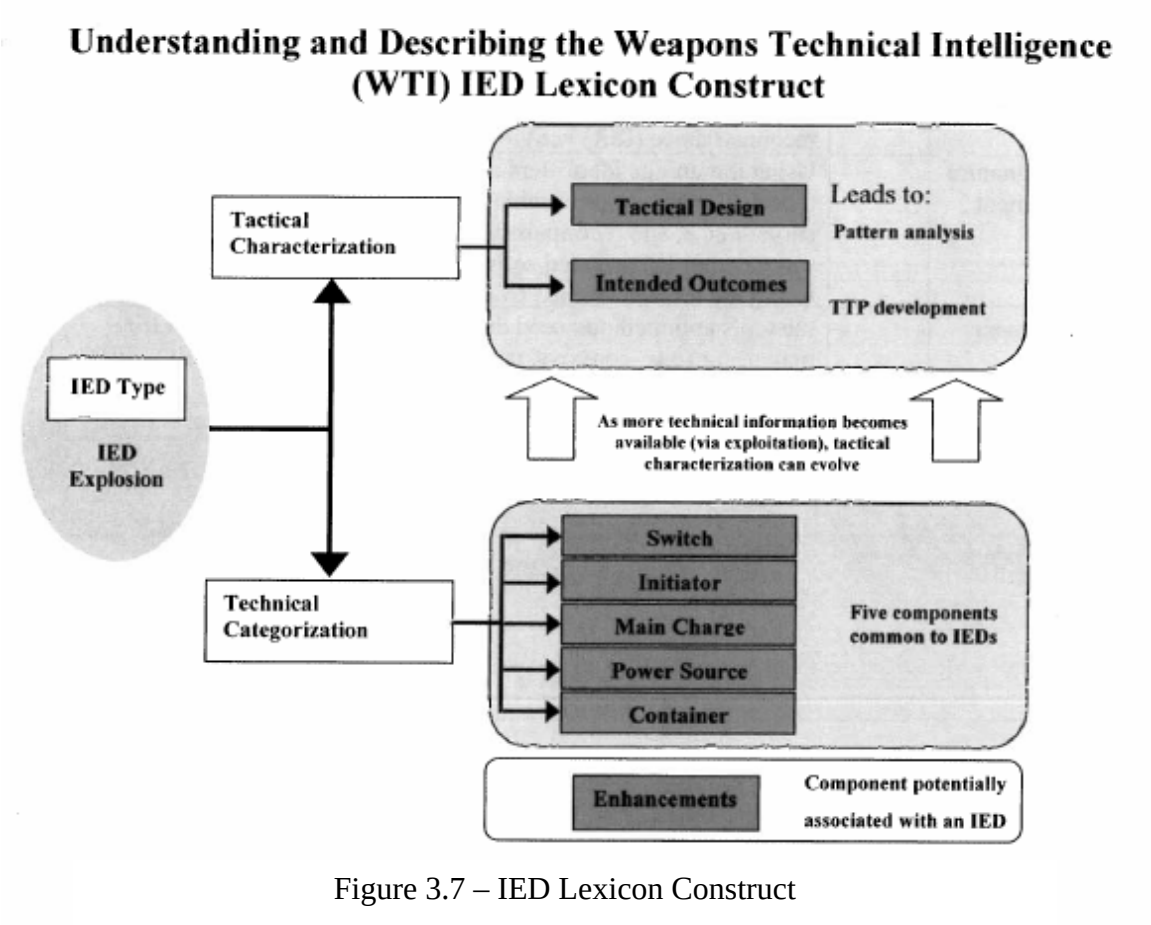

Figure 3.7 – IED Lexicon Construct

Source: DND, *CF C-IED Lexicon*, 3.

This Weapons Technical Intelligence construct is simply a manner in which the Defeat the Device and Attack the Network lines of operation can be seen as mutually supporting activities. In this construct, technical categorization activities form part of Defeat the Device activities which, in turn, support tactical categorization activities.[52] Tactical categorization analysis forms part of Attack the Network activities and tactical

[51] Department of National Defence, *Canadian Forces Joint Doctrine Note: Canadian Forces Improvised Explosive Device (IED) Lexicon - DRAFT*, 3.

[52] *Ibid*.

categorization activities will evolve based on the results of its own analysis and that of technical categorization, as indicated in Figure 3.7.

Following an IED event, which is depicted as an IED explosion in this construct, the two activities of Tactical Categorization (Attack the Network) and Technical Categorization (Defeat the Device) examine both the device and its identifiable components, and the manner in which it was employed with a view to determining a method or any trends in employment, as well as the method or any trends of construction. Both of these categorizations can then be fed into a larger intelligence system that can examine a particular IED event, and all its constituent aspects, to potentially identify the source(s) (network) of the IED.

As articulated early in this chapter, the COE can be view as a complex system of systems and C-IED efforts can feed into defining these systems within a COIN campaign. The same experiences in the COIN campaigns in Iraq and Afghanistan that guided C-IED operations to employ the construct above have also identified capability gaps within modern conventional forces. While such capabilities may be lacking in western military structures, the capabilities required to conduct the necessary forensic analysis as part of tactical and technical categorization are not new and exist within most western countries' national arsenal. This paper will now examine areas of both Defeat the Device and Attack the Network activities that were previously identified in Chapter 2 and which may be enhanced by harnessing the talent, expertise and technological capabilities of other government agencies to produce a truly whole-of-government approach to defeating an IED system.

CHAPTER 4 – Gaining the Upper Hand: Whole-of-Government Opportunities in the Defeat the Device and Attack the Network Lines of Operation

Having painted C-IED operations within the broader tapestry of COIN operations in the complex COE, this chapter will explore some possible activities where a whole-of-government approach to the C-IED fight could bring skills, expertise, knowledge and efficiencies to compliment those of the military component in a COIN campaign. The examples provided herein do not constitute an exhaustive list, rather they are merely possibilities of where other government departments could provide relevant value-added to C-IED operations. As military knowledge of devices and insurgent tactics evolves, it is conceivable that additional and currently unforeseen government agencies could assist in specific areas of C-IED. Defeat the Device activities of electronic analysis, explosive analysis and radio propagation will be examined first followed by the Attack the Network activities of network financing, signals intelligence, and the criminal intelligence areas of biometrics, behavioural analysis and geographic profiling to demonstrate WoG potential.

