National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

SHARPENING THE SPEAR: OPTIMIZING CANSOFCOM'S INTELLIGENCE FUNCTION TO MEET APPROACHING CHALLENGES

Major A.K. Brown

JCSP 39

Master of Defence Studies

Disclaimer

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

PCEMI 39

Maîtrise en études de la défense

Avertissement

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

Canada

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

MASTER OF DEFENCE STUDIES – MAÎTRISE EN ÉTUDES DE LA DÉFENSE

SHARPENING THE SPEAR : OPTIMIZING CANSOFCOM'S INTELLIGENCE FUNCTION TO MEET APPROACHING CHALLENGES

By Major A.L. Brown
Par le major A.L. Brown

Word Count: 18 820

Compte de mots : 18 820

ABSTRACT

Canadian Special Operations Forces Command (CANSOFCOM) is a potent national tool that is well-suited for prosecuting the emerging complex threats now visible on the horizon. To execute its mandate, however, the Command requires high-quality, precision intelligence. But good intelligence does not come cheap. And given the potentially high strategic stakes of CANSOFCOM operations, inadequate intelligence support could have serious negative results. As such, this paper considers how CANSOFCOM's intelligence establishment can be optimized to meet the future's predictably difficult challenges and deliver the high-calibre intelligence support the Command requires.

This paper argues that CANSOFCOM's intelligence function requires better-developed personnel and collection capabilities than those normally inherent to Canadian military intelligence organizations. In particular, the author reasons that the Command's intelligence establishment should design and implement a screening and training program for new personnel to produce the best possible intelligence work force. The author also argues for investments of effort and resources towards a vigorous liaison program that tightly networks CANSOFCOM intelligence with external intelligence partners and towards maintaining on-demand access to high-end collection capabilities in the domains of HUMINT, interrogation, Intelligence, Surveillance and Reconnaissance (ISR), and exploitation services.

Table of Contents

LIST OF ACRONYMS

AQ – Al Qaida

CCNS – Cabinet Committee on National Security

CDI – Chief of Defence Intelligence

CSEC – Communications Security Establishment Canada

CSIS – Canadian Security Intelligence Service

DDMA – Defence, Diplomacy and Military Assistance

DIMC – Defence Intelligence Management Committee

DOMEX – Document and Media Exploitation

F3EAD – Find, Fix, Finish, Exploit, Analyze, Disseminate

FMV – Full Motion Video

I&W – Indications and Warnings

ISR – Intelligence, Surveillance and Reconnaissance

JSOC – Joint Special Operations Command (U.S.)

PCO – Privy Council Office

RCMP – Royal Canadian Mounted Police

SOF – Special Operations Forces

SOIC – Special Operations Intelligence Centre

SOTF – Special Operations Task Force

WMD – Weapons of Mass Destruction

WME – Weapons of Mass Effect

INTRODUCTION

Canadian Special Operations Forces Command (CANSOFCOM) constitutes a valuable element of national military power that provides light, agile forces capable of deploying rapidly and delivering precision effects in high-risk environments. The Command's capabilities are likely to prove particularly relevant in an evolving global security environment increasingly characterized by complex conflicts fought by regular and non-state combatants, often in civilian centres where collateral damage concerns run high. Amongst the likely future threats to Canadian and Western interests are adversaries who employ asymmetric warfare to deter, intimidate, or wear down the will of Western governments and populations. These same adversaries will make every effort to remain invisible, avoiding confrontation with the West's overwhelming conventional military power. CANSOFCOM offers a potent and politically attractive option for combating such threats. Amongst many other things, the Command is capable of rapidly projecting elements to conduct difficult missions, employing force where necessary with remarkable precision to minimize collateral damage. CANSOFCOM can also help contain threats abroad by providing expert training and mentoring to friendly nations striving to build their own capabilities to deal with complex security threats.[1]

However, special operations forces (SOF) are dependent on high-quality, accurate intelligence.[2] Indeed, SOF units are known to be ravenous intelligence consumers due to

[1] Department of National Defence, *Canadian Special Operations Forces Command: An Overview* (Ottawa: Canadian Special Operations Forces Command, 2008), 6-7.

[2] *Ibid*., 8 and 15.

the complexity and high stakes of special operations.[3] To support its operations in the evolving and complex global security environment, then, CANSOFCOM requires well-developed intelligence machinery, oriented to evolving threats and capable of providing precise and actionable intelligence on clever, evasive enemies. At the same time, the Command's intelligence organization (henceforth referred to as its intelligence function) needs to avoid certain hazards known to promote intelligence failure, because the high stakes of CANSOFCOM operations mean that the consequences of an intelligence breakdown could be grave to the national interest. As such, the challenge for the Command's intelligence planners as they look to the future is how to build capacity to meet particularly demanding intelligence requirements while minimizing the potential for intelligence failure. Consequently, it is worthwhile to ask the question: how can CANSOFCOM's intelligence function be optimized to meet future requirements?

This paper argues that CANSOFCOM's intelligence function requires better-developed personnel and collection capabilities than Canadian military organizations normally possess. This argument will be supported by research showing that CANSOFCOM intelligence can realize its fullest potential to be a world-class intelligence support organization by investing effort and resources towards developing a highly-skilled personnel force, access to high-end information-gathering means, and well-refined operating procedures. Indeed, just as SOF in general require focused outlays to produce highly-capable units comprised of demonstrably talented, motivated people paired with cutting edge technology, so too does SOF's intelligence component. In fact, effective military intelligence support in any context requires investment in proportion to

[3] Lawrence E. Cline, "Special Operations and the Intelligence System," *International Journal of Intelligence and Counterintelligence* 18, no. 4 (2005): 575-576.

the military capability it supports.[4] And CANSOFCOM's world-class operators require, and deserve, nothing less than world-class intelligence support.[5] Such high-end intelligence, however, does not come cheap.

This paper broadly aligns to the themes of personnel and collection capabilities. It reasons that CANSOFCOM's intelligence function should rest on a foundation of high-performing personnel whose aptitudes for demanding intelligence work are proven through a carefully developed applicant screening process. Those found suitable for service should undergo training designed to prepare them for the unique and demanding challenges they will face supporting CANSOFCOM's commanders and operators. The long-term development of intelligence personnel should continue through immersion in a tailored CANSOFCOM intelligence culture that promotes attitudes and behaviours known to foster good intelligence work. The intelligence organization should be structured such that the weight of the personnel force is vested in unit-level close intelligence support, while a relatively lean J2 Staff focuses on meeting the commander's requirements, exercising functional oversight and conducting force development. Meanwhile, key focus areas for investing effort and resources should include a vigorous liaison program that networks CANSOFCOM intelligence tightly with other Canadian intelligence agencies and its close allied counterparts, and a plan to maintain on-demand access to high-end information gathering capabilities in the domains of HUMINT,

[4] Robert L. Hubbard, "Another Response to Terrorism: Reconstituting Intelligence Analysis for 21st Century Requirements," *Defense Intelligence Journal* 11, no. 1 (2002): 76-77.

[5] This paper is not the first to assert that CANSOFCOM requires high-calibre organic intelligence support. In 2006, Colonel J. Paul de B. Taillon (Adjunct Professor at the Royal Military College) argued that CANSOFCOM requires high-performing, integral intelligence support, capable of integrating and exploiting interagency collection expertise and providing sophisticated and actionable intelligence on complex adversaries. J. Paul de B. Taillon, "Canadian Special Operations Forces: Transforming Paradigms," *Canadian Military Journal* 6, no. 4 (2006): 71.

interrogation, Intelligence, Surveillance and Reconnaissance (ISR), and exploitation services.

It is necessary to limit this paper's scope to achieve an appropriate balance between depth and breadth. Therefore, some of the analysis presented will point to areas requiring further research. Furthermore, this paper is limited to a theoretical examination of how CANSOFCOM's intelligence function can be optimized through the best use of finite resources. As such, this paper does not examine, let alone critique, the Command's extant intelligence function. Similarly, there is no agenda here to argue for an increased establishment. Rather, this paper is a forward-looking endeavour that seeks to assess likely future intelligence challenges and define realistic solutions that respect the hard-won lessons of running effective intelligence organizations. This paper will be of no value if it does not respect the reality of the current resource-constrained environment. It therefore assumes that the Command's intelligence resources are fixed and suggests where finite resources and staff capacity might best be invested to achieve the greatest efficiencies. Some of the intelligence challenges examined here are not unique to CANSOFCOM, though they are examined from a CANSOFCOM perspective. Because such challenges are within the Command's ability to control, however, they merit inclusion in this paper—and the potential mitigating measures identified may very well be applicable to intelligence agencies in general.

This paper is based almost entirely on open-source academic and professional literature. Fortunately, a wide body of literature on intelligence matters allows for extraction of insight into select issues of interest. This paper's first chapter presents the key pieces of literature consulted for this study. Following this literature review, chapter

2 considers CANSOFCOM's future challenges in the context of the future security environment. Chapter 3 assesses the likely future intelligence tasks by considering how the intelligence function will need to support CANSOFCOM in meeting the challenges identified in chapter 2. From there, this paper's main section follows (chapter 4), assessing areas where investment of resources and effort would contribute to optimizing the intelligence function, with specific elements grouped under the headings of People, Process, and Structure.

CANSOFCOM is a flexible and highly-responsive strategic tool that supports government objectives by operating independently, in conjunction with conventional forces, with allied SOF, or in support of other government agencies. It provides the government with a rapidly deployable, agile, and self-sufficient military response capable of undertaking physically and politically risky operations. High quality intelligence plays a key role in this capability.[6] Therefore, how the Command's intelligence function can operate as effectively as possible within the constraints of finite resources merits close consideration. In short, this paper seeks to generate insight into how CANSOFCOM's intelligence function may be optimized to make it as capable as possible of meeting the Command's intelligence requirements in the future's complex battlespaces.

[6] Department of National Defence, *Canadian Special Operations Forces Command: An Overview*, 8.

CHAPTER 1—REVIEW OF PERTINENT LITERATURE

This chapter highlights the key pieces of literature consulted for this study. It begins by reviewing CANSOFCOM publications that articulate the Command's standing tasks and how the Command supports Canadian Forces (CF) objectives. The same documents are critical for understanding the cultural values that are fundamental to CANSOFCOM's effectiveness, as these values constitute the foundation upon which an enriched CANSOFCOM intelligence culture may be developed. Equally important to this study are other government documents that assess the future security environment, as they provide insight into future conflict areas where CANSOFCOM can expect to operate. They are therefore also useful for assessing the type of support CANSOFCOM's intelligence function will need to provide in the foreseeable future. Furthermore, a large body of scholarly literature dealing with a wide range of intelligence matters allows for inquiry into particular subjects of interest. To this end, this paper consults select pieces of academic work to develop insight into how CANSOFCOM's intelligence function can approach certain challenges, such as the recruiting and training of personnel, intelligence ethics, avoiding intelligence failures, effective targeting methodologies, and the strategic risks associated with HUMINT and interrogation operations.

This chapter reviews the key pieces of literature used for this study in the thematic order that organizes this paper: the Future Security Environment, the Likely Scope of Future Tasks for CANSOFCOM Intelligence, and Defining an Optimized Intelligence Organization in the domains of *People*, *Structure*, and *Process*.

The Future Security Environment

The nature of warfare in the post-Cold War era continues to evolve dramatically, prompting some militaries to exert considerable effort to comprehend the so-called "future security environment." An excellent example of such work is the Canadian Forces' *The Future Security Environment 2008-2030*, which provides a detailed analysis of future warfare's complexity. It assesses the likely operating environments (characterized as austere, urban, and littoral) and the wide range of state and non-state actors. Of particular importance, *The Future Security Environment* warns that future conflict may include "hybrid war," or a blend of conventional and unconventional forms of fighting.[7] Frank Hoffman provides a concise overview of the literature and professional thinking regarding hybrid conflict in *Hybrid Warfare and Challenges.*[8] The British Ministry of Defence's *Global Strategic Trends—Out to 2040* is also excellent, with detailed analysis that leads to very similar conclusions as the Canadian assessment—particularly with predictions of complex warfare involving a multitude of state and non-state actors in complex battlespaces—but boldly looking out ten years longer.[9] The Canadian Defence and Foreign Affairs Institute examines what future security threats will mean to Canada in *A Threatened Future: Canada's Future Strategic Environment and Its Security Implications*. Written by academics Gordon Smith, Denis Stairs, and the eminent Jack Granatstein, this publication assesses how future threats will

[7] Department of National Defence, *The Future Security Environment 2008-2030* (Ottawa: Chief of Force Development, 2009).

[8] Frank Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly* First Quarter, no. 52 (2009): 34-48.

[9] Ministry of Defence, *Global Strategic Trends – Out to 2040 (Fourth Edition)* (London: Development, Concepts and Doctrine Centre, 2010).

affect Canada's security and finds, amongst other things, that Canada will probably require more SOF to combat future challenges to Canadian interests.[10]

The Likely Scope of Future Tasks for CANSOFCOM Intelligence

To assess the nature of intelligence support CANSOFCOM will require in the future, it is necessary to appreciate what the Command may be expected to accomplish and how it sees itself operating. Consequently, the *CANSOFCOM Capstone Concept for Special Operations* is an important document, as it articulates the Command's overall role and general *modus operandi*. For example, the *Capstone Concept* describes CANSOFCOM's core tasks, including counter-terrorism, maritime counter-terrorism, and other high-value tasks assigned by the Canadian government such as Special Reconnaissance, Direct Action, Counter-Proliferation, and Defence, Diplomacy and Military Assistance (DDMA) missions. CANSOFCOM's ethos, a sub-set of CF ethos, is also described. Furthermore, the document emphasizes the central importance of people to the Command's culture of excellence. The *CANSOFCOM Capstone Concept* also stresses that the Command contributes to Whole of Government efforts and therefore must be a trusted, credible partner to other Canadian defence and security agencies. Finally, the *CANSOFCOM Capstone Concept* emphasizes the crucial role intelligence plays in enabling special operations.[11] All of these subjects are directly relevant to this study because they constitute the Command's fundamental foundations upon which the

[10] J.L. Granatstein, Gordon S. Smith, and Denis Stairs, *A Threatened Future: Canada's Future Security Environment and its Security Implications* (Calgary: Canadian Defence and Foreign Affairs Institute, 2007).

[11] Department of National Defence, *CANSOFCOM Capstone Concept for Special Operations* (Ottawa: Canadian Special Operations Forces Command, 2009).

intelligence function's evolving organization and development must be based. Colonel Mike Rouleau, whose long service with JTF 2 includes command of the unit, expands on some of these fundamental themes in *Special Operations Forces: Shaping the Area of Operations.* He emphasizes that high-calibre personnel are critical for CANSOFCOM's effectiveness, a theme that merits close consideration in the context of intelligence.[12]

Finally, to appreciate how CANSOFCOM is likely to operate in the future—particularly in the context of Whole of Government efforts—and to extrapolate accordingly how the intelligence function will need to support the Command, it is necessary to examine the Government of Canada's strategy for dealing with terrorism, *Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy*.[13] This very important document highlights the government's expectations of interagency and interdepartmental cooperation. Of significance to this paper, it also notes that CF counter-terrorism operations are enabled by robust intelligence collection and analysis capabilities.[14] Clearly, CANSOFCOM intelligence needs to live up to these expectations.