DEFEAT THE DEVICE

Electronic Analysis

One of the common forms of switches experienced in the IEDs encountered in Iraq and Afghanistan was some form of electronic device. Various low-tech options have been applied by insurgents such as cellular phones or garage door openers.[53] These types of electronics are easy to acquire commercially and be funnelled into the desired operating area by insurgent networks. However, they also provide an electronic signature that can be exploited by C-IED operations.

[53] *Ibid*.

Military capability could conceivably, or presumably, provide some form of analysis of captured/recovered electronic devices, however one federal agency that may be able to provide detailed, relevant and actionable analysis could be the Communications Security Establishment Canada (CSEC). One of CSEC's assigned tasks is "Testing, inspecting and evaluating IT [Information Technology] products and systems to identify risks, vulnerabilities and appropriate mitigation measures."[54] It is also mandated to "provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties"[55] and has close working relationships with Canada's key allies that can involve intelligence sharing as well as research and development.[56] It is CSEC's implied ability to conduct technical analysis and its potential to act as another conduit to foreign technical intelligence that makes CSEC a potentially invaluable asset to C-IED operations.

If CSEC could provide timely and relevant analysis of the interrogation of the technical characteristics for various chosen means of electronic initiation, this valuable data could be used to advise in-theatre formations of known operating characteristics for selected electronic initiators such that patterns could potentially be established. Such pattern analysis could potentially assist intelligence and command staffs better target insurgent networks. From a force protection perspective, this type of data could be fed back into the military system to evaluate current counter-measures and make informed

---

[54] Communications Security Establishment Canada, "The Anti-Terrorism Act and CSEC's Evolution," Government of Canada, http://www.cse-cst.gc.ca/home-accueil/nat-sec/ata-lat-eng.html (accessed April 14, 2010).

[55] *Ibid*.

[56] *Ibid*.

assessments on any potential research and development that may need to take place, particularly in the case of a newly discovered or evolving threat.

CSEC's relationships with its sister organization in the United States, the United Kingdom, Australia and New Zealand cannot be understated in this endeavour. Their (CSEC) perceived ability to share and obtain information from these allies could be of tremendous benefit to Canada. CSEC could conceivably provide current Canadian data from a particular theatre of operations, as well as obtain foreign data and intelligence on similar matters from its close relationships. Information sharing of technical intelligence and analysis could assist Canada's ability to monitor current and emerging trends as well as warn of new threats that may be appearing in other theatres of operation.

Regardless of the source of analysis, CSEC or a foreign ally, CSEC can play a key role in the analysis of electronic components of captured/recovered devices. This expert feedback can be fed into both the intelligence and targeting cycles, but also into the never-ending cycle of review of tactics and procedures.

Explosive Analysis

Canadian soldiers in Afghanistan have been exposed to IEDs with two principal types of explosive charge: a conventional munition or some form of homemade explosive comprised of commercially available components/ingredients.[57] In both the Iraq and Afghanistan theatres of operation here is no shortage of accessible conventional munitions from former weapons stockpiles or the black market and there is presumably sufficient data available to determine the source of such munitions should they be used in an IED. The presence of some form of homemade explosive provides a more significant

[57] Department of National Defence, *Canadian Forces Joint Doctrine Note: Canadian Forces Improvised Explosive Device (IED) Lexicon - DRAFT*, 14.

challenge to military capabilities in determining any likely source of the explosive such that further intelligence analysis can take place. In the Canadian context, however, this analysis void may be potentially assisted by Natural Resources Canada (NRCan).

Within NRCan exists the Explosives Safety and Security Branch and one of this branch's principal components is the Canadian Explosives Research Laboratory (CERL). The CERL offers a broad range of services to the government and the public ranging from "testing whether a product is fit for use to reducing the effects of accidental or terrorist blasts."[58] As part of this mandate, the CERL conducts explosive analysis on a "wide range of energetic materials associated with commercial blasting explosives, initiators, fireworks and pyrotechnic devices."[59] Given its routine tasks and scope of operations, the CERL could be useful source of detailed analysis on any recovered explosive materials from IEDs that are not clearly identifiable as conventional munitions. The CERL could potentially provide analysis of the chemical composition of explosives, its likely blast effects and potentially the potential range of sources for the explosive ingredients. This type of data could then potentially be fed back into the larger intelligence community to then further define any known links to previous IED attacks. This type of link analysis could potentially allow for the definition of a potential IED network or system that is unique to a particular explosive recipe.

NRCan explosive analysis could also provide IED mitigation benefits. If the explosive potential of IED charges can be appropriately analyzed to gain a sound

---

[58] Canadian Explosives Research Laboratory, "Explosive Analysis," Government of Canada, http://www.nrcan.gc.ca/mms-smm/expl-expl/sci-sci-eng.htm (accessed May 1, 2010).

[59] *Ibid*.

understanding of its blast potential, as NRCan does on a routine basis for industry,[60] this data could assist the CF in assessing current and future force protection measures. Specifically, NRCan could potentially assist with the testing and analysis of current armour protection systems for personnel and equipment. It could also assist with research into improved systems if/when deficiencies are identified. With procedures and protocols already established, NRCan is a potential source of proven, timely and valuable explosive analysis capability.

Radio Frequency Propagation

The use of remotely controlled devices within IEDs provides another weapons signature that coalition forces can potentially attack. To do so, coalition forces must gain knowledge of frequencies and conditions that optimize their use. In Canada, the department that considers such issues on a routine basis, although from a commercial perspective, is Industry Canada. Specifically, the Communications Research Centre (CRC) within Industry Canada is the government's "primary research lab for communications technologies."[61] Within the CRC, one of the areas of research is satellite communications and radio propagation.

As part of its radio propagation research and analysis, the CRC conducts research "over a broad range of radio frequencies and link geometries used by a variety of communications services."[62] Although focused on commercial and domestic propagation issues, the CRC could provide some added value to C-IED through its research in the areas of "tropospheric phenomena and surface environmental effects caused by terrain,

---

[60] *Ibid*.

[61] Communications Research Centre, *Research and Development*

[62] *Ibid*.

vegetation and manmade obstacles."[63] It also conducts some of its research activities in the area of radio frequency propagation "impairment mechanisms."[64] If the scientific potential of the CRC, as well as its established scientific database(s) could be harnessed within C-IED, it could provide tremendous benefit to potential insurgent network definition and with the development of new technologies to counter the use of the radio frequency spectrum by insurgents, and also in the development of new or revised tactics and procedures.

Similar to the data and analytical feedback loop back into the overall COIN intelligence machine that could be established with electronic and explosive analysis, radio frequency propagation analysis of applicable captured/recovered IED components can assist with defining an insurgent footprint. If CRC analysis could assist in determining methods and locations for the components' best use by insurgents, insurgent tactics could be better analyzed to potentially lead to a targeting plan or any other concept with which to neutralize this threat. Such data could also assist Canadian and coalition forces in determining areas where radio frequency use by insurgents is hampered or where it is maximized and, therefore, assist with determining potential IED 'hotspots' as part of an IED trend analysis. Additionally, radio frequency propagation counter-measures could be developed from the CRC's analysis data. This could be in the form of a technological counter-measure, or more simply an amendment of tactics and procedures to minimize the threat to Canadian and coalition forces.

This discussion of potential whole-of-government collaboration within the Defeat the Device line of operation are simply examples of some potential sources of expertise

---

[63] *Ibid*.

[64] *Ibid*.

in other government departments that can feed the C-IED and COIN intelligence cycles. As was noted in each of the three Defeat the Device examples above, analytical data pulled from captured or recovered device components can assist C-IED operations in focusing 'left of boom' and increase the potential for success in preventing and predicting IED strikes. Whole-of-government analysis possibilities within the Attack the Network line of operation will now be examined.

ATTACK THE NETWORK

IED Network Financing

As IED systems or networks get defined from pattern and link analysis from the outputs of technical and tactical exploitation, it is possible that IED system financing nodes and activities could be determined. These sources of financing could range from local to national to transnational sources and can conceivably be appropriately targeted in whatever manner desired by a theatre or strategic commander. Analyzing and targeting financial networks is not a traditional function for which militaries are prepared and this presents another possibility for whole-of-government collaboration. In the Canadian context, the Financial Transactions Analysis Centre (FINTRAC) could provide such analysis.

FINTRAC's mission is to "contribute to the public safety of Canadians and help protect the integrity of Canada's financial system through the detection and deterrence of money laundering and terrorist financing."[65] As apart of its terrorist financing analysis activities, FINTRAC supports the Canadian Security Intelligence Service (CSIS) with financial intelligence for investigations of threats to Canada. FINTRAC defines terrorist

[65] Financial Transactions Analysis Centre, "Terrorist Financing," Government of Canada, http://www.fintrac-canafe.gc.ca/fintrac-canafe/1-eng.asp (accessed April 22, 2010).

financing as "funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion."[66] While the procedures used by FINTRAC to define and track such financial activities remain in the classified realm, it is reasonable to infer that FINTRAC would be able to provide similar analysis in the event that an IED system extended into the transnational arena. While such circumstances would indicate a much larger insurgent funding issue than a simple IED network, the point is that FINTRAC conducts forensic financial analysis as a matter of routine and could, therefore, provide some assistance in the analysis of known or suspected IED systems.

While the potential for counter-insurgent forces to piece together a large, complex and transnational IED system financing network could exist, the potential for FINTRAC to assist Canada's C-IED operations could also be by simply providing advice and guidance at the operational (in-theatre) level. The entire weight and expertise of FINTRAC would not necessarily have to be engaged at the national level to produce tangible results. Once C-IED and COIN intelligence staffs have started to piece together the financing chain within a particular IED system, FINTRAC personnel could be able to guide and advise operational staffs on the further collection of intelligence and evidence, as well as provide a gateway into any relevant and known international linkages that may be established. In the case of Afghanistan, this could prove to be of tremendous benefit as it is alleged that a significant amount of financing for the insurgency is provided by the

[66] *Ibid*.

drug trade.[67] Clearly, any such link analysis spans beyond simply C-IED operations. FINTRAC analysis and guidance would permit a commander to better determine how he/she may wish to address the financing dimension as part of the overall COIN campaign, and avoid prematurely targeting the IED financing chain at the risk of disrupting other closely-related and equally important COIN activities.

Signals Intelligence

The ability to monitor the communications within an IED system would provide obvious and significant benefit for the Predict and Prevent functions within the Attack the Network line of operation. Indeed, this benefit would not be unique to C-IED operations. However, as this paper has previously highlighted, IED systems have proven to be adaptive systems that learn from the successes and failures of their own actions, and the mistakes and successes of those they target (Figure 3.6 - Functional Flow Diagram of a Terrorist Attack). The ability to monitor and assess the insurgents' planning and execution of an IED event at various stages would enable an operational commander to determine his/her options in preventing a successful IED strike and enable him/her to conduct C-IED operations at the time and place of their choosing. Additionally, insurgent reactions to Canadian or coalition actions could also be monitored and assessed. Within the government of Canada, such foreign communications monitoring is provided by CSEC.