Defining an Optimized Intelligence Organization in the Domain of People

The aforementioned CANSOFCOM documents stress the importance of highly motivated, competent people to the Command's success. To contextualize this notion for the intelligence function, Professor Thomas Hammond (who at Michigan State University specializes in the scientific study of bureaucracies) provides a useful article

[12] Mike Rouleau, "Special Operations Forces: Shaping the Area of Operations," in *Special Operations Forces: A National Capability*, ed. Emily Spencer, 87-93 (Kingston, Ontario: Canadian Defence Academy Press, 2011).
[13] Ministry of Public Safety, *Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy* (Ottawa: Government of Canada, 2011).
[14] *Ibid*., 28.

called *Intelligence Organizations and the Organization of Intelligence.* Hammond contends that there is no single optimized model for organizing intelligence organizations, despite widespread attempts to find one based on, for example, centralized versus decentralized control or regional versus topical organization. He cites research suggesting that having good people is what truly makes an intelligence organization effective.[15]

Given the importance of personnel, then, and their principal output—analysis—it is useful to consider the scholarly literature regarding intelligence analysis issues. Professor Uri Bar-Joseph (Haifa University in Israel) shows that faulty analysis tends to be the most frequent cause of intelligence failure. He contends that analysts, to be good at their jobs, require particular traits such as being open to new information that does not match extant views. He also provides valuable insight into the classic traps analysts fall into, such as belief perseverance, group think, and tailoring intelligence to satisfy a user's agenda.[16] Bar-Joseph and Professor Rose McDermott (Brown University) provide further useful information on the importance of carefully developing competent analysts in *Change the Analyst and Not the System: A Different Approach to Intelligence Reform.* The authors emphasize that intelligence organizations should pay close attention to certain personality characteristics when recruiting, training and promoting personnel.[17] Dan Gardner provides a very useful appreciation of what is and is not possible when making predictive assessments, and how analysts can furnish decision-makers with useful forecasts, in *Future Babble: Why Expert Predictions Fail—and Why We Believe Them*

[15] Thomas H. Hammond, "Intelligence Organizations and the Organization of Intelligence," *International Journal of Intelligence and Counterintelligence* 23, no. 4 (2010): 683-686 and 703.

[16] Uri Bar-Joseph, "The Professional Ethics of Intelligence Analysis," *International Journal of Intelligence and Counterintelligence* 24, no. 1 (2011): 24-29.

[17] Uri Bar-Joseph and Rose McDermott, "Change the Analyst and Not the System: A Different Approach to Intelligence Reform," *Foreign Policy Analysis* 4, no. 2 (2008): 127-145.

Anyway.[18] Given the importance CANSOFCOM places on organizational culture, it is useful to consider how the Command's intelligence function can inculcate its members with an appropriately tailored culture. Professor Edgar H. Schein, whose has researched and taught extensively on organizational culture, provides useful information in *Organizational Culture and Leadership.* Of particular relevance to this study, Schein emphasizes the critical role of leadership in developing cultures that promote organizational success.[19] Professor William Nolte (University of Maryland) makes a compelling argument in *Ethics and Intelligence* that intelligence organizations must maintain high ethical norms because some intelligence activities, such as HUMINT, can be morally challenging.[20]

This literature will be useful for informing an assessment of how CANSOFCOM's intelligence function can recruit and train the right people and, through strong leadership, inculcate them with a tailored culture that, while entirely and firmly fastened to CANSOFCOM culture, further emphasizes sound analytical and ethical intelligence practices.

Defining an Optimized Intelligence Organization in the Domain of Process

This paper will emphasize the fundamental precept that the intelligence cycle's first step—direction, especially from commanders to their intelligence organizations—is critical for ensuring that the entire intelligence effort is applied efficiently against the

[18] Dan Gardner, *Future Babble: Why Expert Predictions Fail—and Why We Believe Them Anyway* (Toronto: McClelland and Stewart, 2010).

[19] Edgar H. Schein, *Organizational Culture and Leadership (Third Edition)* (San Francisco: Jossey-Bass, 2004), xi, 19, 23, 262 and 270.

[20] William M. Nolte, "Ethics and Intelligence," *Joint Force Quarterly* 54 (July 2009): 22-29.

commander's requirements. Indeed, Geraint Evans (an experienced British military intelligence officer) warns that intelligence failures can often be traced back to the direction issued to an organization or to a lack of precision in putting questions to intelligence agencies.[21] The implication is that intelligence organizations need to be proactive in involving their commanders in the intelligence cycle, seeking and revisiting direction to ensure that the intelligence effort provides precisely and only what the commander requires while avoiding effort that is, as Evans aptly describes, "pointless and self-serving."[22]

Given that the Canadian government demands that its intelligence agencies cooperate and collaborate, it is useful to assess the potential institutional obstacles that hinder such cooperation. Professor Greg Fyffe (University of Ottawa) provides an excellent account of the Canadian intelligence community's recent expansion and maturation in *The Canadian Intelligence Community After 9/11*. He emphasizes the critical importance for all intelligence agencies of maintaining healthy, routine relations with each other. However, he warns, the existence of individual oversight bodies for Canadian intelligence agencies tends to encourage separation.[23] Meanwhile, Stéphane Lefebvre, a strategic analyst at Defence Research and Development Canada (DRDC), notes that Canadian agencies—especially the RCMP and CSIS—do not gather information in the same manner. CSIS, for example, has a mandate to collect threat information and intelligence that is not intended to meet the standards required for

[21] Geraint Evans, "Rethinking Military Intelligence Failure—Putting the Wheels Back on the Intelligence Cycle," *Defence Studies* 9, no. 1 (2009): 34-35.

[22] *Ibid*., 34.

[23] Greg Fyffe, "The Canadian Intelligence Community After 9/11," *Journal of Military and Strategic Studies* 13, no. 3 (2011): 1-17.

judicial prosecution.[24] Agencies may therefore have differing perspectives of developing threats. The implication for CANSOFCOM intelligence is that it needs to be networked with each of Canada's principal intelligence gathering agencies, if the Command is to have the best possible understanding of threats that may activate CANSOFCOM involvement. Furthermore, Professor Martin Rudner (Carleton University) provides an excellent overview of Canada's Communications Security Establishment (CSEC) in *Canada's Communications Security Establishment, Signals Intelligence and Counter-Terrorism*. Rudner's description of CSEC's range of capabilities and access to allies' enormous capabilities, and of the agency's contributions to Canadian operations in Afghanistan, strongly suggests that CANSOFCOM should maintain particularly strong links with this important agency.[25]

Targeting—particularly the capture/kill of terrorists or insurgents—is practically certain to be a CANSOFCOM mission in the future. This paper will therefore exploit the professional and academic literature regarding SOF targeting processes. Charles Faint and Michael Harris, who are American military intelligence and SOF officers respectively, argue that the F3EAD cycle (find, fix, finish, exploit, analyze, and disseminate) is a particularly effective targeting process due to its fusion of the intelligence and operations functions. Their article *F3EAD: Ops/Intel "Feeds" the SOF Targeting Process* provides a detailed and up-to-date examination of how this cycle functions effectively.[26] Chief Warrant Officer 4 Jimmy Gomez of the U.S. Army,

---

[24] Stéphane Lefebvre, "Canada's Legal Framework for Intelligence," *International Journal of Intelligence and Counterintelligence* 23, no. 2 (2010): 254.

[25] Martin Rudner, "Canada's Communications Security Establishment, Signals Intelligence and Counter-Terrorism," *Intelligence and National Security* 22, no. 4 (2007): 473-490.

[26] Charles Faint and Michael Harris, "F3EAD: Ops/Intel Fusion "Feeds" the SOF Targeting Process," *Small Wars Journal* 8, no. 1 (2012). Last accessed 10 October 2012, http://50.56.4.43/jrnl/art/f3ead-opsintel-fusion-%E2%80%9Cfeeds%E2%80%9D-the-sof-targeting-process.

however, warns that while F3EAD is excellent for quick capture/kill missions, the older D3A cycle (decide, detect, deliver, and assess) is better for campaign planning.[27] This paper will consider both arguments for their relevance to CANSOFCOM.

Finally, the issue of intelligence oversight has gained high attention in Canada during the past decade owing to increased national investments in intelligence and security. Jacques Shore, a lawyer with extensive experience with the Federal Solicitor General and the Security Intelligence Review Committee (SIRC), examines Canadian intelligence oversight regimes in *Intelligence Review and Oversight in Post-9/11 Canada* and emphasizes the importance of effective oversight of intelligence activities, a notion relevant to this study given the potentially sensitive intelligence activities CANSOFCOM may engage in.[28]

The aforementioned literature will be useful for understanding the processes an optimized CANSOFCOM intelligence function might employ, including targeting methodology, robust linkages with agencies that track terrorist threats, and respect for policy and oversight mechanisms that ensure intelligence agencies function within Canadian law.

Defining an Optimized Intelligence Organization in the Domain of Structure

Recent literature on successful intelligence practices strongly indicates that if CANSOFCOM's intelligence function is to provide the best possible all-source intelligence support, it requires on-demand access to several particularly important

[27] Jimmy A. Gomez, "The Targeting Process: D3A and F3EAD," *Small Wars Journal* 7, no. 7 (2011): 13-14.
[28] Jacques J.M. Shore, "Intelligence Review and Oversight in Post-9/11 Canada," *International Journal of Intelligence and Counterintelligence* 19, no. 3 (2006): 456-479.

intelligence collection capabilities, including HUMINT, interrogation, SIGINT, and exploitation of captured material. However, the literature also shows that there are serious risks associated with some of these disciplines that CANSOFCOM's intelligence function should respect.

Professor Robert Betts (Columbia University) emphasizes in *Fixing Intelligence* that HUMINT is critical for intelligence penetration of terrorist groups and for identifying group members and their plans. He warns that developing a HUMINT capability, however, is neither easy nor inexpensive.[29] Professor Thomas Mahnken provides insight into the serious risks associated with HUMINT in *Spies and Bureaucrats: Getting Intel Right*, noting that human sources should always be treated with suspicion because they are engaged in betrayal, they may be telling handlers what they wish to hear, or they may simply be passing on inaccurate information.[30] Similarly, Professor Peter Gill (Liverpool John Moores University) warns that using informers has the potential to result in charges of unethical information gathering that embarrass the government, as occurred with Special Branch operations in Northern Ireland that allegedly turned a blind eye to serious crimes committed by informers.[31]

The scholarly and professional literature indicates that interrogation is another highly important collection method, though its users should consider the significant risks involved with it. Professor Arthur Hulnick (Boston University) argues in *What's Wrong with the Intelligence Cycle* that interrogation is a proven means of acquiring valuable

[29] Robert K. Betts, "Fixing Intelligence," *Foreign Affairs* 81, no. 1 (2002): 46.
[30] Thomas G. Mahnken, "Spies and Bureaucrats: Getting Intel Right," *Public Interest* 159, no.1 (2005): 37.
[31] Peter Gill, "Security Intelligence and Human Rights: Illuminating the 'Heart of Darkness'," *Intelligence and National Security* 24, no. 1 (2009): 78-102

information, using methods that cause no harm to prisoners.[32] The U.S. Department of Defense's *Final Report on the Independent Panel to Review DoD Detention Operations* likewise claims that interrogation has proven an important source of intelligence, with interrogation-derived information being used to disrupt terrorist operations and to ascertain how the 9/11 attacks were planned. The same report, however, warns that interrogation is potentially an ethically challenging activity that if not carefully managed risks conduct society would not condone.[33] Professors Len Scott and Gerald Hughes (both of Aberystwyth University) remind readers in *Intelligence in the Twenty-First Century: Change and Continuity or Crisis and Transformation* that the British government suffered significant public embarrassment in the 1970s as a result of army interrogation methods in Northern Ireland that brought charges of abuse against the British government in the European Court of Human Rights.[34]

The value of exploiting captured material for its intelligence value has gained increasing attention since 9/11, suggesting that "exploitation" will be another especially important intelligence discipline in the future. For example, Charles Faint makes a very strong case for institutionalizing policy and training for document and media exploitation (DOMEX) in the U.S. intelligence community, given the enormous intelligence value DOMEX has provided since 9/11.[35] Lieutenant General Thomas Metz (Commander Multi-National Corps Iraq from May 2004 to February 2005) *et al* offer a similar perspective in *OIF II: Intelligence Leads Successful Counterinsurgency Operations*,

---

[32] Arthur S. Hulnick, "What's Wrong with the Intelligence Cycle," *Intelligence and National Security* 21, no. 6 (2006): 971.

[33] Department of Defense, *Final Report of the Independent Panel to Review DoD Detention Operations* (Arlington, VA: Department of Defense, 2004): 64-65, and Annex H (pg 1).

[34] Len Scott and R. Gerald Hughes, "Intelligence in the Twenty-First Century: Change and Continuity or Crisis and Transformation," *Intelligence and National Security* 24, no. 1 (2009): 16-17.

[35] Charles D. Faint, "DOMEX : The Birth of a New Intelligence Discipline," *American Intelligence Journal* 29, no. 1 (2010): 65-69.

reporting that DOMEX has become an important enabler for target development and execution.[36]

In summary, a wide body of scholarly and professional literature exists, much of it based on experience since 9/11, which one can use to explore select intelligence topics of interest. For the purposes of this paper, it is first necessary to consult CANSOFCOM documents that describe the Command's mission sets as well as literature that assesses the future security environment in which CANSOFCOM will operate. From there, one can assess the intelligence tasks CANSOFCOM's intelligence practitioners will need to execute. Then, exploiting the scholarly and professional literature regarding aspects of particular interest to CANSOFCOM's intelligence function, one can investigate how CANSOFCOM can optimize its intelligence organization to be the efficient, high-performing entity it needs to be.

[36] Lieutenant General Thomas F. Metz, Colonel William J. Tait and Major J. Michael McNealy, "OIF II: Intelligence Leads Successful Counterinsurgency Operations," *Military Intelligence Professional Bulletin* 31, no. 3 (2005): 12.

CHAPTER 2—CANSOFCOM AND THE FUTURE SECURITY ENVIRONMENT

To understand the future challenges CANSOFCOM's intelligence function will likely face, it is necessary first to consider the operating environment in which the Command will operate. Therefore, this chapter examines the future security environment's main characteristics as forecast by the military and academic communities, focusing particularly on those aspects that pertain to CANSOFCOM. This chapter will also draw preliminary conclusions relevant to CANSOFCOM's intelligence function.

Tomorrow's Battlespace: Main Characteristics of the Future Security Environment

The likelihood of traditional, inter-state conventional warfare will probably continue to decline as a result of globalization and the interdependence of global markets. However, conflict in the foreseeable future—that is, for the next two to three decades, as assessed by agencies such as the CF and others—is likely to be a complex blend of conventional and unconventional warfare.[37] Such "hybrid warfare" may be practiced by both state and non-state actors.[38] In fact, the blurring of regular and irregular forms of warfare will result partly from states that develop irregular warfare capabilities to supplement their conventional arsenals. Already, nations such as China and Iran have begun to consider how to use unconventional methods to fight conventionally superior

[37] Department of National Defence, *The Future Security Environment 2008-2030*, 6.
[38] *Ibid*., 81 and Hoffman, *Hybrid Warfare and Challenges*, 34-48.

forces.[39] Meanwhile, non-state actors are likely to employ hybridized methods of warfare by developing conventional capabilities for their irregular forces. Hezbollah demonstrated such a tendency in 2006 when its guerillas in Lebanon fought Israeli forces with conventional systems such as unmanned aerial vehicles and stand-off missiles.[40]

In future hybrid wars, asymmetric tactics will likely be commonplace as conventionally disadvantaged groups attempt to establish balance by avoiding their opponents' conventional military strength while seeking targetable weaknesses. Indeed, competent enemies of Western nations understand that it would be foolish to seek decisive engagement with Western forces in traditional force-on-force clashes.[41] Defence analysts expect terrorism to be a particularly common asymmetric tactic. In fact, globalization is already making terrorism an increasingly attractive option for non-state actors. The Internet and increased trans-national links between groups have empowered terrorists to recruit, train, communicate, and plan on a global basis. At the same time, the Internet has created huge international audiences for terrorist attacks, making terrorism increasingly effective and cheap.[42]

Canada is unlikely to be safe from future terrorist threats. Sunni extremism is but one example of emerging terrorist threats to Canadian interests. Sunni terrorist groups include Al Qaida (AQ) and its franchises, such as Al Qaida in the Arabian Peninsula (AQAP) which in December 2009 attempted to bomb Northwest Airlines Flight 253 in Canadian airspace, or Al Qaida in the Islamic Maghreb (AQIM) which in 2008 kidnapped two high-ranking Canadian officials, holding them for ransom for three

[39] For China, see Thomas Owens Mackubin, "Reflections on Future War," *Naval War College Review* 61, no.3 (2008): 72. For Iran, see Marc Lindemann, "Laboratory of Asymmetry: The 2006 Lebanon War and the Evolution of Iranian Ground Tactics," *Military Review* 90, no. 3 (2010): 110-111.