While the details of procedures employed by CSEC in the execution of communications surveillance are highly sensitive, for the sake of this discussion it appears reasonable to proffer that CSEC possesses such capability. Indeed, open source

[67] Lee Windsor, David Charters and Brent Wilson, eds., *Kandahar Tour* (Mississauga, ON: Wiley, 2008), 93, 175.

information provided by CSEC indicates that a strong relationship exists between CSEC, CSIS and the CF on issues of national security.[68] What is important to this discussion is to highlight the potential to harness CSEC capabilities to assist with the definition, monitoring and targeting of IED systems. Through CSEC, operational commanders could also leverage the capabilities of close allies. This could be of tremendous benefit and allow for economies of effort, particular if IED system monitoring evolved into a transnational issue. That is to say, for example, that a Canadian signals intelligence collection plan on an IED network in Afghanistan could lead into broader networks that cross over the border into Pakistan or Iran. If allied collection agencies are already collecting intelligence in those areas, there is potential for information sharing and joint analysis. Barring any national caveats preventing the sharing of certain intelligence, the potential exists for better definition of IED systems within the broader coalition intelligence effort. The principal issue for consideration is that CSEC possesses signals intelligence collection and analysis capabilities, and the potential to leverage those of Canada's close allies, which can directly support C-IED operations.

Criminal Intelligence

The final area of potential whole-of-government collaboration that will be examined within the Attack the Network line of operation is criminal intelligence. Criminal intelligence analysis is broad term used to define tools and procedures to provide some form of link analysis of crime data. The International Criminal Police Organization (INTERPOL) defines criminal intelligence analysis as "The identification of and provision of insight into the relationship between crime data and other potentially

[68] Communications Security Establishment Canada, *The Anti-Terrorism Act and CSEC's Evolution*

relevant data with a view to police and judicial practice."[69] It further states that the intent or purpose of such analysis is "help officials - law enforcers, policy makers, and decision makers - deal more effectively with uncertainty, to provide timely warning of threats, and to support operational activity by analysing crime."[70] If such analysis can assist in defining links between various sources of crime data, it may prove beneficial to efforts in defining links in C-IED data as both deals within the realm of human (criminal/insurgent) networks. In Canada, the Royal Canadian Mounted Police (RCMP) possesses a Criminal Intelligence Program that may provide some analytical capability and experience that can be leveraged in support of C-IED operations.

The RCMP conducts criminal investigation analysis as a matter of routine and use tools that would benefit C-IED operations. Specifically, biometric data analysis, behavioural analysis and geographic profiling are three niche areas that can be leveraged for C-IED. Similar to police investigations into serial, gang or organized crime activities, C-IED operations seek to determine linkages and trends to define the IED system.[71] When combined with data, knowledge and intelligence gleaned from other defeat the Device and Attack the Network analysis activities, these analytical processes can provide exponential returns in the effort to provide commanders with a coherent picture of the IED system from which decisions and operational priorities can be made.

---

[69] International Criminal Police Organization, "Criminal Intelligence Analysis," http://www.interpol.int/public/CIA/Default.asp (accessed April 14, 2010).

[70] *Ibid*.

[71] NATO Joint Warfare Centre, *Joint Opeational Guideline for Counter-IED*, 1-76.

Biometric Analysis

Biometrics is term used to describe the "automated or semi-automated use of physiological or behavioural characteristics to determine or verify identity."[72] There are different forms of biometric data that are commonly used for identification analysis, but some of the more common forms are deoxyribonucleic acid (DNA), fingerprints, and iris recognition.[73] Like other analytical outputs already discussed in this paper, biometric data could be collected from captured or killed insurgents or equipment related to an IED event, or any insurgent or person or vehicle of interest detained by Canadian or coalition forces. This data could then be analyzed against in-theatre, national and/or coalition databases to assist in conducting link analysis and trend analysis. The RCMP, or any other police agency possessing the requisite experience in this field, could provide technical advice in the collection, analysis, storage and manipulation of biometric data in support of C-IED operations. Soldiers would be able to collect most biometric data, but law enforcement officials may be best placed to guide the preservation, storing and tracking of such important data, particularly if it were to be used as evidence in any form of future legal prosecution by host nation or international courts.

Behavioural Analysis

Behavioural analysis, as described by the United States Federal Bureau of Investigation (FBI), is a process of "reviewing and assessing the facts of a criminal act, interpreting offender behavior, and interaction with the victim, as exhibited during the

[72] Lalita Acharya, *Biometrics and Government* (Ottawa: Library of Parliament, (2006), 1.

[73] *Ibid*., 3-5.

commission of the crime, or as displayed in the crime scene."[74] Designed to interpret and predict offender behaviour in criminal cases, this process is another potential source of analysis in C-IED operations. This approach could be used to determine the patterns of behaviour or tactical signature displayed by an IED system at the tactical or local level, or perhaps even on a larger scale. The intent is to profile IED events with a view to determining any patterns of behaviour by a particular IED system such that its activities could be mapped and/or forecasted based on assessed behavioural trends, much like the profiling of a serial offender or organized criminal enterprise. These profiles may reveal patterns in relation to the types of attacks conducted, the time of day they are usually conducted, the type of targets usually selected, or any common characteristics of the selected attack locations. This is not an exhaustive list of possible analytical outcomes, but is merely an appreciation of the types of information that may be able to be gleaned from this type of activity.

Geographic Profiling

This analytical tool was developed as an aid to criminal investigations to "predict the serial offender's most likely location including home, work, social venues, and travel routes"[75] by using mathematical models to "analyze the locations of the crimes and the characteristics of the local neighbourhoods in order to produce a map showing the areas in which the offender most likely lives and works."[76] This technique allows investigators to focus their efforts in a specific geographic area (profile) that is produced by the

---

[74] Federal Bureau of Investigation, "Investigative Programs Critical Incident Response Group," United States Government, http://www.fbi.gov/hq/isd/cirg/ncavc.htm#bau (accessed April 14, 2010).

[75] Royal Canadian Mounted Police, "Geographic Profiling," Government of Canada, http://www.rcmp-grc.gc.ca/tops-opst/bs-sc/geographic-g-profil-eng.htm (accessed April 14, 2010).

[76] *Ibid*.

model.[77] In the same manner serial offences can be analyzed by geoprofiling, IED events could be mapped or profiled using this tool to produce a map of IED event histories. This could assist in the identification of IED 'hot spots' which could the immediate effect of providing useful information in convoy or patrol planning such that friendly forces avoid known 'hot spots' whenever possible, particularly during times of day the profile indicates as having a high probability of IED attack.

If geoprofiling models could be manipulated to geographically represent IED events by type of device used, time of day of the attack, by target of attack, or any other metric deemed useful by C-IED or operational planning staffs, this tool could potentially provide a useful prediction analysis. When contrasted or combined with other C-IED analytical outputs, geographical profiles could provide further definition of an IED system or network modus operandi which could contribute to the overall C-IED and COIN intelligence and targeting apparatus.

In 2007 the Canadian Forces engaged civilian industry to assist in the development of a geoprofiling tool designed specifically to support C-IED operations.[78] It is unknown if such a tool has been released for use by the CF in Afghanistan, but like biometric data collection and analysis, it is the experience in collating, analyzing and manipulating the geoprofile data that the RCMP can provide in order to ensure the potential benefits of this tools are maximized.

This chapter examined several potential C-IED activity areas within which other government agencies could potentially provide some valuable contributions to the fight.

---

[77] *Ibid*.

[78] "MDA to Demonstrate Information Solution for Soldiers," *Canada NewsWire* (Jun 18, 2007), 1, http://proquest.umi.com/pqdweb?did=1290006891&Fmt=7&clientId=1711&RQT=309&VName=PQD.

When taken together as complimentary actions, they are a potentially powerful enabler to C-IED operations. So how can Canada capitalize on this potential? The next chapter will discuss some possible options for consideration to ensure a coherent, enduring and truly whole-of-government approach to C-IED.

CHAPTER 5 – DISCUSSION: IF WE BUILD IT, WILL THEY COME?

This paper has heretofore focused on defining key terminology and concepts in the C-IED lexicon to establish a common understanding. It has also established a firm link between the nature of C-IED operations within the context of COIN in a complex COE that would be greatly enhanced by WoG collaboration in C-IED. Possible areas for such collaboration were then discussed to demonstrate this potential to deliver effective C-IED capability for expeditionary operations. This paper will now transition into a discussion of potential mechanisms Canada could consider to institutionalize a truly WoG approach to C-IED in order to promote, build and sustain a more aggressive and comprehensive C-IED capability. To do so, this discussion will review some potential options at the strategic and operational (theatre of operations) levels, and some benefits and risks associated with doing so. The intent of this chapter is not to discuss structures and specific tasks; rather it is intended to discuss ways in which Canada can provide WoG capability and collaboration to the C-IED fight.

STRATEGIC LEVEL OPTIONS

Canada does not currently have a WoG interagency organization charged with bringing strategic coherence among all applicable government departments with an interest or role in C-IED. What appears critical, however, is creating some form of framework that will provide this coherence and bring together the full potential of Canada's national power, some of which was identified in Chapter 4, to guide Canada's C-IED efforts. It should also be of sufficient depth to ensure that sufficient WoG expertise spans the three C-IED lines of operation. The intent of the framework would be to provide strategic coherence to C-IED, to harness all applicable facets of national

power, to promote and build a common understanding of C-IED issues and challenges across government, and to facilitate the delivery of concrete C-IED effects to Canadian international engagements abroad. While no WoG framework currently exists, the Department of National Defence possesses a capability from which a WoG and interagency framework could be built: the Canadian Forces C-IED Task Force (CF C-IED TF).

WoG C-IED Task Force

The CF C-IED TF was established in 2007. This small, approximately 25-person Task Force was given a broad mandate to establish "cohesive C-IED governance" to the CF's C-IED efforts and also to promote and create an "integrated and synchronized effort"[79] for C-IED. In the interest of maintaining the strategic military coherence already established by the C-IED TF, and in the interest of maintaining strategic coherence with our allies, using the C-IED TF as a building block would allow for economies of effort and scale. The size and exact composition of such an organization is not particularly relevant to this discussion. The point for consideration is that any and all applicable federal agencies and departments would be appropriately represented in this organization. Whether or not the C-IED TF remained under the umbrella of the CF and Department of National Defence (DND) could be the subject of debate, but it would arguably be more expedient to keep existing infrastructure and key procedures extant instead of changing them unnecessarily. Similarly, the permanent manning of the organization by WoG partners is also open for some debate.

[79] Chief of the Defence Staff, *CDS Supplemental Directive - Enhancement of CF C-IED Capabilities in Afghanistan*, February 29, 2008), 3-4.

The establishment of a strategic C-IED framework cannot allow itself to get bogged down in perceptions of 'empire building' or any other form of unnecessary bureaucracy. What must be maintained is the aim of attaining strategic coherence and unity of effort, thought and purpose. In the example of using the C-IED TF as a building block, any expansion of its manning by WoG partners does not necessarily translate into the permanent transfer of people and positions from other departments into the DND. To attain a sense of permanency in the manning of a new strategic framework, applicable personnel could simply be seconded between departments in order to achieve the intent and avoid unnecessary resistance to the concept. The exact scope or magnitude of such personnel exchanges is also open to debate and would be best left to the subject matter experts to best determine what skills would need to be represented within the organization.

The wholesale transfer of unique departmental capabilities is not advocated in this concept. Rather, it is proposed that appropriate representatives from applicable departments would work within one unified command and control structure and these members would represent the skills, capabilities and interests of their parent department. The common situational awareness and understanding that would be achieved within this pan-government organization would then make their way back into the other government departments to help guide the efforts within their unique areas of expertise. Admittedly, a more formal and permanent arrangement may not be the only manner in which to achieve this desired effect.