[40] Ministry of Defence, *Global Strategic Trends,* 84.

[41] Department of National Defence, *The Future Security Environment*, 81.

[42] *Ibid.*, 82-83.

months. Another AQ-affiliated group, the Somalia-based Al Shabaab, has attracted Canadian citizens to join its ranks.[43] Even within Canada, dissatisfied religious, racial and ethnic groups—some including second and third generation Canadians known to be sympathetic to the terrorists who attacked Westerners in London and Madrid—harbour potential anger over Canadian policies that may prompt some angry individuals to turn to terrorism.[44] Meanwhile, some radicalized Canadians have travelled abroad to train and fight with Sunni terrorist groups in Pakistan, Yemen, Somalia and North Africa. Consequently, Canadian authorities remain concerned that such individuals might return to Canada to carry out operations or encourage others to join their ranks.[45] In addition, certain non-AQ international terrorist groups threaten Canadian interests, as they have for decades, as exemplified by the Sikh extremists' bombing of an Air India flight in 1985 that killed 329, including 280 Canadians.[46]

Another key aspect of the future security environment is that conflict will increasingly involve non-state actors, such as militia groups, warlords, rebel movements, radical religious groups, or gangs and bandits. These groups will probably not respect the laws and conventions that constrain state militaries by governing the use of force. They will likely attempt to hide within the civilian population and will therefore be difficult to identify.[47] Furthermore, serious threats to national security will increasingly come from transnational actors, or well-networked groups that operate internationally by exploiting the advantages of rapid global travel, modern communications, and the growth of globalized financial systems. The implication is that transnational threats will only be

[43] Ministry of Public Safety, *Building Resilience Against Terrorism*, 7.
[44] Granatstein, Smith, and Stairs, *A Threatened Future*, 14 and 20.
[45] *Ibid*.
[46] Ministry of Public Safety, *Building Resilience Against Terrorism*, 8.
[47] Department of National Defence, *The Future Security Environment*, 8 and 79-80.

neutralized by transnational responses, as no single state will be able to do the job alone.[48] Overall, the increasing presence of non-state, non-uniformed combatants will present a challenge to professional forces that must discriminate between adversaries and non-combatants.

Conflict in the future security environment is likely to occur in congested battle spaces, especially urban and littoral areas. Urbanization is an ongoing phenomenon analysts project will continue intensifying. In 2006, urban dwellers outnumbered the world's rural population, and by 2040, 65 per cent of the world will probably be urbanized.[49] Many urban areas will be massive built-up zones in the developing world. By 2025, 75 per cent of the world's "large cities" (with populations between five and ten million) will be in developing nations, as will 80 per cent of all "mega cities" (with populations in excess of ten million).[50] Congested battle spaces will also emerge in littoral regions, where already today three quarters of the global population and 80 per cent of all cities exist.[51]

Such congested battle spaces will have serious implications for military planners. Western forces will face difficult challenges in identifying adversaries and discriminating them from the civilian populations in which they hide. Furthermore, given the intermixing of adversaries and civilians, the capability to use force with precision will be essential for avoiding collateral damage.[52] For these reasons, CF planners already

[48] William J. Lahneman, "The Need for a New Intelligence Paradigm," *International Journal of Intelligence and Counterintelligence* 23, no. 2 (2010): 201.
[49] Ministry of Defence, *Global Strategic Trends*, 99.
[50] Department of National Defence, *The Future Security Environment*, 22.
[51] Department of National Defence, *The Future Security Environment*, 9 and 17.
[52] Ministry of Defence, *Global Strategic Trends*, 88-89 and 99.

recognize the challenging requirement to be capable of operations in urban and littoral regions.[53]

Implications for CANSOFCOM's Intelligence Function

This overview of the future security environment points towards future battlespaces that have high potential for being chaotic and complex, with state and/or non-state adversaries who are decentralized, live and operate amongst civilian populations to avoid the overwhelming strength of conventional forces, and fight using asymmetric means. Such an operating environment is precisely the type for which CANSOFCOM is optimized due to its agility, technological edge, and—above all—its high levels of operator training and cognitive ability.[54] However, given that CANSOFCOM operations are dependent on intelligence,[55] the future is certain to hold significant challenges for the Command's intelligence function.

For example, the globalized nature of future threats will require globalized responses. No single nation, and certainly no single agency, will be unilaterally capable of defeating transnational threats. This will make it necessary for CANSOFCOM to increase ties with trusted allies.[56] By extension, CANSOFCOM intelligence will need to

[53] *Ibid*., 34.
[54] Department of National Defence, *Canadian Special Operations Forces Command: An Overview*, 6.
[55] Department of National Defence, *CANSOFCOM Capstone Concept for Special Operations*, 21.
[56] In fact, opportunities to increase relationships with the U.S. already appear to manifesting. On 22 February 2013, Admiral Bill McRaven, Commander of U.S. Special Operations Command (SOCOM), stated during a speech to a Conference of Defence Associations meeting in Ottawa that allies should tighten relationships between their SOF establishments because the challenges of terrorism and containing instability are too big for any single nation—including the U.S.—to deal with alone. The Associated Press, "U.S. Admiral Calls for Alliance of Special Forces," last accessed 24 February 2013, http://www.cbc.ca/news/canada/story/2013/02/23/us-special-operations-command-us.html.

work closely with foreign counterparts as Canada contributes to international responses to extremism and conflict. This suggests that CANSOFCOM intelligence needs to maintain credibility as a trusted, competent partner to important allies. Such relations need to be maintained as standing arrangements, as creating well-functioning partnerships after a crisis erupts would prove difficult and time-consuming. Similarly, the terrorist threat to Canada suggests that CANSOFCOM intelligence needs to maintain a standing, robust liaison network with numerous domestic agencies that track potential threats.

The probability of highly congested battle spaces poses other significant intelligence challenges. Locating and tracking adversaries with the degree of precision required to cue SOF operations will require a host of dedicated collection capabilities. Robust aerial ISR packages, capable of providing persistent collection (the "unblinking eye") at the tactical level, will be necessary. Other support will be required from national agencies that provide strategic intelligence collection services.

However, such tactical ISR and strategic technical capabilities will not be enough. Indeed, the commonly used technical collection means—including overhead imaging and signals intelligence—are already seeing limitations against terrorist groups. A great deal of information regarding technical collection has become public knowledge, permitting adversaries to take countermeasures. Terrorists generally know, for example, not to use cell phones or to use fibre optic cables or encryption for sensitive communications. Sophisticated adversaries can even ascertain satellite overflight schedules and avoid conducting observable activities during vulnerable periods.[57] Consequently, intelligence

[57] Betts, *Fixing Intelligence*, 46.

penetration of adversarial groups will also require non-technical collection methods that adversaries will always remain vulnerable to, such as HUMINT and interrogation.

Finally, providing the high-quality, accurate intelligence CANSOFCOM will require for operations in complex environments will necessitate a high standard of intelligence analysis. From conducting Intelligence Preparation of the Battlespace (IPB) in complex and chaotic urban and littoral areas, to managing collection feeds and developing meaningful and predictive intelligence assessments, analysts will need to be very high performers. This suggests that CANSOFCOM's intelligence function would benefit from investing in recruiting the right people and developing them to their fullest potential.

This chapter's findings, as summarized in table 2.1, need to be matched against the specific tasks CANSOFCOM can expect to execute in the future, which is the focus of the next chapter.

Table 2.1—Summary of Implications of the Future Security Environment for CANSOFCOM Intelligence

Ser	Factor	Deduction
1	Adversary activities will transcend national borders, requiring global responses.	Requirement to maintain standing liaison with international partners with whom CANSOFCOM may operate.
2	Ongoing threat of terrorism within Canada.	Requirement to maintain standing liaison and close relations with numerous Canadian security and intelligence agencies.
3	Requirement to locate and track adversaries in congested battlespaces.	Requirement for on-demand access to robust, leading edge ISR.
4	Limitations of aerial ISR platforms owing to the physical complexity of dense urban areas and knowledgeable adversaries that take effective countermeasures to technical	Requirement for on-demand access to robust HUMINT capability to penetrate adversary organizations.

	collection platforms.	
5	Difficulty in discriminating adversaries from civilians.	Requirement for on-demand access to robust HUMINT capability for locating and identifying adversaries.
6	Very high standard of intelligence analysis required to process masses of complex data and to produce precision intelligence and meaningful predictive analysis.	Requirement for investment in recruiting and training of analysts.

CHAPTER 3—THE SCOPE OF LIKELY FUTURE TASKS FOR CANSOFCOM INTELLIGENCE

Having deduced in chapter 2 a preliminary set of implications the future security environment has for CANSOFCOM intelligence, it is necessary to refine and deepen the assessment of future intelligence challenges. This chapter does so by considering the Command's standing core tasks in the context of the future security environment, and how the intelligence function will be required to support those tasks.

Standing CANSOFCOM Tasks and the Future Security Environment

The mission of CANSOFCOM is to "provide the Government of Canada with agile, high-readiness Special Operations Forces capable of conducting special operations across the spectrum of conflict at home and abroad."[58] To accomplish this mission, the Command organizes, trains and equips its units to accomplish three core tasks:

Counter-Terrorism Operations. This task includes preventing, deterring, pre-empting and responding to terrorism. CANSOFCOM conducts counter-terrorism operations both in Canada (always in support of law enforcement) and abroad. Counter-terrorism is usually offensive in nature and includes such missions as hostage rescue, recovering sensitive material, or conducting strikes on terrorist infrastructure.[59] Intelligence support to counter-terrorism operations is intensive. In fact, Canada's national counter-terrorism strategy recognizes that intelligence cues military counter-

[58] Department of National Defence, *CANSOFCOM Capstone Concept for Special Operations*, 8.
[59] *Ibid*.

terrorism operations, necessitating significant intelligence collection and analysis support.[60] And, as the previous chapter notes, terrorism is likely to remain a threat with domestic and international dimensions. As such, CANSOFCOM's domestic counter-terrorism role in support of law enforcement will remain important, while expeditionary counter-terrorism operations, including hostage rescue, will continue to be a potential mission. Already today, the kidnapping abroad of Westerners (including Canadians) is a serious problem. In the past decade, religious extremists have significantly increased kidnapping Western victims. And data suggests that terrorist-related kidnapping will not abate.[61] The implications for CANSOFCOM are potentially quite challenging. The Command, if it is to be capable of prosecuting counter-terrorism missions abroad, needs to be capable of geo-locating and tracking targets that move frequently and make every effort to avoid detection. Similarly, if the mission is hostage rescue, finding hostages held by adversaries determined to keep their location secret may prove especially difficult.

Maritime Counter-Terrorism Operations. Counter-terrorism operations in the maritime environment are exceptionally complex and require a great deal of skill, owing to the intricacy of inserting, fighting, and extracting forces in the prosecution of targets at sea.[62] The previous chapter noted that terrorism will be a significant feature of future battlespaces and that conflicts will occur in congested littoral regions. Maritime counter-terrorism will therefore remain an important task, and could include expeditionary

[60] Ministry of Public Safety, *Building Resilience Against Terrorism*, 28.
[61] James Forest, "Global Trends in Kidnapping by Terrorist Groups," *Global Change, Peace & Security* 24, no. 3 (2012): 311, 320 and 329.
[62] Department of National Defence, *CANSOFCOM Capstone Concept*, 8.

missions in regions where extremists' areas of operation span inland and offshore zones. The current volatile situations around the Horn of Africa and coastal Nigeria underscore the viability of this notion.

High Value Tasks. These refer to other missions, in Canada or abroad, the government may assign to the Command. They include a wide range of possible missions, such as counter-proliferation of Weapons of Mass Effect (WME), Special Reconnaissance to acquire information of strategic or operational importance, Direct Action (short term, precision operations to "seize, destroy, capture, exploit, recover or damage designated targets"), and Defence, Diplomacy, and Military Assistance (DDMA) operations that contribute to nation-building programs with military advice, training and assistance.[63] High Value Tasks may be assigned to CANSOFCOM owing to its wide range of kinetic and non-kinetic capabilities, such as surveillance and reconnaissance that provides senior decision makers with timely and accurate ground truth or missions that require the precise use of force to minimize collateral damage.

In addition to its readiness to conduct these standing tasks, CANSOFCOM fully subscribes to the principal of supporting Whole of Government national security efforts.[64] This is consistent with the national counter-terrorism strategy which emphasizes that close interagency efforts are essential to achieving the most effective counter-terrorism efforts possible. The strategy assigns counter-terrorism roles to a wide range of federal departments and agencies with which CANSOFCOM may need to interact (figure 3.1).

[63] *Ibid.*
[64] *Ibid*., 5.

Federal Agencies with Assigned Counter-Terrorism Roles

- Canadian Border Services Agency (CBSA)
- Canadian Air Transport Agency (CATSA)
- Department of Finance
- Department of Foreign Affairs and International Trade (DFAIT)
- Department of Justice
- The Canadian Forces
- Financial Transactions and Reports Analysis of Canada (FINTRAC)
- Government Operations Centre (GOC)
- Health Canada
- Integrated Terrorism Assessment Centre (ITAC)
- Privy Council Office (PCO)
- Public Health Agency of Canada (PHAC)
- Public Prosecution Service of Canada
- Public Safety Canada
- Royal Canadian Mounted Police
- Transport Canada

Figure 3.1
Source: Ministry of Public Safety, *Building Resilience Against Terrorism*, 11 and 27-30.

Again, then, it is clear that CANSOFCOM intelligence personnel need to be prepared to work closely with other agencies, collaborating in a substantive manner that contributes to mission success. This idea is not a truism to be taken lightly, but rather deserves close consideration, particularly given the well-known phenomenon that interagency cooperation in any nation is easily and often undermined by friction and competition.

It is clear that the future security environment will hold considerable challenges for CANSOFCOM intelligence in supporting the Command's execution of tasks. For example, successfully dismantling an extremist or insurgent network—arguably a mission of high likelihood—involves targeting individuals with important roles. The difficulty, experience shows, is developing an understanding of an adversary's network in order to identify key nodes for targeting purposes and to determine how an individual's

removal will harm the network (as opposed to creating space for a more competent or extreme individual to occupy).[65] Furthermore, once a network is understood and the targets identified, finding the individuals selected for prosecution is inherently difficult. Recent experience shows that the "find" phase of targeting, which falls to the intelligence function, is perhaps the most difficult targeting phase, as human targets are particularly elusive.[66] Finding hostages will be equally difficult.

Deductions for the CANSOFCOM Intelligence Function

Two major deductions can be drawn from juxtaposing CANSOFCOM's core tasks with forecasts of the future security environment. First, CANSOFCOM intelligence must be accustomed to operating in Whole of Government contexts on a standing basis, before crises occur. Second, the intelligence function must be prepared to support expeditionary counter-terrorism missions, including maritime counter-terrorism and hostage rescue, which are bound to be complex. Therefore, a proven intelligence methodology is required for finding and tracking targets and hostages in austere and complex (eg. urban) environments. These deductions demand further consideration to inform the next chapter's assessment of how the CANSOFCOM intelligence function should be optimized.

CANSOFCOM intelligence personnel need to be highly adept at working in multi-agency contexts. This may require determination to overcome the bureaucratic

[65] Matt Frankel, "The ABCs of Targeting: Key Lessons from High Value Targeting Campaigns Against Insurgents and Terrorists," *Studies in Conflict and Terrorism* 34, no. 1 (2011): 26.

[66] Aki Peritz and Eric Rosenbach, *Find, Fix, Finish: Inside the Counterterrorism Campaigns that Killed Bin Laden and Devastated Al-Qaeda* (New York: PublicAffairs Books, 2012), 5.

frictions and inertia that notoriously plague Whole of Government efforts. It will certainly require that personnel intimately understand the greater intelligence and security community, how it functions, and the specific roles, strengths and weaknesses of each agency. There must be a mature understanding of where the potential friction points lie between agencies and what CANSOFCOM intelligence must do to maintain standing as a trusted, credible partner. And there must be active interpersonal connections, the lifeblood of effective cooperation that can only be maintained through a vigorous and sustained effort to maintain strong ties. All this is necessary so that when the time comes to operate, CANSOFCOM's intelligence is running at maximum efficiency, not burning valuable time and energy learning about, and integrating into, the greater Whole of Government community.