WoG C-IED Working Group

If the idea of a larger, permanently manned, pan-government C-IED organization is deemed to be unachievable for whatever reason, then it is possible that a 'virtual' C-IED organization could be formed to achieve the same results. The C-IED TF could still provide a sound starting point from which to build a pan-government organization, but WoG representation could be on a less formal basis. The establishment of a Working Group (WG) could possibly achieve the same effect. Within this concept, a WoG C-IED WG could be established with the C-IED TF as the lead organization, and further WG membership would be comprised of relevant government departments with an interest in C-IED. This WG would meet on a regular basis (monthly) to discuss current C-IED trends, issues and challenges in operations abroad, and it would also provide a venue for WG members to provide situational awareness of their departmental C-IED activities for the other WG members. This concept assumes that ministerial level support of the WG would exist and membership and participation would not be optional.

Regardless of the mechanism chosen, a more formal and permanent arrangement or a less formal organization that meets on a regular basis, either approach could provide unity of thought, effort and purpose across the C-IED lines of operation and from a WoG perspective. The key benefits to be achieved would be strategic coherence, leveraging of experience, knowledge and skills, and leveraging of allied (foreign) partnerships resident within each department. If this could be achieved at the strategic level, it would pave the way for tangible collaboration and cooperation at the operational level.

Regardless of whatever model may be selected with which to create a strategic WoG C-IED organization, any such endeavour must ensure that is able to provide certain

functions. Specifically, it must have a clearly identified and endorsed (by Cabinet) lead agency. This lead agency, DND in the proposals above, would be responsible for the activities and outputs of the WoG C-IED organization. It must also be able to influence the inputs from the WoG members of the organization. That is to say that its membership needs to be comprised of representatives from an appropriate level of departmental management such that these representatives can influence activities within their parent departments to appropriately support C-IED operations. It must also be of sufficient breadth that all known areas of C-IED are appropriately accounted for by national capabilities and departments. This also implies that if a new development in C-IED necessitates the addition of a new department, the organization would have the ability to mandate the inclusion of the new department.

Finally, any strategic organization would need to possess the ability to manage and warehouse a wide variety of information in the classified realm. This would be critical to effectively support deployed operations, conduct operations with allies, and to safeguard sensitive capabilities and procedures. At the risk of negating other viable options, it would seem that the CF C-IED TF may be the most expeditious option from which a strategic WoG capability could grow.

OPERATIONAL LEVEL OPTIONS

WoG options for employment at the operational level are potentially easier to implement that those at the strategic level. WoG efforts in C-IED operations at the operational level are likely to involve individual personnel support in relatively small numbers and in niche areas. As outlined in Chapter 4, most of the areas for WoG collaboration involve exploitation activities that require national level facilities resident

in Canada. There are, however, some capabilities that can be deployed into a theatre of operations to extend the direct WoG support to C-IED operations.

Exploitation Collaboration

The exploitation laboratory deployed by the CF to Afghanistan in 2009[80] may be one such opportunity to extend WoG collaboration to the operational level. The exact capabilities of the Canadian exploitation lab are classified; however it could be possible for applicable analysts from appropriate government agencies to deploy in support of this facility. Even if in an advisory role, WoG partners could support efforts within this facility to process materiel for further analysis at strategic facilities. It could also serve to build and maintain an increased level of understanding among WoG partners of the operating realities and challenges faced by deployed forces in the conduct of C-IED operations. Such understanding could have the resultant benefit of the amending of strategic level procedures in specific WoG areas of expertise to better support operational level C-IED efforts. Similar to the potential for an advisory role within the lab for applicable WoG partners, there are potential roles for law enforcement partners as advisors to operational commanders.

Law Enforcement Collaboration

Chapter 4 outlined some areas of criminal intelligence that could contribute to a WoG approach to C-IED. The assistance of criminal intelligence expertise can extend to the operational level. While most criminal intelligence support activities may have to remain within Canada, the deployment of police officers with experience in criminal

[80] "Explosive Disposal Conference to Focus on IEDs," *The Maple Leaf*May 6, 2009, http://www.forces.gc.ca/site/commun/ml-fe/vol_12/vol12_17/1217_full.pdf.

intelligence could assist operational commanders with the coordination of C-IED operations as part of their COIN campaign.

Large numbers of law enforcement professionals would not have to be deployed in support of C-IED operations to have an effect at the operational level. Similar to the proposed concept of deploying various exploitation analysts in support of an exploitation lab, or any other technical analysis function, law enforcement agents could provide valuable inputs to the C-IED intelligence analysis efforts, as well as with C-IED operational planning.

Chapters 3 demonstrated the need to define IED systems. It also demonstrated the need to define these systems as part of a larger and interdependent system of multiple factors in the COIN campaign. Criminal intelligence analysts could assist intelligence staffs with this link analysis and provide direct guidance on the interpretation and assessment of IED system intelligence. In a similar vein, experienced law enforcement members could provide guidance and advice to operational commanders on how to best target identified systems, or how to better collect intelligence on these human networks. This type of advice and guidance would be leveraging law enforcement's in-depth knowledge and experience in defining and targeting human networks of various descriptions (gangs, drug trafficking networks, organized crime, terror groups, etc).

As this paper has previously discussed, COIN operations necessitate a deliberate and coordinated approach to targeting of IED systems as they are just one sub-set of the larger COIN dynamic. The successful integration at the operational level of WoG capabilities and collaboration could have an exponential effect for deployed forces. The

WoG approach at the operational level could also permit Canada to project unique capabilities abroad in pursuit of strategic objectives.

In the Canada First Defence Strategy, one of the mandated roles given to the CF in that document is "Contributing to International Peace and Security – Projecting Leadership Abroad", wherein one of the manners Canada may achieve this is by "leading a specific component of a multinational operation."[81] If Canada were to successfully integrate WoG expertise into its deployable exploitation capability, this may be one niche area that Canada could commit to a multinational operation. The benefits to coalition forces to be realized from the outputs of an effective exploitation capability are exponentially greater than the size of such a capability. If Canada could leverage its WoG expertise in this area, Canada would be able to make an extremely meaningful contribution to a multinational effort and at comparatively low cost in terms of personnel and money.