The potential for expeditionary maritime counter-terrorism operations suggests particular intelligence challenges. CANSOFCOM intelligence will need to maintain the ability to find and track sea-borne targets and provide basic but vital information on battlespace characteristics needed at the tactical level, such as meteorological and oceanographic data. All of this will be necessary in austere regions where data sets and historical trends may be scarce or difficult to access.

Finally, CANSOFCOM intelligence should consider exactly how it will locate and track targets to cue operations such as raids on terrorist nodes and expeditionary hostage rescue operations. This is clearly a function of targeting. It is suggested that CANSOFCOM intelligence should institutionalize expertise in the F3EAD doctrine that Western militaries are increasingly adopting because of its proven effectiveness.

F3EAD is a targeting process that has proven particularly useful in recent years for prosecuting missions against human targets, often referred to as "man-hunting." The process is designed to fuse the operations and intelligence functions: commanders determine targeting priorities that drive intelligence efforts to identify a target (*find*), intelligence locates the target (*fix*), operations apply an effect against it (*finish*), intelligence analyzes recovered personnel and material (*exploit/analyze*) and shares the results as widely as possible (*disseminate*). F3EAD has evolved into a refined process based on experience and best-practices developed around the world. Canada's closest allies are increasingly adopting it as standard practice. U.S. forces now teach it at the Military Intelligence Officer Basic Course and at eleven courses at the John F. Kennedy Special Warfare Center and School. Furthermore, the Joint Special Operations Command (JSOC) Intelligence Brigade employs the F3EAD cycle,[67] while the British Army has formally integrated F3EAD into its counter-insurgency doctrine.[68]

Table 3.1 summarizes this chapter's findings.

Table 3.1—Summary of Challenges for the Intelligence Function in Supporting CANSOF Operations in the Future Security Environment

Ser	Factor	Deduction
1	CANSOFCOM missions will be conducted in support of Whole of Government efforts.	The intelligence function should invest effort to guarantee its status as a respected, credible and effective partner within the national security and intelligence community.

[67] Charles Faint and Michael Harris, "F3EAD: Ops/Intel Fusion "Feeds" the SOF Targeting Process," *Small Wars Journal* 8, no. 1 (2012). Last accessed 10 October 2012, http://50.56.4.43/jrnl/art/f3ead-opsintel-fusion-%E2%80%9Cfeeds%E2%80%9D-the-sof-targeting-process.

[68] Ministry of Defence, *British Army Field Manual Volume 1 Part 10: Countering Insurgency* (Warminster: Land Warfare Centre, 2009), 5-5 to 5-10.

2	High potential for expeditionary maritime CT missions.	Require capability to support Maritime CT operations by finding and tracking sea-borne targets and by providing maritime battlespace conditions in austere regions.
3	High potential for CANSOFCOM tasks to prosecute terrorist/extremist targets, including possible hostage rescue missions.	Doctrine required to locate and track highly evasive human targets and to locate hostages. Recent Western experience suggests F3EAD is an ideal doctrine.

The findings at Table 3.1, when combined with the deductions made at the end of chapter 2 (Table 2.1), highlight broad areas where the CANSOFCOM intelligence function should consider investing resources and effort (presented in table 3.2 below). These combined deductions will be used to inform a detailed analysis of how the CANSOFCOM intelligence function can be optimized for operations in the future security environment, which is the aim of the next chapter, this paper's main section.

Table 3.2—Consolidated Deductions of CANSOFCOM Intelligence Function Requirements for Supporting Operations in the Future Security Environment

Ser	Key Deductions	Broad Investment Area
1	Requirement to maintain standing liaison with international partners with whom CANSOFCOM may operate.	Standing and robust liaison with domestic and international partners.
2	Requirement to maintain standing liaison and close relations with numerous Canadian security and intelligence agencies.	
3	Requirement to guarantee CANSOFCOM intelligence function's status as a respected, credible and effective partner within the national security and intelligence community.	
4	Requirement for on-demand access to robust, leading edge ISR.	Collection capabilities.
5	Requirement for on-demand access to robust HUMINT capability to penetrate adversary organizations.	

6	Requirement for on-demand access to robust HUMINT capability to provide positive identification of adversaries.	
7	Require capability to support Maritime CT operations by finding and tracking sea-borne targets and by providing maritime battlespace conditions in austere regions.	
8	Requirement for investment in recruiting and training of analysts.	Personnel.
9	Require doctrine and capability to locate and track highly evasive human targets and to locate hostages. Experience suggests F3EAD is an ideal doctrine.	

CHAPTER 4—OPTIMIZING THE CANSOFCOM INTELLIGENCE FUNCTION

This chapter, which constitutes the main section of this paper, provides specific detail on how the CANSOFCOM intelligence function can be optimized to meet future challenges. It addresses the deductions made thus far, assessing how the Command's intelligence leadership can make the best use of resources so as to furnish the best possible intelligence support. To this end, this chapter examines specific potential solutions for meeting the challenges deduced at the end of chapter 3. It is broken down into three sections, or major domains, where investment and effort can best be applied: People, Structure and Process.

Optimizing CANSOFCOM Intelligence in the Domain of People

> *...you must get down to the fundamental problem that intelligence is people and personalities more than it is organization . . . in the end it has to be people, and you have to rely on people, whether they are in this box or that box, to produce what is ultimately needed in the future.*
>
> -Walter Pforzheimer, founding member of the CIA[69]

It is appropriate to begin this chapter by focusing on the central importance of people. Indeed, CANSOFCOM emphatically holds that its core strength is the quality of its personnel. At the same time, the Command considers intelligence critical to operational effectiveness.[70] Taken together, these two points emphasize that the Command's intelligence personnel must be high-performing individuals. As such, this section argues that CANSOFCOM intelligence needs to implement measures to ensure

[69] Quoted in Hammond, *Intelligence Organizations and the Organization of Intelligence*, 686.

[70] Department of National Defence, *Canadian Special Operations Forces Command: An Overview*, 7 and 15. See also Rouleau, *Special Operations Forces: Shaping the Area of Operations*, 89-90.

that its personnel are demonstrably capable of achieving the intelligence excellence the Command demands.

Unfortunately, at the moment an individual volunteers to serve with CANSOFCOM intelligence, he or she is unlikely to be capable of performing to the standard CANSOFCOM requires. This is because Intelligence Branch personnel do not undergo a selection process that ensures all Branch members are high performers. Furthermore, standard Intelligence Branch training does not prepare personnel to meet CANSOFCOM's unique and demanding intelligence requirements. Recommended measures for ensuring that the Command's intelligence personnel are discernibly high-performers include recruiting the right people, refining their skills through special training, and immersing them in a tailored intelligence organization culture.

To begin, CANSOFCOM intelligence should establish and/or refine procedures for screening and selecting those volunteering to serve in the Command's intelligence organization. In fact, there are very strong reasons for carefully screening applicants. For example, effective interpersonal skills are an absolute necessity, as strong and positive group dynamics are core to SOF's potency. However, because it is not possible to impose the interpersonal skills and positive group dynamics that make for high-performing teams, it is necessary to assess applicants for traits that contribute to team effectiveness.[71] Furthermore, Canadian experience shows that SOF intelligence personnel need to be adept at contributing to positive group dynamics during joint and coalition operations. They must be capable of cultivating effective interaction with foreign counterparts, overcoming the potential friction associated with sensitive

[71] Anna Simons, "The Evolution of the SOF Soldier: An Anthropological Perspective," in *Force of Choice: Perspectives on Special Operations*, ed. Bernd Horn, J. Paul de B. Taillon, and David Last, 80 (Montreal and Kingston: McGill-Queen's University Press, 2004).

intelligence operations, foreign agendas, and cultural differences.[72] Finally, screening is important because it is not clear that the typical CF Intelligence Branch member is suitable for employment with CANSOFCOM.

Some contend that the Intelligence Branch's own selection standards are too low. The Intelligence Branch fills its officer ranks in large part with personnel transferring in from other military occupations or the Reserve Force, and who are expected to meet only basic thresholds (that is, candidates must hold an undergraduate degree, exhibit at least average leadership abilities, and have three years of service including operational experience).[73] Such standards hardly identify those likely to thrive in intelligence work. Unfortunately, then, the Intelligence Branch does not screen applicants for the traits necessary to flourish in the intelligence domain. Consequently, should CANSOFCOM intelligence choose to screen applicants to identify those most likely to succeed in the demanding CANSOFCOM environment, it runs the risk of engendering the oft-leveled criticism that SOF skims the best talent.[74] So be it—because not screening personnel for either intelligence or SOF, experience shows, has highly undesirable consequences.

For example, experience in the U.S. Special Forces community suggests that lack of a selection process for support personnel has caused problems. American Special Forces have taken on support personnel who later proved unsuited to working with SOF due to inability to function effectively in fast-paced, small team environments, or sometimes due simply to low performance. When this occurs, units must expend time and effort attempting to raise such personnel to an acceptable standard or taking

---

[72] Taillon, *Canadian Special Operations Forces: Transforming Paradigms,* 72.

[73] Andrew J. Duncan, "From Ethos to Culture: Shaping the Future of Army Intelligence," *Canadian Army Journal* 9, no. 3 (2006): 45.

[74] This criticism is discussed in Bernd Horn, "Burn the Witch: A Case for Special Operations Forces," *The Army Doctrine and Training Bulletin* 2, no. 3 (1999): 28.

administrative action to remove them.[75] In contrast, other elements of the U.S. SOF community, such as the Ranger and the 160th Special Operations Aviation Regiments, now demand that support personnel meet certain high standards before they can be posted to an operational unit.[76]

Furthermore, for intelligence organizations in particular, failure to screen personnel can lead to intelligence failure, especially when low performing analysts are hired. In fact, this has contributed to a call for the implementation of a personnel screening program for the U.S. intelligence community.[77]

There is insufficient space here—and, indeed, it would be beyond the scope of this paper—to prescribe a detailed screening program. However, it is worth considering how to begin developing such a program, including several key aspects that would be fundamental to its design. First, certain factors should be considered central to the development of a CANSOFCOM intelligence personnel screening program. Fundamentally, SOF selection processes assess a candidate's future performance by measuring the individual's ability to accomplish certain tasks. Therefore, to develop any selection process, planners must first conduct a job analysis to identify exactly what an individual is expected to accomplish, with concrete examples of successful and

[75] Mathew N. Butler, "A Few Good Men: Support Soldier Selection and Training," *Special Warfare* 23, no. 6 (2010): 6-7.

[76] *Ibid*., 7-8. Butler proposes a 17-day Support Soldier Selection and Training model that screens candidates appropriately and gives them the basic physical, mental and emotional skills to succeed in working in the Special Forces environment.

[77] Adrian Wolfberg, "To Transform into a More Capable Intelligence Community: A Paradigm Shift in the Analyst Selection Strategy" (22nd Annual Chairman of the Joint Chiefs of Staff Strategy Essay Competition paper, U.S. National War College, 2003), page 3 and *passim*.

unsuccessful performance. The job analysis must also ascertain attributes that predict successful performance and establish ratings scales that measure ability.[78]

Furthermore, identifying traits that are particularly important to CANSOFCOM intelligence merits attention. CANSOFCOM fundamentally seeks individuals who are accepting of risk, creative, agile thinking, adaptive, self-reliant, eager for challenge, naturally oriented to the pursuit of excellence, and relentless in the pursuit of mission success.[79] This list provides a foundation of traits that are arguably very important, if not essential, for excellence in intelligence work, and therefore could serve as the foundation for an intelligence screening program. Additionally, the list could be supplemented with other traits known to be especially important for intelligence personnel. For example, the National Security Agency (NSA) has identified certain desirable traits for intelligence analysts, including curiosity, sharp observation skills, ingrained reading habits, self-motivation, ability to consider multiple perspectives, creativity, good reasoning skills and an ability to concentrate intensely and recognize patterns.[80] It may also be useful to assess for negative traits. American Special Forces selection does this, seeking to weed out those who will not fit into small teams and rejecting those who lack a natural tendency to get along with others.[81]

Furthermore, positive and cooperative personality dispositions are extremely important to intelligence organizations, while the opposite qualities—negativity and egocentrism—are essential to avoid. In her study of factors that cause interagency

---

[78] Tony Balasevicius, "Finding the Right Stuff: Special Operations Forces Selection," in *Casting Light on the Shadows: Canadian Perspectives on Special Operations Forces*, ed. Colonel Bernd Horn and Major Tony Balasevicius, 42 (Kingston, Ont: Canadian Defence Academy Press, 2007).

[79] Department of National Defence, *CANSOFCOM Capstone Concept for Special Operations*, 4-5.

[80] Wolfberg, *To Transform into a More Capable Intelligence Community*, 4-5. This document is recommended reading for consideration of how an intelligence screening program might be developed.

[81] Simons, *The Evolution of a SOF Soldier*, 84 and 89.

intelligence organizations to succeed or fail, Jeanne Hull found personality to be a potentially decisive factor. She shows that strong, positive, committed personalities have exceptionally favourable influences and can make otherwise dysfunctional intelligence organizations perform well. Conversely, negative or egocentric personalities within an intelligence organization can cause it to fail outright.[82] Surely this is an important recruiting consideration, and indeed a cultural phenomenon, the Command's intelligence professionals should respect in the design of a screening program.

Another particularly important trait for intelligence personnel is the capacity to accept the ambiguity of unclear situations one is responsible for assessing. Intelligence failures are known to result often from analysts' tendency to maintain preconceived notions in the face of new contradicting information.[83] This has significant but often unappreciated implications for intelligence recruiting programs. Intelligence organizations typically search for people who possess high intelligence, effective written and verbal communications competencies and strong managerial skills. While these are certainly important traits, equally so is the capacity to live with ambiguity and be open to new information. But some people naturally tend to make quick judgements in order to have cognitive closure, rather than engage in the slower and cautious deliberation needed to arrive at informed conclusions. Consequently, intelligence agencies should place particular emphasis on recruiting personnel who possess the mental propensity to process new information appropriately, regardless of whether or not it supports extant beliefs.

[82] Jeanne Hull, "We're All Smarter than Any One of Us," *Journal of Public and International Affairs* 19, no. 1 (2008): 44-45.

[83] Bar-Joseph and McDermott, *Change the Analyst and Not the System*, 172.

Fortunately, it is possible to screen for the undesirable trait of "belief perseverance" using psychologically validated testing models.[84]

This brief section on desirable personnel attributes is intended to provide a starting point for considering how the Command's intelligence function should screen applicants. The Command's intelligence leadership would undoubtedly identify other important characteristics, perhaps including such traits as natural curiosity, assertiveness, and effectiveness under pressure to name but a few. Further research is therefore required to develop a comprehensive set of characteristics a screening program would measure and to investigate how such a screening program should be designed and scientifically validated. The major point to emphasize is the fundamental importance of recruiting people with the right attributes to succeed in CANSOFCOM intelligence. Success or failure to screen applicants accordingly has potential to be the difference between intelligence success or failure.

Personnel who pass a CANSOFCOM intelligence screening process and are accepted for service require orientation training to ensure their effectiveness at delivering intelligence excellence tailored to CANSOFCOM's requirements. Empirical evidence shows that endowment with a sharp mind is not enough to succeed in intelligence work. This is because even the smartest people are surprisingly prone to making grave analytical errors, a fact that Richards Heuer (a forty-five year veteran of the CIA and renowned authority on analytical reasoning) argues should be taken very seriously by the intelligence community. Indeed, the history of intelligence failures relating to poor

[84] *Ibid*., 128, 136 and 139.

analytical work strongly suggests that intelligence agencies should train personnel to avoid disastrous analytical traps.[85]

In fact, analytical reasoning—the core service CANSOFCOM intelligence provides—is inherently predisposed to a host of faulty tendencies. To emphasize the point, a few key ones are listed here. For example, this chapter has already mentioned "belief perseverance" (the difficulty of integrating new refuting information). Also reprehensible is "intelligence to please" or tailoring intelligence to a user's agenda. So too is "groupthink" which occurs when members of a group support a collective position out of a desire to be appreciated or to avoid being rejected by the majority.[86] "Layering" occurs when an analyst bases his/her judgement on older analysis, but discards the old assessment's caveats of uncertainty—a fault that undermined America's 2002 National Intelligence Estimate that confidently predicted Iraq's possession of WMD.[87] "Mirror imaging," or casting one's sense of logic onto an adversary, can lead to overestimating an adversary's aversion to risk, with dire consequences.[88] Similarly, undue attribution of Western-style rationality to an adversary, which also occurs too often, can be equally disastrous. The U.S. Office of National Estimates assessment in September 1962 that the Soviet Union was unlikely to place nuclear weapons in Cuba—less than a month before analysts found evidence that Khrushchev had done exactly that—is a dramatic example

[85] Colin A. Wastell, "Cognitive Predispositions and Intelligence Analyst Reasoning," *International Journal of Intelligence and Counterintelligence* 23, no. 3 (2010): 449-453 and 458. Uri Bar-Joseph argues that intelligence failures to forecast threats is usually not a matter of insufficient collection, but a matter of faulty analysis of the information collected, in *The Professional Ethics of Intelligence Analysis*, 24.