Whether or not Canada would pursue such an option remains to be seen. Important to this discussion, however, is the realization that a WoG approach to C-IED operations can extend beyond the strategic level. A truly WoG approach to C-IED operations at the operational level could extend from a coherent strategic approach and provide tremendous effect to Canadian military and civilian forces deployed around the world in an IED threat environment. A broad review of some benefits and risks of institutionalizing a WoG approach to C-IED operations will now be examined.

---

[81] Department of National Defence. *Canada First Defence Strategy*. Ottawa, ON: Government of Canada, 2008, 6-7, http://www.forces.gc.ca/site/focus/first-premier/June18_0910_CFDS_english_low-res.pdf (accessed January 8, 2010).

BENEFITS AND RISKS

Benefits

The obvious benefit in formalizing and institutionalizing a truly WoG approach to C-IED operations has been stated several times throughout this paper: strategic coherence. If this can be achieved the leveraging of talent, skills, expertise and technology from across the government should permit Canada to properly train and equip its forces to operate in an IED threat environment and allow deployed forces to deliver desired effect to the IED systems that employ these weapons. This would have the further benefit of increasing Canada's credibility among its allies as a contributing partner in the allied C-IED fight and would, therefore, have the spin-off benefit of potentially having increased access to allied C-IED information and cooperation.

Closer to home, the successful integration of all relevant government partners in the C-IED fight could assist in breaking down perceived cultural barriers and challenges that may be hampering other similar WoG efforts. Whether the issue is C-IED or anything else, there is always risk of inefficiency and waste when parallel organizations are conducting similar and complimentary activities in a 'stovepipe' fashion. In the seemingly overly bureaucratic and protectionist environment of Ottawa, a breakthrough in the area of C-IED could pave the way for increased collaboration in other critical areas.

More critically, however, the institutionalization of a WoG approach to C-IED would allow the CF and its WoG partners to capture key lessons learned in C-IED. Not only would this increase our preparedness to operate in IED threat areas, but it could also allow Canada to more easily adapt to any new evolving threat that may arise in the future.

With a WoG organization already in place to deal with the IED threat, it is conceivable that this same organization could provide a starting point to determine how to address any new or emerging threat. WoG solutions to a defined problem may be more efficiently achieved with the WoG C-IED architecture already in place.

Risks

Should Canada decide to not pursue a WoG approach to C-IED and not to formalize any such endeavour, then the best that Canada could hope to achieve is ad hoc collaboration. This may prove acceptable for short term or crisis response issues, but Canada would not achieve any synergies, or any pan-government coordination of C-IED activities. Therefore, Canada may miss opportunities to provide the best and most timely solutions to C-IED problems for its deployed forces. This would be symptomatic of a larger problem; a lack of government understanding of the FSE.

Chapter 3 highlighted some characteristics of the FSE and it also described the COE. If the FSE idea of failed and failing states with state and non-state actors is accepted, as well as the systems approach to the COE, then a failure to endorse any WoG effort would indicate a failure to understand or acknowledge how to achieve strategic objectives in the FSE. The government would run the risk of achieving strategic failure if it does not accept and embrace the idea that non-traditional inter-state problems may require non-traditional (WoG) approaches or solutions. Operational and tactical commanders must be given the proper tools to conduct operations in the COE in pursuit of national objectives.

CHAPTER 6 – CONCLUSION

This paper has discussed C-IED operations within the context of COIN in the complex COE. Key terminology in the C-IED lexicon was presented to establish a baseline understanding of C-IED issues. The discussion then transitioned to an examination of the COE as a complex system of systems and why the conduct of COIN operations in the COE requires national capabilities beyond those possessed by military forces. C-IED operations were then presented within the context of COIN and were demonstrated to be a sub-set of COIN operations. Like COIN operations, C-IED operations were also demonstrated to be activities that require capabilities from all relevant agencies of national power and some examples of specific capabilities were examined to demonstrate their utility to the C-IED fight. Finally, a discussion of strategic and operational level options to achieve WoG coherence in C-IED operations was presented.

The COE is an adaptive system of systems that is continually changing in response to changes in its components parts in the political, military, social, economic, information, infrastructure spheres. Any actions taken against any one or combination will have an effect on any one or combination of the other systems. With this type of dynamic characterizing the COE, the conduct of COIN operations cannot rely solely on military approaches and capabilities to achieve desired effects among the interrelated systems of the COE. With IEDs being widely employed in by insurgents in the COE, the targeting of IED systems must be a coordinated effort as part of the overall COIN campaign in order to ensure C-IED operations compliment COIN operations and do not have an adverse impact on overall objectives. The factors involved with the employment

of IEDs require capabilities from other government areas of expertise in order to be truly effective and stand a reasonable chance of success against IED systems.

This paper has demonstrated that Canada must apply a WoG approach to its C-IED efforts and must develop and maintain a WoG C-IED capability now and into the future. As Canada prepares to withdraw from Afghanistan in 2011, this argument gains an even greater sense of urgency before Canada loses what it has learned during its almost 10 year engagement in Afghanistan.

Canada possesses the tools and capabilities to apply a WoG approach to C-IED operations, but the lack of strategic coherence and governance across government has left WoG efforts to be ad hoc at best. Unifying all government stakeholders within a unified framework could permit Canada to achieve greater effects at the strategic level and, most importantly, at the operational level where it matters most.

The establishment of a strategic WoG organization, built upon the current CF C-IED TF, is recommended as the most expeditious and realistic manner in which to create this desired capability. The C-IED TF has been the lead agency within the CF for C-IED operations for three years and should be able to easily assume a larger WoG lead agency function on behalf of the DND and on behalf of the Government of Canada (GOC). The composition and manning of this new WoG C-IED TF is best determined by the applicable departmental experts, but it must be able to achieve strategic coherence for the GOC and it must also enable operational C-IED operations.