[86] Bar-Joseph, *The Professional Ethics of Intelligence Analysis*, 27-29.

[87] Mahnken, *Spies and Bureaucrats: Getting Intel Right*, 39.

[88] Bar-Joseph and McDermott, *Change the Analyst and Not the System*, 129. The authors cite an arm's length list of examples since the German invasion of the Soviet Union where overestimating an adversary's risk aversion led to grave intelligence failure.

of underestimating an actor's risk aversion by otherwise exceptionally capable and experienced intelligence personnel.[89]

Of particular relevance to CANSOFCOM intelligence is the folly of "single-outcome forecasting," or the adherence to, and inappropriate reinforcement of, the prevailing perception of a situation. A CIA investigative panel discovered this phenomenon in 1983, when the team reviewed intelligence assessments that preceded serious intelligence failures over a twenty-year period. The panel concluded that intelligence managers and analysts must recognize the importance of dealing logically and realistically with uncertainty and assessing possible outcomes. Interestingly, the panel advised that intelligence estimates should not be restricted to providing limited views on potential outcomes, even when there is general consensus amongst analysts, but rather should provide brief assessments on "alternative outcomes" in addition to high-confidence assessments.[90] CANSOFCOM's intelligence leadership should consider this idea for its merit, given the doctrinal and process-driven tendencies for military intelligence staffs to provide limited assessments of future adversarial action (usually "most likely" and "most dangerous" scenarios). This is not to suggest that intelligence staffs should hedge their analysis by providing a wide range of remotely plausible outcomes, but rather that they should provide commanders and planners with the most thorough and balanced assessments possible to inform decision-making.

Aside from the requirement to avoid these well-documented analytical traps, there are other strong reasons for investing in a training regime for new CANSOFCOM intelligence personnel. Counter-terrorism operations are a high-stakes business for which

[89] Hedley, *Learning from Intelligence Failures*, 439.
[90] *Ibid*., 444.

a breakdown of intelligence can be disastrous, resulting in mission failure and friendly force fatalities.[91] Furthermore, training and developing intelligence personnel for counter-terrorism requires a concerted effort.[92] The Americans learned this painful lesson in the aftermath of 9/11, when the intelligence community realized it was deficient in analytical capabilities (amongst other things).[93] U.S. intelligence leadership recognized that to provide high-fidelity predictive assessments, analytical capabilities needed to be improved, in part by taking a more scientific approach to analysis.[94] The same argument could be applied to Canadian military intelligence today.

The point to emphasize is that CANSOFCOM intelligence should enhance individual analytical performance with a training regime for new personnel that emphasizes effective analytical practices while deterring the bad. While further research is required to develop a comprehensive training regime, it is worthwhile to consider here factors that would be particularly important for such a program. For example, CANSOFCOM's intelligence leadership should consider the argument that more science needs to be integrated into intelligence analytical processes. Intelligence agencies have not traditionally emphasized scientifically-based analytical practices, instead preferring art over science. This is a fault that is particularly serious for organizations responsible for delivering predicative analysis, the most difficult type of analysis to produce.[95]

---

[91] Mark V. Kauppi, "Counterterrorism Analysis 101," *Defense Intelligence Journal* 11, no. 1 (2002): 45.

[92] Sir Richard Dearlove and Tom Quiggin, "Contemporary Terrorism and Intelligence," *Institute of Defence and Strategic Studies Commentaries* 78 (2006): 3. According to Dearlove (former head of the UK's Secret Intelligence Service), it can take in excess of five years to make intelligence personnel truly effective at counter-terrorism.

[93] Hubbard, *Another Response to Terrorism: Reconstituting Intelligence Analysis for 21st Century Requirements*, 71.

[94] *Ibid.*, 78-79.

[95] Michael W. Collier, "A Pragmatic Approach to Developing Intelligence Analysts," *Defense Intelligence Journal* 14, no. 2 (2005): 17-35.

While there are several scientifically-based analytical techniques analysts can use, one stands out as particularly useful for CANSOFCOM's needs: Richards Heuer's Analysis of Competing Hypotheses. Heuer's seminal work on Analysis of Competing Hypotheses is a widely-cited method for improving intelligence analysis by minimizing the cognitive biases that inherently afflict human reasoning. Given the value Heuer's methodology would likely add to a CANSOFCOM intelligence training regime, a brief summation of the method is merited.

Heuer cites research showing that most analysts assess future outcomes by drafting a hypothesis then searching for information that supports it. If evidence appears to support the hypothesis, the idea accepted. If not, the process begins again with the drafting of a new hypothesis. This method is fundamentally flawed because analysts are easily seduced into perceiving information as reinforcing a hypothesis when the information actually supports numerous potential outcomes.[96]

The Analysis of Competing Hypotheses process begins by selecting numerous hypothetical outcomes. A matrix is then developed, allowing analysts to apply the available evidence and assumptions to each of the hypotheses, recording them on the matrix as supporting or refuting. The aim, it must be emphasized, is to refute hypotheses with evidence confirming them as wrong. Generally speaking, the more uncertain a situation is, or the greater the impact on policy the final assessment will have, the more hypotheses should be developed. More than seven, however, may prove unmanageable.[97]

Analysts must also consider the significance of an absence of evidence for a given hypothesis, as it takes considerable mental effort to appreciate what indications are

[96] Richards J. Heuer, *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence—Central Intelligence Agency, 1999), 95-96.
[97] *Ibid*, 98.

missing when they should not be (i.e. certain adversary courses of action should be preceded by tell-tale indicators). Furthermore, analysts must consider the *diagnosticity* of each element of information. That is, information that supports all hypotheses has no diagnostic value. Conversely, information that strongly refutes certain hypotheses is highly diagnostic and should drive judgment. And such information should therefore be re-checked for credibility. Refuting information is far more significant than confirming information. As such, the hypothesis with the most refuting indicators is probably the least likely. Conversely, however, the one with the most reinforcing indicators is not necessarily the most likely, as it is surprisingly easy to create long lists of supporting information.[98]

Human judgment makes the final call as to what hypotheses likely represent future outcomes. As such, the Analysis of Competing Hypotheses matrix is not guaranteed to generate a correct answer, as human judgment is always fallible. It does, however, ensure that the analytical process is sound and that biased thinking is minimized. Furthermore, it may produce multiple potential outcomes, in turn presenting an uncertain picture. But—and this is key—this may accurately reflect the best possible analysis, as opposed to the greater but artificial certainty that comes with presenting a single outcome the analyst prefers as "most likely." Also, the analyst can apply relative likelihoods to the remaining feasible hypotheses, which may be useful for decision makers who then judge that certain contingency measures are necessary.[99]

Another particularly important consideration for a CANSOFCOM intelligence training program is the desirability of teaching analysts to develop empathy for the

[98] *Ibid.*, 99-104.
[99] *Ibid*, 106-109.

adversary. Empathy refers to "understanding the thoughts and feelings of others."[100] It involves appreciating others' viewpoints, or getting inside their skin, to appreciate "what the world would look like through their eyes."[101] Empathy is not, it must be stressed, synonymous with sympathy. Experience shows that lack of empathy has serious negative repercussions for intelligence assessments, causing analysts to underestimate the potential or actual resolve or even anger an adversary may harbour.[102] It leads to a misunderstanding of adversaries that results in surprise at their actions. In fact, lack of empathy is arguably one of the most serious types of intelligence faults because it causes analysts to underappreciate the adversary's perceptions that drive his behaviors. Conversely, however, developing empathy can serve as an antidote to "mirror imaging" and inappropriate assumptions of an adversary's rationality.[103] Empathy also helps analysts break down the stereotypes that undermine analysis by allowing analysts to disregard complexity and simplify judgments.[104]

Teaching analysts to cultivate empathy for the adversary is much more a matter of art than science. But it needs to be cultivated at all levels of an intelligence organization. Intelligence leaders can foster empathy development by teaching analysts to assess an adversary's actions vice his words (as words are normally aimed at domestic audiences

---

[100] Ralph K. White, "Empathy as an Intelligence Tool," *International Journal of Intelligence and Counterintelligence* 1, no. 2 (1986): 57.

[101] *Ibid*., 58.

[102] White, *Empathy as an Intelligence Tool*, 64.

[103] Stephen Marrin, "Adding Value to the Intelligence Product," in *Handbook of Intelligence Studies*, ed. Lock K. Johnson, 207-208 (New York: Routledge, 2007).

[104] Unfortunately, stereotyping is seductive to analysts because it allows them to ignore the requirement for meticulous analytical effort. White, *Empathy as an Intelligence Tool*, 64.

and are therefore of little value to analysts).[105] Another way is to encourage analysts to ask frequently "How would I feel if I were facing the situation they are facing now?"[106]

Science also confirms that analysts can markedly improve performance by adjusting how they think. Research shows that people who are particularly confident in their predictive analysis, including experts in any given domain, are no better at predicting the future than random guesses. However, people do better at prediction when they are comfortable accepting that the world is inherently complex and uncertain. Such people tend to build analysis by seeking information from as many sources as possible. They tend to be skeptical and constructively self-critical. And when proven wrong, they simply accept it without excuse and adjust their thinking appropriately.[107] Understanding these notions has proven to make for an effective intelligence organization—a notion that CANSOFCOM's intelligence leadership should consider in the development of a training program.[108]

Group (collective) training should also be considered for inclusion in a CANSOFCOM intelligence training program. Of interest to CANSOFCOM intelligence, the United States Air Force (USAF) has looked closely at how to overcome certain intelligence challenges that are remarkably similar to CANSOFCOM's, such as tracking time sensitive targets in complex environments, using ISR to locate insurgent nodes, and generating high fidelity intelligence to cue operations, all of which demand high

[105] *Ibid*., 70.
[106] *Ibid*., 73.
[107] Gardner, *Future Babble: Why Expert Predictions Fail*, 26-27.
[108] Gardner explains that intelligence staff at Canada's Privy Council Office have been shown through empirical research to be effective at predictive analysis because the organization subscribes to these principles. *Ibid*, 251-255.

standards of analysis.[109] To this end, the USAF has developed collective training methods that might be useful for informing the design of a CANSOFCOM intelligence collective training regime.

For example, the USAF intelligence "schoolhouse" at Goodfellow Air Force Base (17th Training Group) conducts SIGINT exercises that integrate the latest technologies and allow students to employ a wide range of SIGINT capabilities. This training teaches participants to exploit SIGINT to its fullest capacity.[110] Other exercises bring together all intelligence disciplines to train in highly realistic scenarios, permitting various specialists, such as SIGINT and intelligence analysis personnel, to work together and see how each brings expertise and specialized insight to a problem. Students prosecute high-value, time-sensitive targets using near real-time intelligence feeds. The training is intensive and cultivates the substantive collaboration that must occur in any all-source intelligence organization that conducts targeting.[111] USAF intelligence students also take part in exercises during which participants analyze real-world scenarios from previous operations in Iraq and Afghanistan. Participants must develop and brief ISR plans that make the best use of scarce ISR resources, while instructors with operational experience provide feedback on what the students do right and wrong. The use of instructors with such operational expertise is considered essential to training. Finally, the USAF recognizes that intelligence interaction with other national agencies is essential. Therefore, the Intelligence School brings together intelligence personnel from the military and other national agencies, particularly the National Security Agency (NSA), to

[109] Scott George and Robert Ehlers, "Air-Intelligence Operations and Training: the Decisive Edge for Effective Airpower Employment," *Air and Space Power Journal* 22, no. 2 (2008): 62-63.
[110] *Ibid*., 64.
[111] *Ibid.,* 64.

conduct leading-edge training.[112] Such collective training initiatives could provide inspiration for a CANSOFCOM intelligence training plan.

In addition to an entry training program for new personnel that would provide familiarization with CANSOFCOM intelligence capabilities and operating procedures, periodic exercises or seminars for all intelligence personnel would also be useful for maintaining collective skills sets and distributing operational experience. Such events could focus on sharing best-practices developed on operations, examine previous operations to share what went well and what did not, and discuss emerging technologies and how to apply them. This type of continuation training could be particularly valuable by involving other national agencies and allied counterparts.

Once CANSOFCOM intelligence trains new personnel to ensure their effectiveness in the CANSOFCOM intelligence environment, it would be useful to cultivate their abilities over the long term by encouraging performance that capitalizes on their talent. At the same time, it is important to prevent negative cultural aspects, such as elitism or insularity, from growing within the team. An effective way to accomplish these goals would be to inculcate intelligence staffs with an appropriate CANSOFCOM intelligence culture. Because leadership clearly drives culture,[113] CANSOFCOM's intelligence leaders should consider deliberately modelling and fostering a carefully developed intelligence culture. Such a culture should, first and foremost, fully encompass the Command's clearly-articulated ethos (figure 4.1).

[112] *Ibid*, 64-65.
[113] Schein, *Organizational Cultures and Leadership,* 19, 23, and 270.

CANSOFCOM Ethos

1. Internalization of the CF Core Values of *Duty*, *Loyalty*, *Integrity*, and *Courage*
2. Relentless Pursuit of Excellence
3. Indomitable Spirit
4. Shared Responsibility
5. Creativity
6. Humility

Figure 4.1
Source: *CANSOFCOM Capstone Concept for Special Operations*, 8-9.

Other values known to be especially important for effective intelligence work could be added to those listed above to form a tailored CANSOFCOM intelligence culture. For example,

Intelligence personnel should appreciate the importance of moral courage to their effectiveness. Experience shows that intelligence personnel will occasionally feel pressured to bend their assessments to meet a superior's agenda. This is known as "politicization." Unfortunately, the politicization of intelligence is a very real phenomenon that has manifest even at the highest levels. Famous examples include Director of Central Intelligence George Tenet's advice that evidence of Iraqi weapons of mass destruction was a "slam dunk" and Britain's prestigious Joint Intelligence Committee having oversold Iraqi WMD to the public.[114] Because of the influence intelligence has on critical decision-making, the politicization of intelligence should be regarded a "cardinal sin" of intelligence work.[115] CANSOFCOM would do well to recognize the regrettable potential for this phenomenon and demand that its intelligence

[114] Scott and Hughes, *Intelligence in the Twenty-First Century*, 13.
[115] Nolte, *Ethics and Intelligence*, 25.

personnel place a premium on the morale courage required to keep intelligence analysis pure.

CANSOFCOM's intelligence culture should also emphasize strong intelligence ethics. Certain intelligence activities, particularly involving the collection of information, can be ethically tricky. Therefore, there is—as Professor William M. Nolte (University of Maryland and former executive in the National Security Agency) argues—a strong requirement for intelligence work to include particularly high ethical standards. Agent handlers, for example, may engage in ethically precarious activity by recruiting individuals willing to commit serious acts of betrayal, including treason. Interrogation has similar potential to include practices that could, if not controlled carefully, be considered unethical. What is more, such intelligence activities constitute part of the state's coercive power, and therefore intelligence agencies need to be able to reassure the political establishment that they act for the public good and unquestionably respect society's values.[116] For CANSOFCOM, given the critical importance identified in chapter 3 for the Command's intelligence function to maintain a high degree of trust and credibility, it cannot risk even the slightest perception of ethically-questionable conduct. Emphasizing high ethical standards in the conduct of intelligence activities is essential to sustaining high credibility.

A CANSOFCOM intelligence culture need not necessarily be formal. It can be informal, though deliberately propagated through leadership-by-example. Figure 4.2 depicts a potential start point for consideration of how a CANSOFCOM intelligence culture might look.

[116] *Ibid*., 23-24 and 29.

Potential Elements of a CANSOFCOM Intelligence Culture

1.	Internalization of the CF Core Values of *Duty*, *Loyalty*, *Integrity*, and *Courage*	Essential CANSOFCOM Ethical Values
2.	Relentless Pursuit of Excellence	
3.	Indomitable Spirit	
4.	Shared Responsibility	
5.	Creativity	
6.	Humility	
7.	Analytical excellence (including systemic avoidance of analytical faults)	Potential Intelligence-specific values
8.	Moral courage—keeping intelligence analysis pure and free from interference	
9.	Intelligence ethics that unquestionably respect Canadian laws and social values	

Figure 4.2

This section argues that CANSOFCOM intelligence should implement measures to ensure that its personnel are demonstrably capable of achieving the intelligence excellence the Command demands. To this end, it is necessary to recruit the right people, which requires a well-planned screening process designed to assess the degree to which a candidate possesses requisite (and perhaps intolerable) traits. Applicants accepted for service should receive training to give them the skills required for the demanding CANSOFCOM intelligence environment. Inculcating intelligence personnel with an organizational culture firmly anchored to the Command's ethos and further tailored to the intelligence function would foster desirable attitudes and behaviour while suppressing those known to undermine effective intelligence work. Strong leadership—which this paper assumes is a given requirement for CANSOFCOM's intelligence leaders—plays the central role in modeling and fostering the desired culture.[117] Acknowledgement that even the brightest individuals are prone to making grave analytical errors is a serious potential problem—particularly given the intelligence function's core task of rendering

[117] Schein, *Organizational Culture and Leadership*, 270.

analytical services—and taking measures to avoid such errors through training and establishing cultural norms would contribute significantly to optimizing the intelligence function's critical human resources.

Optimizing CANSOFCOM Intelligence in the Domain of Structure

This section argues that the structure of CANSOFCOM's intelligence function must be designed in a way that guarantees a capability to deliver on-demand, multi-source intelligence support to tactical operations. Indeed, the time to consider how the Command's intelligence structure should evolve is now, before a crisis occurs. Fortunately, the previous discussion on the future security environment provides valuable insight into where CANSOFCOM intelligence should invest effort in refining its structure. To this end, the section begins with a discussion of appropriate roles between the headquarters and unit intelligence staffs. Also, the summarized deductions and anticipated intelligence tasks listed at the end of chapter 3 are used to inform analysis of capabilities likely to be required for supporting operations in the future security environment, specifically in the domains of ISR, HUMINT, and exploitation. Indeed, access to these capabilities should constitute part of the organization's structure.[118]

[118] While the general structure of the CANSOFCOM intelligence function merits consideration as a major component of this paper's analysis, it is not necessary or even desirable to examine how the Command's intelligence would best be organized, working towards a line diagram depicting a theoretically optimized organization. In fact, this paper resists the temptation to seek detailed organizational solutions for optimizing intelligence efficiency, acknowledging instead the scholarly evidence showing that there is no proven best way for organizing an intelligence agency. For example, Hammond explains that despite frequent efforts to improve intelligence agencies by altering organizational structures (especially in the U.S. where structures have often received considerable scrutiny and adjustment in response to intelligence failures), research shows that there is no best model for organizing an agency. Hammond, *Intelligence Organizations and the Organization of Intelligence*, 683-686 and 703.

An important caveat is required here: while some of the following discussion focuses on collection capabilities, it does not suggest where they should reside. In fact, this paper does not advocate that any such capabilities necessarily be integral to CANSOFCOM's intelligence organization. The emphasis is on collection capabilities the intelligence function will require access to. Exactly where these capabilities should reside is a topic that requires a degree of consideration that would overly broaden this paper's scope, and is best left to further research. The following discussion on capabilities is therefore limited to analysis of information-gathering effects the Command will likely require, leaving to future consideration whether such capabilities should be organic to the intelligence function or another group within the Command, or perhaps accessed from external agencies.

First, the roles between the headquarters and unit intelligence staffs deserve consideration. The following analysis regarding roles takes a theoretical perspective that considers fundamental factors, though without regard for how the current J2 and S2 organizations currently operate. As such, this section is not a critique of the status quo.

The Command's units arguably require sizeable, standing intelligence staffs with access to a wide range of collection capabilities to support tactical operations. This is because the Command, through its units, provides the Government of Canada with unique military capabilities kept at high-readiness.[119] In fact, all CANSOFCOM units contribute to the force generation and force employment of Special Operations Task Forces (SOTF).[120] JTF 2, for example, maintains "extremely short notice" readiness to form and deploy the Immediate Response Task Force (IRTF) to conduct counter-

[119] Department of National Defence, *Canadian Special Operations Forces Command: An Overview*, 12.
[120] Department of National Defence, *CANSOFCOM Capstone Concept for Special Operations*, 11.

terrorism operations anywhere in the world or for other operations deemed to be in the national interest.[121] The Canadian Joint Incident Response Unit (CJIRU) maintains a Chemical, Biological, Radiological and Nuclear (CBRN) Task Force ready to respond at short notice to support the RCMP-led national CBRN Response Team. And the Canadian Special Operations Regiment (CSOR) maintains Task Force Arrowhead, a high-readiness SOTF prepared to deploy globally on short notice.[122] Each of these SOTFs is supported by a Special Operations Intelligence Centre (SOIC) that conducts all-source fusion and analysis for both domestic and expeditionary operations.[123] Given the permanent high-readiness to deploy these SOTFs, the SOICs need to be enabled in two areas. First, they require standing on-demand access to robust, leading-edge collection capabilities. Second, they require enough personnel who are intimately familiar with their units' unique intelligence requirements and operating procedures (SOPs, battle rhythm, etc) to provide sustained tactical intelligence support. Arranging for external provision or augmentation of collection and analytical services after a no-notice deployment occurs would be difficult, untimely, and detrimental to the mission.

There is a counter argument to the notion that it is ideal in principal to maintain robust standing unit intelligence staffs. Kostas Rimsa (former Canadian military intelligence officer) argues that a centralized CF military intelligence and collection support unit should be formed to serve units such as JTF 2 when they deploy for operations. He argues that such a unit would guarantee Canadian support to Canadian

[121] Department of National Defence, "CANSOFCOM Integrated Operating Concept," last accessed 15 January 2013, http://www.cansofcom.forces.gc.ca/gi-ig/ioc-coi-eng.asp.
[122] *Ibid*.
[123] Department of National Defence, *CANSOFCOM Capstone Concept for Special Operations*, 18-19.

units.[124] Despite Kostas's recommendation, however, brigading personnel at a central location from where they can be force generated is not an ideal option, for CANSOFCOM or any other military organization. Both the Canadian and American armies have recently identified requirements to maintain sizeable, standing intelligence staffs with tactical units, and have therefore planned to triple and double their tactical intelligence staffs respectively.[125] Similarly, CANSOFCOM units would best be served by standing tactical-level intelligence staffs, with personnel familiar to and trusted by the commanders and operators they support, and with enough staff to sustain close intelligence support services. Brigading intelligence personnel as Rimsa advises would not achieve the tight integration, intimate familiarity with intelligence requirements, sense of unit pride, and tactical ownership of the intelligence function that is best achieved by posting personnel to units.

The two tactical-level requirements identified above—access to robust collection capabilities and sizeable standing tactical intelligence staffs—have important implications for the Command's J2 staff and informs the following discussion on J2 roles. The J2 is, of course, the Commander's threat advisor. This fact alone emphasizes that the J2 requires an analytical capability in his staff for generating the Situational Awareness (SA) and Indications and Warnings (I&W) intelligence the Commander always requires. This is not to say, however, that the J2 staff needs to produce such intelligence from scratch, which would require significant effort by numerous personnel and could result in duplication of effort conducted by other agencies. Rather, a relatively

[124] Kostas Rimsa, "Very Special Forces," in *Inside Canadian Intelligence: Exposing the New Realities of Espionage and International Terrorism*, edited by Dwight Hamilton, 169 (Toronto: Dundurn, 2011).

[125] Lieutenant Colonel J.A.E.K. Dowell, *Intelligence for the Canadian Army in the 21st Century*, Jadex Papers 5 (Kingston, Ontario: Department of National Defence, Directorate of Land Concepts and Designs, 2011), 36.

small number of personnel could meet the Commander's intelligence requirements largely by accessing I&W and analytical products generated by other agencies such as Chief of Defence Intelligence (CDI), the Privy Council Office (PCO), CSIS and allies. The J2 also requires staff capacity to support the headquarters' J3 Operations and J5 Plans branches.[126] Furthermore, the J2 is responsive to the CDI, who as the military's Functional Authority for intelligence holds responsibility for intelligence policy, doctrine, and oversight within the Department of National Defence.[127] The J2 therefore exercises governance and oversight of the Command's intelligence function, ensuring that CDI functional direction is met.

The Command J2 is also responsible to the Commander for the intelligence function. To this end, in the future security environment the J2 will play an important role in enabling the SOTF SOICs, whose requirements for collection capabilities are likely to be high. As deduced in chapter 3, CANSOFCOM units will require robust collection capabilities in order to identify, locate and track highly evasive targets. However, it is safely assumed here that CANSOFCOM will not possess all the requisite collection capabilities within its organization based on, as a minimum, the probable requirement to access strategic collection systems. In fact, consistent with the government's expectations that agencies work together, it is all but certain that CANSOFCOM will require the support of other agencies to enable the SOTF SOICs. Reaching outside the Command to arrange for such support is clearly a role for the J2 staff.

[126] Lieutenant Colonel Cody Sherman, J2 CANSOFCOM, conversation with author, 12 February 2013.

[127] Department of National Defence, *Canadian Forces Joint Publication 01—Canadian Military Doctrine* (Ottawa: Joint Doctrine Branch, 2011), page 5-9, and Lefebvre, *Canada's Legal Framework for Intelligence*, 263.

Furthermore, as deduced at the end of chapter 3, CANSOFCOM will require standing and active liaison with the numerous domestic and foreign intelligence agencies the Command may work with or require support from. If detailed familiarity with important domestic partner agencies is to be maintained—including understanding of key personnel, strengths and weaknesses, and potential friction points—and if the Command is to maintain trust and credibility, sustained investment in domestic liaison will be necessary. Similarly active and ongoing liaison will be required with close allies, particularly the J2's counterpart organizations. This will be necessary not only for maintaining an active network of connections with potential operational partners, but also for staying abreast of our close allies' world views and of evolving SOF intelligence methodologies for supporting increasingly complex tactical operations. In addition, allies can provide essential information and ground truth for global regions and potential hot spots where Canada has little or no national footprint or local expertise.[128] In short, sustained intelligence liaison with other government agencies and important allies is an especially important J2 task that requires a considerable investment in effort.

J2 staff also play a role in enabling the SOTF SOICs with access to leading edge collection capabilities. Such capabilities are often developed or governed by external agencies, to which the J2 staff are generally responsible for dealing with. To this end, the J2 requires staff capacity to conduct Force Development activities.[129]

Aside from the J2 and S2 roles, it is necessary to consider what collection capabilities will be required to support operations in the future security environment. For example, CANSOFCOM intelligence will undoubtedly require access to Intelligence,

[128] Lieutenant Colonel Cody Sherman, J2 CANSOFCOM, conversation with author, 13 February 2013.
[129] *Ibid*.

Surveillance and Reconnaissance (ISR) capabilities. ISR, which is usually associated with aerial platforms such as unmanned aerial vehicles (UAVs) and reconnaissance aircraft, provides highly valuable information—as made abundantly clear during the wars in Afghanistan and Iraq—especially from full-motion video (FMV) and SIGINT sensors.[130] Despite the secrecy that generally cloaks SOF tactics, techniques and procedures, open professional military literature shows just how important ISR is to SOF intelligence. For example, U.S. Special Forces have used such sensors to great effect in recent counter-insurgency campaigns, intercepting enemy communications to reveal strengths, intentions and morale, and tracking enemy movements, in turn enabling meaningful predictive analysis of future enemy actions.[131] Furthermore, the SIGINT and imagery collected by aerial ISR provides valuable multi-source information to complement HUMINT, rendering a holistic understanding of an enemy or objective area.[132]

In fact, ISR has proven exceptionally valuable in recent campaigns against the types of decentralized non-state adversaries CANSOFCOM is likely to encounter in the future. In Iraq, U.S. forces found that air-breathing ISR not only provided a significant proportion of their actionable intelligence, but also outperformed space-based SIGINT and imagery platforms that experienced limitations when the enemy acquired emerging technologies that degraded the orbital collectors' capabilities.[133] ISR was key to SOF's successful targeting of Abu Musab al-Zarqawi, Al Qaida in Iraq's extreme and

[130] Michael T. Flynn, Rich Juergens and Thomas L. Cantrell, "Employing ISR: SOF Best Practices," *Joint Force Quarterly* 50, no. 3 (2008): 57.

[131] Michael Erwin, "Integrating Intelligence with Operations," *Special Warfare* 21, no. 1 (2008): 11.

[132] Michael L. Downs, "Rethinking the Combined Force Air Component Commander's Intelligence, Surveillance, and Reconnaissance Approach to Counterinsurgency," *Air & Space Power Journal* 22, no. 3 (2008): 68.

[133] William B. Danskine, "Aggressive ISR in the war on Terrorism: Breaking the Cold War Paradigm," *Air and Space Power Journal* 19, no. 2 (2005): 76.

gruesomely violent leader, in 2006.[134] JSOC units in Iraq found that aerial ISR was an exceptionally effective enabler because of the volume of actionable intelligence it provided. JSOC went from conducting a monthly rate of 18 raids in August 2004 to a fantastic 300 raids in August 2006, all with a higher success rate, thanks to increasing use of ISR (especially FMV) to develop targeting opportunities by following people and vehicles and developing patterns of life.[135]

In the future security environment, aerial ISR is likely to continue increasing in importance. The analysis in chapter 3 highlighted the need for an ability to collect against clever, discrete enemies in urban and littoral areas, including tracking sea-borne targets for maritime counter-terrorism operations. Aerial ISR can be of enormous value in such circumstances. ISR has tremendous potential, for example, to enable intelligence staff to learn a great deal about adversary networks by following individuals and tracking vehicles, allowing for an appreciation to develop of a network's nodes, patterns of life at important locations, and a target's personal indicators—such as gait and dress—that become high-confidence targeting cues.[136] In fact, an emerging school of thought in the U.S. calls for significant investments in additional ISR capabilities, arguing that they are invaluable but chronically "low density/high demand" assets for which demand will only increase.[137] Indeed, the significant importance of FMV and SIGINT ISR, as realized during counter-insurgency operations in Afghanistan and Iraq, is leading to calls in the

---

[134] Flynn, Juergens and Cantrell, *Employing ISR: SOF Best Practices*, 56.

[135] Brookings Institution, *The Evolution of Joint Special Operations Command and the Pursuit of Al Qaeda in Iraq: A Conversation with General Stanley A. McChrystal* (Washington: the Brookings Institution, 2013), 19.

[136] *Ibid*, 58-59. Insight into the U.S. Army and Air Force's investments in sophisticated ISR platforms that combine SIGINT and surveillance cameras to detect and follow adversaries is found in Amy Butler, "Intel Posturing," *Aviation Week & Space Technology* 172, no. 46 (2010): 28.

[137] Glenn W. Goodman, "ISR Now Synonymous with Operations," *Journal of Electronic Defence* 30, no. 7 (2007): 20. Also, Lieutentent Colonel William B. Danskine argues that "Increased reliance on air-breathing and surface collectors seems inevitable" in *Aggressive ISR in the war on Terrorism*, 76.

U.S. for a substantial growth of ISR fleets.[138] In other words, Canada's most important ally sees a very strong requirement to prepare for the future security environment by investing heavily in an already well-endowed ISR capability. There is a significant implication here for CANSOFCOM intelligence: if it is to fulfill its role in cueing operations against future threats, it too will require access to leading-edge ISR capabilities. Conversely, insufficient access to ISR in CANSOFCOM could leave the Command's intelligence capability lagging far behind its close allied counterparts, possibly undermining the Command's credibility as a world-class partner that wields the capabilities needed to fight tomorrow's enemies.