The focus of discussions in this paper has been on deployed expeditionary operations. While this is where the most urgent need currently resides, further research is recommended into the applicability of a WoG C-IED TF in the domestic context. If

Canada were to invest time, personnel and money to institutionalize C-IED for expeditionary operations, would there be collateral benefit for domestic C-IED? Would CF involvement create substantial legal questions and debate? The government and CF focus has been on IEDs encountered on deployed operations, but what could be leveraged by law enforcement in support of their operations? These questions warrant some research to determine if such WoG collaboration has to limited to international operations only.

There is no panacea in C-IED operations. No one piece of technology is going to negate the threat of IEDs. Destroying one IED system is not going to prevent another system from evolving and taking its place. The C-IED lines of operation must be viewed as mutually supporting activities that are best achieved through truly WoG means, and within the context of a larger COIN campaign. As Canada draws down and pulls out of Afghanistan over the next year and a half, Canada cannot afford to lose momentum in its C-IED fight as these weapons may appear in any theatre of operations in the future. A WoG approach to C-IED operations offers Canada its best opportunity to protect its forces and deter the use of IEDs. Canada cannot afford to put itself in a position to re-learn old lessons learned in blood.

BIBLIOGRAPHY

"Explosive Disposal Conference to Focus on IEDs." *The Maple Leaf*, May 6, 2009.

"MDA to Demonstrate Information Solution for Soldiers." *Canada NewsWire* (Jun 18, 2007): 1.

Acharya, Lalita. *Biometrics and Government*. Ottawa: Library of Parliament, 2006.

Army Lessons Learned Centre. "The Dispatches." Department of National Defence. http://armyapp.dnd.ca/allc-clra/Downloads/dispatches_e.asp (accessed April 14, 2010).

CACI International Inc and National Defense University. "Dealing with Today's Asymmetric Threat to U.S. and Global Security." Arlington, VA, 2008.

Caldwell, Wiiliam B. and Steven M. Leonard. "Field Manual 3-07, Stability Operations: Upshifting the Engine of Change." *Military Review* LXXXVIII, no. 4 (July-August, 2008): 56-63.

Canadian Explosives Research Laboratory. "Explosive Analysis." Government of Canada. http://www.nrcan.gc.ca/mms-smm/expl-expl/sci-sci-eng.htm (accessed May 1, 2010).

Chief of the Defence Staff. . *CDS Supplemental Directive - Enhancement of CF C-IED Capabilities in Afghanistan*, February 29, 2008.

Communications Research Centre. "Research and Development." Government of Canada. http://www.crc.gc.ca/en/html/crc/home/research/research (accessed April 23, 2010).

Communications Security Establishment Canada. "The Anti-Terrorism Act and CSEC's Evolution." Government of Canada. http://www.cse-cst.gc.ca/home-accueil/nat-sec/ata-lat-eng.html (accessed April 14, 2010).

Department of National Defence. *Canada First Defence Strategy*. Ottawa, ON: Government of Canada, 2008, http://www.forces.gc.ca/site/focus/first-premier/June18_0910_CFDS_english_low-res.pdf (accessed January 8, 2010).

———. "Canadian Forces Joint Doctrine Note: Canadian Forces Improvised Explosive Device (IED) Lexicon - DRAFT." Joint Doctrine Note, Ottawa.

———. "Fallen Canadians." Department of National Defence. http://www.forces.gc.ca/site/news-nouvelles/fallen-disparus/index-eng.asp (accessed May 19, 2010).

Federal Bureau of Investigation. "Investigative Programs Critical Incident Response Group." United States Government. http://www.fbi.gov/hq/isd/cirg/ncavc.htm#bau (accessed April 14, 2010).

Financial Transactions Analysis Centre. "Terrorist Financing." Government of Canada. http://www.fintrac-canafe.gc.ca/fintrac-canafe/1-eng.asp (accessed April 22, 2010).

Gompert, David, Gordon, John. *War by Other Means: Building Complete and Balanced Capabilities for Counterinsurgency*. Santa Monica, CA: RAND Corporation, 2008.

Independent Panel on Canada's Future Role in Afghanistan. *Independent Panel on Canada's Future Role in Afghanistan: Final Report*. Ottawa: Public Works and Government Services, 2008.

International Criminal Police Organization. "Criminal Intelligence Analysis." http://www.interpol.int/public/CIA/Default.asp (accessed April 14, 2010).

Joint Improvised Explosive Device Defeat Organization. "About JIEDDO." US Department of Defense. https://www.jieddo.dod.mil/about.aspx (accessed April 22, 2010).

———. "Attack the Network." US Department of Defense. https://www.jieddo.dod.mil/attack.aspx (accessed April 22, 2010).

Nagl, John A. *Learning to Eat Soup with a Knife*. Chicago, IL: University of Chicago Press, 2005.

NATO Joint Warfare Centre. "Joint Opeational Guideline for Counter-IED." Draft Publication, Stavanger, Norway.

Orchard, Phil. "Canada and the Changing Strategic Environment: The Canada First Defence Strategy and Beyond." UBC, 2008.

Royal Canadian Mounted Police. "Geographic Profiling." Government of Canada. http://www.rcmp-grc.gc.ca/tops-opst/bs-sc/geographic-g-profil-eng.htm (accessed April 14, 2010).

Staff. "Israel Finds another IED Along Eqyptian Border." *World Tribune*, April 9, 2010, http://www.worldtribune.com/worldtribune/WTARC/2010/me_israel0297_04_09.asp.

US Department of Defense. *Commander's Handbook for an Effects-Based Approach to Joint Operations* US Joint Forces Command, 2006.

———. *Joint Publication 3-24: Counterinsurgency Operations* US COIN Center, 2009.

———. . *Quadrennial Defense Review Report*. Washington, DC: US Department of Defense, 2006.

Whiteman, Shannon. "Improving Situational Awareness in the Counter-IED Fight with the Utilization of Unmanned Sensor Systems." Master's Thesis, Naval Postgraduate School, 2009.

Windsor, Lee, David Charters, and Brent Wilson, eds. *Kandahar Tour*. Mississauga, ON: Wiley, 2008.