HUMINT is another capability the Command's intelligence will likely require. This is because technical collection means, while undeniably important, have limitations. Recent transnational threats have shown that technical collection has limited effectiveness in penetrating extremist organizations, an area where HUMINT can be more effective.[139] A 2004 U.S. government investigation into intelligence practices found that SIGINT and imagery intelligence each have limitations for locating small, dispersed insurgent cells that hide amongst the population.[140] Some potential adversaries understand the nature of overhead capabilities and have developed methods for evading them. Also, satellites have limited, non-persistent coverage simply because they are orbiting the globe. And adversaries can now encrypt their communications with widely

[138] Flynn, Juergens and Cantrell, *Employing ISR*, 61.
[139] William J. Lahneman, "Is A Revolution in Intelligence Affairs Occurring?" *International Journal of Intelligence and Counterintelligence* 20, no. 1 (2007): 7-8.
[140] Department of Defense, *Final Report of the Independent Panel to Review DoD Detention Operations*, 31.

available software.[141] HUMINT offers a means of filling the gap left by technical platforms.

HUMINT is therefore vitally important to intelligence collection against extremist groups. In fact, U.S. experience in fighting global terrorism has shown that HUMINT can be the greatest source of the actionable intelligence needed to cue operations.[142] It has proven particularly useful, if not sometimes crucial, for enabling the capture of individuals.[143] Consequently, HUMINT is now widely considered essential for dismantling terrorist groups by penetrating their organizations, identifying members and learning of their plans.

Of course, HUMINT will continue to be an important intelligence collection discipline in the future security environment. Although the future is likely to see incredible technological advances affecting collection, the need for human sources to penetrate adversaries' organizations and learn about their intentions will remain strong.[144] Professor Oleg Kalugin (Centre for Counterintelligence and Security Studies and former Major General in the Soviet KGB) argues that even America's colossal technological collection capability cannot substitute for the capability a human agent provides to penetrate an adversary's organization. Kalugin argues that intelligence efforts to penetrate extremist organizations must place a heavy priority on recruiting agents within, or infiltrating agents into, such groups.[145]

---

[141] Mahnken, *Spies and Bureaucrats*, 35.

[142] Luca Follis, "Laboratory of War: Abu Ghraib, the Human Intelligence Network and the Global War on Terror," *Constellations* 14, no. 4 (2007): 641.

[143] Frankel, *The ABCs of Targeting: Key Lessons from High Value Targeting Campaigns*, 25. Lawrence E. Cline argues "that human intelligence (HUMINT) is the most critical intelligence discipline in counterterrorism has become an axiom." *Special Operations and the Intelligence System*, 579.

[144] Jack Devine, "Tomorrow's Spygames," *World Policy Institute* 25, no. 3 (2008): 141.

[145] Oleg Kalugin, "Terrorism and the Human Intelligence: the Soviet Experience," *The Brown Journal of World Affairs* 11, no. 1 (2004): 183-184.

However, if CANSOFCOM intelligence is to have access to a HUMINT capability, and if it is to be expert at exploiting this valuable means of collection, it needs to be cognizant of the potential serious risks inherent to this capability. The risks associated with HUMINT are many and potentially grave. While it is not appropriate to provide a detailed appreciation of all the risks here, it is worth providing some examples to underscore the point. First, HUMINT operations inherently deal with treachery, and human sources willing to engage in acts of serious betrayal need to be treated with suspicion from the outset. Also, some sources may tell their handlers what they want to hear simply to gain financial benefit. Others with more honesty may pass on bad information they genuinely believe to be true (as was the case with Iraqi military commanders who advised U.S. and European handlers that Iraq possessed WMD).[146] American SOF in Afghanistan found that sources sometimes deliberately provided inaccurate information in an attempt to have their enemies targeted by U.S. forces.[147] There is also the very serious risk that a source could be a double agent. Such a person could prove extremely dangerous, for example, by leading friendly forces into an ambush. Then there are internal bureaucratic problems that may beset HUMINT collection. For example, former CIA members have criticized the agency for rewarding field officers for the number of sources they recruited rather than the quality of information they obtained, resulting in the frequent recruiting of sources who provide little value.[148] All of these can threaten the mission or needlessly risk operators' lives.

HUMINT operations can also be politically risky. For agents to have intelligence value, they must often be associated with illegal activities, which can result in

[146] Mahnken, *Spies and Bureaucrats*, 37.
[147] Cline, *Special Operations and the Intelligence System*, 579.
[148] Mahnken, *Spies and Bureaucrats*, 36.

accusations towards intelligence agencies of unethical behaviour. This occurred, for example, in Northern Ireland where critics scorned the British Special Branch for allegedly turning a blind eye towards—or even deliberately obscuring—serious crimes committed by informers, including murder. The overarching lesson for CANSOFCOM is that HUMINT operations have potential to be dangerously misleading, politically embarrassing, or even associated with grave human rights abuses.[149] Intelligence personnel therefore need to be trained to understand fully how to direct HUMINT collection, remaining cognizant of the potential risks while aggressively exploiting the capability to the fullest extent. Such training could be part of the orientation training regime recommended in the paper's previous section.

Interrogation, a specific form of HUMINT, is another collection discipline CANSOFCOM intelligence will likely require. Interrogation of captured personnel has tremendous potential for providing valuable information, particularly for counter-terrorism operations. A highly-trained interrogator can obtain valuable information that cues further operations or disrupts extremist plots.[150] Substantial evidence emphasizes the importance of interrogation to fighting insurgency and extremists.

For example, CIA post-9/11 interrogation efforts, despite sensationalist media coverage, and conducted under very close Justice Department scrutiny, produced invaluable intelligence that enabled the U.S. to disrupt terrorist plots in America and abroad. Declassified documents show that CIA interrogation produced critically important information, uncovering plans to attack the American consulate in Karachi, fly aircraft into London's Heathrow airport, derail a train in the U.S., fly aircraft into a

[149] Gill, *Security Intelligence and Human* Rights, 93-94.

[150] Amos N. Guiora and Erin M. Page, "The Unholy Trinity: Intelligence, Interrogation and Torture," *Case Western Reserve Journal of International Law* 37, no.2/3 (2006): 446.

building in California, and destroy bridges in New York City.[151] Interrogation has proven particularly valuable for special operations. JSOC units in Iraq routinely employed interrogators to extract information from detainees, frequently obtaining actionable information that cued subsequent operations, sometimes launched the same day.[152] Intelligence derived from interrogation led to Saddam Hussein's capture.[153] Interrogation also yielded the starting point for locating Abu Musab al-Zarqawi, thanks to skilful interrogators who gradually convinced a detainee that Al Qaida in Iraq acted immorally by killing innocent civilians and that cooperating was the right thing to do.[154]

But just as with using informers, there are significant risks with interrogation that CANSOFCOM must be cognizant of. Research shows that one of the biggest challenges of using interrogation-derived information is gauging its accuracy which for several reasons may be suspect. The interrogated individual's knowledge may simply be wrong or may have been inaccurately recalled. There is also a possibility of deception.[155] Research shows that deception is very difficult to detect, regardless of an interrogator's expertise or experience. Even when the most modern techniques to detect deception are used, success is barely above 50 per cent.[156]

A particularly problematic aspect of interrogation is that it has potential to be ethically difficult. Interrogation inherently requires that detainees be deceived, seduced

---

[151] Richard Lowry, "Getting to the Truth," *National Review* 61, no. 17 (2009): 39-40.
[152] Peritz and Rosenbach, *Find, Fix, Finish*, 128.
[153] Department of Defense, *Final Report of the Independent Panel*, 65.
[154] Brookings Institution, *The Evolution of Joint Special Operations Command and the Pursuit of Al Qaeda in Iraq: A Conversation with General Stanley A. McChrystal*, 22.
[155] Jacqueline R. Evans, Christian A. Meissner, Susan E. Brandon, Melissa B. Russano, and Steve M. Kleinman, "Criminal versus HUMINT Interrogations: the Importance of Psychological Science to Improving Interrogative Practice," *The Journal of Psychiatry & Law* 38, no. 1/2 (2010): 226-227.
[156] *Ibid*., 231-232.

or coerced in ways that some would find distasteful.[157] And there can be no risk whatsoever that authorized interrogation techniques be exceeded, resulting in human rights abuse. Close oversight of interrogation operations is therefore essential to guard against potential abuse, such as that which occurred at Abu Ghraib by intelligence personnel and poorly-trained reservists.[158] (Quite aside from the ethical reasons to prevent abuse, inappropriately harsh interrogation—including torture—is ineffective and counter-productive.[159]) Even the perception of abuse can be strategically disastrous, as the British in Northern Ireland learned. British interrogators used five techniques to prepare detainees for interrogation, including "wall standing, hooding, continuous white noise, food denial and sleep deprivation."[160] While certainly unpleasant for the detainee, these techniques can hardly be equated with torture. Many Western militaries subject their own personnel to these same techniques during training. Nonetheless, public outrage over allegations of abuse proved a propaganda disaster that drove many moderate community members against the British. Worse, the Republic of Ireland brought charges of abuse against the British to the European Court of Human Rights, which in 1976 and 1978 found the British government guilty of "inhuman and degrading treatment."[161]

Despite the myriad potential problems with interrogation, however, it has proven a remarkably valuable collection technique. As such, CANSOFCOM should consider the benefits of maintaining access to an interrogation capability in support of the high-readiness expeditionary SOTFs. At the same time, though, CANSOFCOM intelligence personnel must have a clear understanding of the potential problems that can accompany

---

[157] Department of Defense, *Final Report of the Independent Panel*, Annex H, 1.
[158] Gill, *Security Intelligence and Human Rights*, 78 and 95.
[159] Hulnick, *What's Wrong with the Intelligence Cycle*, 971.
[160] Scott and Hughes, *Intelligence in the Twenty-First Century*, 16.
[161] *Ibid.*, 15-17.

this otherwise excellent collection method and appreciate that appropriate measures should be taken to preclude the strategic embarrassments suffered by other nations using interrogation.

Finally, CANSOFCOM intelligence requires an exploitation capability. Exploitation is an intelligence discipline that extracts information from captured personnel (i.e. biometric data) and equipment such as documents and electronic media.[162] Exploitation in the modern sense is a relatively new capability that emerged only after 9/11, prior to which the discipline and its enormous potential (especially for document and electronic media exploitation, or DOMEX) were poorly understood.[163] But in recent years, exploitation has quickly developed into a remarkably fruitful collection discipline that supplements other modes of collection by providing information that cannot otherwise be gathered. For example, items recovered from an objective—such as documents, computers, cell phones and "pocket litter" or materials carried by captured personnel—can yield unique information that provides insight into an adversary's organization and its plans.[164] Moreover, intelligence derived from exploitation generally has less uncertainty than intelligence from HUMINT or interrogation because it comes from material that adversaries never expect to be captured. It is therefore generally free from the potential deception or exaggeration associated with other collection disciplines.[165] In March 2009, Defence Intelligence Agency (DIA) officials, including the agency's Director, Lieutenant General Michael Maples, advised a Congressional inquiry that "there is no doubt that DOMEX provides critical intelligence unavailable

[162] Charles D. Faint, "Exploitation Intelligence (EXINT): A New Intelligence Discipline?" *American Intelligence Journal* 29, no. 1 (2011): 68.
[163] Colonel Joseph M. Cox, "DOMEX: The Birth of a New Intelligence Discipline," *American Intelligence Journal* 29, no. 2 (2010): 22.
[164] Flynn, Juergens and Cantrell, *Employing ISR*, 60.
[165] Cox, *DOMEX: The Birth of a New Intelligence Discipline*, 27.

through any other discipline."[166] The unquestionable and now obvious importance of exploitation prompted Colonel Joseph Cox, a veteran U.S. Army intelligence officer, to declare "Saying there is DOMEX-enabled intelligence is akin to stating there is bullet-enabled infantry."[167] Moreover, in recent years, the capture of digital media has increased exponentially, indicating that exploitation`s usefulness will intensify as adversaries increasingly use personal electronic devices and other digital technology.[168]

Furthermore, exploitation is a vital contributor to F3EAD because by providing insight into an adversary's organization and by offering leads that cue follow-on operations, it turns the process into a true cycle.[169] Exploitation has therefore proven an important capability for American SOF. JSOC units in particular have increasingly used exploitation programs—processing captured cell phones, computers, documents and personnel—to cue follow-on operations.[170] According to General (retired) Stanley McChrystal, exploitation proved a "big revolution" for JSOC in Iraq. In 2003, generating actionable intelligence from the results of a raid took up to two weeks, but by 2006, units could conduct three raids in a night, with the last two cued purely by information collected and processed during that evening's operations.[171] Meanwhile, the British Army now recognizes in its doctrine the importance of exploitation to driving the F3EAD cycle, emphasizing that the exploitation of captured material needs to be conducted

[166] *Ibid*.
[167] *Ibid*., 25.
[168] *Ibid*., 27-29.
[169] Flynn, Juergens and Cantrell, *Employing ISR*, 57.
[170] Peritz and Rosenbach, *Find, Fix, Finish*, 7.
[171] Brookings Institution, *The Evolution of Joint Special Operations Command and the Pursuit of Al Qaeda in Iraq: A Conversation with General Stanley A. McChrystal*, 14.

quickly after an operation because of the potential for obtaining intelligence that cues follow-on operations.[172]

The point for CANSOFCOM is that exploitation is an emerging discipline that is increasingly seen as vital for enabling intelligence operations against discrete, networked adversaries. It is an area in which close allies are increasingly investing and developing expertise. CANSOFCOM access to an exploitation capability would contribute to meeting the requirement, as deduced in chapter 3, to identify and locate highly-evasive human targets. Failing to develop access to an exploitation capability for CANSOFCOM intelligence would be tantamount to passing on an emerging capability whose effectiveness against non-state adversaries is proven. It could also leave CANSOFCOM intelligence trailing behind its close allied counterparts.

This section argues that the structure of CANSOFCOM's intelligence function must be designed in a way that guarantees a capability to deliver on-demand, multi-source intelligence support to tactical operations. To support this argument, this section contends that the weight of the personnel force should be vested in standing unit-level close intelligence support organizations. Furthermore, CANSOFCOM's intelligence structure should include on-demand access to certain collection capabilities—especially aerial ISR (SIGINT/FMV), HUMINT, interrogation and exploitation—though it is not clear that such capabilities need to be organic to the intelligence function. Indeed, the argument here is purely for access to intelligence collection effects. Identifying under whose command such capabilities should exist, or if CANSOFCOM intelligence should

[172] Ministry of Defence, *British Army Field Manual Volume 1 Part 10: Countering Insurgency*, 5-9 and 5-10.

simply access such services from external agencies,[173] requires further consideration that is beyond the scope of this paper.

Optimizing CANSOFCOM Intelligence in the Domain of Process

The two previous sections on People and Structure offer insight into several areas where investment of effort and resources would contribute significantly to optimizing the CANSOFCOM intelligence function. However, building a world-class intelligence support organization necessitates doing all that is possible to achieve the best-possible performance. As such, this section argues that the Command's intelligence function should implement a series of processes that would promote the best prospects for intelligence success. In particular, this section builds on the previous two by examining processes that, when added to the recommendations made thus far, would complete meeting the requirements deduced in chapter 3. It focuses on processes that would guard against intelligence failure, provide an appropriate targeting doctrine (especially the F3EAD cycle), network CANSOFCOM intelligence with Canadian agencies and international partners, and guarantee intelligence oversight.

In this examination of processes that would benefit CANSOFCOM intelligence, it is necessary to address a problematic but very real and inescapable phenomenon: the inevitability of intelligence failure. A very strong body of scholarly literature examining intelligence failures shows that, for several reasons, it is impossible to avoid them. For

[173] The CF and other agencies continue to develop ISR capabilities for domestic and expeditionary purposes that could be of value to CANSOFCOM. The CF's Force Development organization provides an excellent overview of national surveillance capabilities and limitations in Department of National Defence, *Department of National Defence/Canadian Forces National Surveillance Study 2010* (Ottawa: Chief of Force Development, 2011).

one thing, intelligence assessments are fundamentally judgements based on incomplete information. They cannot possibly exclude error each time, regardless of the assessor's cognitive capability.[174] Sometimes, though, intelligence failures result from poor intelligence work. Other times, authorities level accusations of intelligence failure, sometimes unfairly, in the face of an unrealized prediction or an unpredicted event that catches people off guard.[175] Regardless, unpredictable surprises, including serious "Black Swan" events, are very much an inescapable phenomenon.[176] Furthermore, some intelligence blindness is inevitable simply because the adversary is a calculating, adaptive human who will occasionally succeed in outmanoeuvring even the best intelligence organization.[177] While these problems are not unique to CANSOFCOM, it is worth considering what the Command can do to minimize the potential for intelligence failure by harnessing factors under its control.

One process that can minimize the risk of intelligence failure is to become a continuously learning organization. Professor Thomas Mahnken—whose extensive intelligence experience includes numerous executive-level jobs in the U.S. Defense Department and operational experience as a military intelligence officer—contends that intelligence organizations tend to do a poor job in measuring the quality of their analysts' work, unlike other professional groups, such as doctors, traders, and lawyers, that maintain clear measures of success. Mahnken recommends that after conducting analytical activities, intelligence organizations should hold after-action reviews—just as

[174] Evans, *Rethinking Military Intelligence Failure*, 25.

[175] John Hollister Hedley, "Learning from Intelligence Failures," *International Journal of Intelligence and Counterintelligence* 18, no. 3 (2005): 435-436.

[176] Devine, *Tomorrow's Spygames*, 150. Scholar/writer Nassim Taleb coined the term Black Swans to describe the inevitability of shocking events that arrive without warning in *The Black Swan: The Impact of the Highly Improbable* (New York: Random House, 2007).

[177] Betts, *Fixing Intelligence*, 44.

other military organizations do—to ascertain what went well, what did not, and why. Such reviews should be routine, and not conducted only after intelligence failures, to uncover biases, unmask bad assumptions and reveal if analysts truly understand their subjects.[178] CANSOFCOM intelligence should implement this simple process and commit to being a continuously learning organization that routinely assesses its own performance against established measures of effectiveness.

Another process that can diminish the risk of intelligence failure is to ensure that clear direction always drives the intelligence effort. Indeed, it is vital from the outset of any operation that intelligence staff receive clear direction to ensure that the intelligence effort is applied efficiently and only against the commander's requirements. That serious misfortune can result from poor direction is exemplified by such high profile disasters as the Dieppe raid in 1942, the Tet Offensive in 1968, the surprise Egyptian-Syrian attack on Israel in 1973, and the Argentinean invasion of the Falkland Islands in 1982. In each of these cases, sufficient information had been collected to warn of the impending threats, but the right questions had not been asked, permitting important pieces of information to go unheeded.[179] Unfortunately, it is not clear that modern militaries always appreciate the importance of issuing clear direction to intelligence staffs.[180] But without clear direction, as Geraint Evans so aptly states, "the remaining elements [of the intelligence

[178] Mahnken, *Spies and Bureaucrats*, 39-40. Professor Mahnken's expertise is in strategy, intelligence and SOF.

[179] Evans, *Rethinking Military Intelligence Failure*, 34-35.

[180] This is not to suggest, however, that such a state exists in CANSOFCOM. In fact, the publicly available information regarding the Command's operations, at least in Afghanistan, suggests that CANSOFCOM intelligence has benefited from clear direction. David A. Charters, "Canadian Military Intelligence in Afghanistan," *International Journal of Intelligence and Counterintelligence* 25, no. 4 (2012): 486. Also, J. Paul de B. Taillon notes that "In Afghanistan, the Canadian Special Operations Intelligence Cell (SOIC) reportedly set the standard for intelligence support for SOF operations," in "Coalition Special Operations Forces: Building Partner Capability," *The Canadian Military Journal* 8, no. 3 (2007): 54.

cycle] are pointless and self-serving."[181] As such, the CANSOFCOM intelligence function cannot succeed, let alone be optimized, if commanders, operators and appropriate staffs are not closely engaged in directing the intelligence effort. It is argued here, then, that intelligence officers—in CANSOFCOM and elsewhere—must be cognizant of their responsibility to keep their commanders well-advised as to the capabilities, strengths and limitations of their intelligence organizations, to seek clear direction, and to ensure that all intelligence efforts are expended solely towards meeting commander and operator requirements.[182]

The analysis in chapter 3 concluded that CANSOFCOM intelligence requires a process to locate and track human targets that in the future are likely to include adversaries who hide amongst the population and are difficult to discern. Chapter 3 therefore suggested that the F3EAD targeting cycle would be an ideal doctrine, based on the cycle's proven effectiveness in fighting insurgents and extremists since 9/11.

There is a counter-argument, however, to the notion that F3EAD is the ideal cycle for combating insurgents and non-state actors. Chief Warrant Officer 4 Jimmy Gomez of the U.S. Army, whose service includes duty in Afghanistan and Iraq, warns that the F3EAD cycle has a serious flaw, despite its effectiveness for targeting high-value individuals. Gomez warns that the cycle lacks a "decide" phase, which is necessary for enabling the commander to contemplate the desired effects of a targeting mission, such as a change in behaviour versus physical

[181] Evans, *Rethinking Military Intelligence Failure*, 34.

[182] Robert D. Steele (USMC retired) suggests that "the most vital part of the intelligence process" may occur when an intelligence officer interviews a decision-maker to understand exactly what intelligence is required, a process that ensures the value of subsequent products and prevents the tremendous waste that occurs from attempting to satisfy "half-baked questions." Robert D. Steele, *The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats* (Carlisle, PA: Strategic Studies Institute, 2002), 24-25.

destruction. He claims, therefore, that F3EAD can result in "targeting for the sake of targeting." He adds that the traditional D3A cycle (decide, detect, deliver, assess) is better for planning targeting campaigns.[183]

Gomez is not entirely correct. During the *Find* phase of F3EAD, particularly when considering a given target, interaction between the intelligence and operations staffs should include an assessment of potential effects that can be achieved. In fact, a common method of assessing a potential target and the effects of its prosecution is use of the acronym CARVER (criticality, accessibility, recuperability, vulnerability, effect and recognisability).[184] Using the CARVER model, or any similar process that demands consideration of the targeting effect, ensures that the F3EAD cycle meets the necessity to ensure the anticipated effect serves the overall campaign plan. What is more, targets are typically assigned, or at least authorized, by a theatre-level headquarters that very carefully considers the likely effect of each target's prosecution before directing it be struck. Therefore, Gomez's concerns with F3EAD should not detract CANSOFCOM from adopting F3EAD doctrine.

The analysis in chapter 3 concluded that CANSOFCOM intelligence should invest in standing and robust liaison with other Canadian intelligence agencies. Indeed, CANSOFCOM SOTFs are designed to support Whole of Government efforts and operate with other government organizations. Furthermore, the Command openly recognizes that its intelligence teams cannot

[183] Gomez, *The Targeting Process: D3A and F3EAD*, 13-14.

[184] For example, U.S. SOF doctrine is to use CARVER for analyzing targets. Department of Defense, *Field Manual 3-05.102—Army Special Operations Forces Intelligence* (Washington: Department of the Army, 2001), article 2-68, page 2-19.

operate independently and must be capable of integrating the support of other domestic security and intelligence agencies.[185] To be competent at integrating such external support demands that officers have a deep understanding of how the national security and intelligence community operates matched with a determination to achieve collaboration where possible.[186] For CANSOFCOM intelligence, then, this necessitates that intelligence staff implement liaison processes that maintain engagement with other agencies on a standing basis so that when a crisis occurs, relationships are already in place and the intelligence effort can be mobilized as quickly and completely as possible. Three agencies are of particular importance to CANSOFCOM intelligence, owing to their mandates and capabilities: the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS), and the Communications Security Establishment Canada (CSEC).

The RCMP is responsible for reducing the risk of terrorism across Canada through its national security law enforcement program. To fulfill this mission, the RCMP leads investigative units called Integrated National Security Enforcement Teams (INSETs) in major cities across Canada. INSETs are interagency teams with representatives from both federal agencies and provincial and municipal police forces.[187] In addition, the RCMP collaborates with the private sector to guard against terrorist threats to critical infrastructure and with community leaders

[185] Department of National Defence, *CANSOFCOM Capstone Concept for Special Operations*, 12 and 19.
[186] Rouleau, *Special Operations Forces: Shaping the Area of Operations*, 88.
[187] Royal Canadian Mounted Police, "Integrated National Security Enforcement Teams," last accessed 25 January 2013, http://www.rcmp-grc.gc.ca/secur/insets-eisn-eng.htm.

to counter threats of violence resulting from extremism and radicalization.[188] Clearly, the RCMP is at the forefront of understanding, and when necessary prosecuting, domestic extremist threats and is therefore a crucially important partner for CANSOFCOM intelligence.

CSIS is similarly important to CANSOFCOM intelligence. The CSIS mandate is to investigate and produce intelligence on security threats to Canada, with counter-terrorism the highest priority.[189] Since 9/11, CSIS has also increased its collection of intelligence outside Canada (which appears to have ended a debate as to whether Canada needs a new foreign intelligence agency).[190] Clearly, Canada's military counter-terrorism force should be networked closely with the national agency responsible for counter-terrorism intelligence. Indeed, CSIS's domestic and international intelligence capabilities could prove vital for intelligence support to CANSOFCOM counter-terrorism operations.[191]

If CANSOFCOM intelligence is to have the fullest possible understanding of the threat environment, it needs to maintain close liaison with both the RCMP and CSIS. Part of the reason is that because of their different mandates, these agencies may not always have the same perspective of the overall threat picture. CSIS, for example, has a mandate to collect threat information and intelligence (under sections 12 and 16 of the CSIS Act) that is not intended to meet criminal prosecution standards. Only when CSIS assesses it has enough information on a

---

[188] Ministry of Public Safety, *Building Resilience Against Terrorism*, 30.
[189] *Ibid*., 26.
[190] Fyffe, *The Canadian Intelligence Community After 9/11*, 10.
[191] In fact, DND deems that there needs to be closer integration between the whole department and the domestic security and intelligence community because of increasing threats of, amongst other things, terrorist and CBRN attacks in the future security environment. Department of National Defence, *The Future Security Environment*, 89.

given file to merit a criminal investigation is the information passed to the RCMP for consideration and further investigation.[192] Moreover, some argue that because of their differing mandates, friction between the RCMP and CSIS is possible, if not inevitable.[193] The aim here is certainly not to criticize the professionalism of these agencies, but rather to suggest that CANSOFCOM has a requirement to assess threat information and trends through its own lens, one that might inform the Command's decision makers on how CANSOFCOM should posture itself to be best prepared to respond when called upon.

CSEC is also highly likely to be relevant to CANSOFCOM in the future. The National Defence Act mandates CSEC to gather signals intelligence in support of the government's intelligence priorities and to render technical assistance to federal law enforcement and security intelligence agencies.[194] CSEC has already proven a valuable partner to DND in the complex and asymmetric battlespace by supporting CF operations in Afghanistan, providing military intelligence staff with a suite of capabilities including technical, linguistic and analytical services.[195] Experience also suggests that CSEC can be an important enabler for hostage rescue missions. In 2006, CSEC reportedly provided SIGINT that helped lead to the rescue of Canadian hostages in Iraq.[196]

A major reason why CSEC is potentially important to CANSOFCOM is the tremendous capability the agency either has or can access through its allied counterparts. CSEC enjoys access to enormous allied capability by virtue of the

[192] Lefebvre, *Canada's Legal Framework for Intelligence*, 254.
[193] Fyffe, *The Canadian Intelligence Community After 9/11*, 9.
[194] Ministry of Public Safety, *Building Resilience Against Terrorism*, 27.
[195] Rudner, *Canada's Communications Security Establishment, Signals Intelligence and Counter-Terrorism*, 483-484.
[196] *Ibid.*, 484.

longstanding five-eyes pact for sharing SIGINT amongst the U.S., Britain, Canada, Australia and New Zealand. For example, in 2007, because of CSEC's membership in the alliance, the agency's $220 million budget provided access to over $10 billion in SIGINT assets.[197] Moreover, since Canadian participation began in the war in Afghanistan, CSEC has proven a world-class SIGINT agency. Whereas during the Cold War Canada received up to 90 per cent of its foreign SIGINT from the five-eyes partners, after the CF deployment to Afghanistan, CSEC became a far greater contributor, generating about 85 per cent of the SIGINT used by Canadians. As such, CSEC became a significant contributor, and not just a consumer, of SIGINT within the five-eyes community.[198] CANSOFCOM would likely benefit from a close relationship with CSEC for the purpose of maintaining knowledge of how to access and exploit the latest SIGINT capabilities. This could be especially important for optimizing the Command's intelligence function, particularly as SIGINT technologies evolve that may prove useful for operating in the future's complex and austere battlespaces.

The aforementioned agencies by no means represent all the national organizations CANSOFCOM should be networked with. However, this brief discussion of their capabilities emphasizes the overarching contention that the Command's intelligence function cannot do its job alone and therefore needs to invest in maintaining meaningful liaison processes with other agencies, if it is to be capable of rendering the best possible intelligence support. Fortunately, a culture of interagency cooperation in Canada appears to be improving. The war

[197] *Ibid*., 479.
[198] *Ibid*., 482.

in Afghanistan in particular has fostered considerable cooperation among DND, the RCMP, CSIS and CSEC.[199]

But a note of caution is required here. The end of Canadian combat operations in Afghanistan may be see the doors of cooperation begin to close. Also, the oversight regime for Canada's intelligence and security community consists of separate oversight bodies for each agency, while Canada lacks a single body that oversees the intelligence community as a whole. This can permit the insidious practice of "stovepiping" to go unchecked. There is therefore risk that interagency cooperation may not always be practiced.[200] These facts reinforce the notion that CANSOFCOM intelligence needs to be linked with all national agencies that play important roles in combating extremism.

At the same time, CANSOFCOM intelligence needs to be networked with its counterparts in allied organizations. Chapter 2 emphasized that the future's serious threats are likely to be transnational in character, demanding transnational responses, and chapter 3 concluded that CANSOFCOM intelligence has a requirement to maintain standing liaison with counterparts in allied organizations with which the Command may operate. Indeed, the range of potential transnational threats—such as terrorism, nuclear proliferation, and the development WME—will require cooperation amongst international forces just to understand the threats, let alone prosecute them.[201] Therefore, CANSOFCOM

[199] Fyffe, *The Canadian Intelligence Community After 9/11*, 9.

[200] In addition, it is yet to be seen if the National Security Advisor, a position created under the National Security Policy of April 2004, will be influential in enforcing interagency cooperation. *Ibid*., 15-17.

[201] Lahneman, *Is A Revolution in Intelligence Affairs Occurring*, 201. CANSOFCOM recognizes this necessity in *CANSOFCOM Capstone Concept for Special Operations*, 19.

intelligence needs to maintain a liaison process that sustains working relationships with trusted international partners before such threats manifest.

By extension, interoperability with close allies is paramount. Of course, CANSOFCOM's allied counterparts face precisely the same potential threats as Canada. They too will be wrestling with issues such as how to locate and track highly evasive human targets in congested, austere battle spaces. CANSOFCOM intelligence can therefore learn from the intelligence support models developed by allies.[202] As such, close liaison is required to ensure that CANSOFCOM maintains intelligence interoperability by staying abreast of practices the greater SOF intelligence community develops to support operations. Close liaison would also allow CANSOFCOM to share its best practices, building credibility as a valued contributor. Staying current with new technologies and knowledge of how to integrate them will be vital for maintaining interoperability.

Conversely, failing to keep current on emerging technologies and evolving practices developed by the greater SOF intelligence community would undermine the Command's interests. CANSOFCOM intelligence could find itself behind allied counterparts, using obsolete methodologies for acquiring and tracking targets. This would not only constitute failure to maintain currency with best-possible intelligence practices, but would also endanger interoperability. The result could be damaged credibility and a perception of amateurism. A strong case therefore exists for placing a high priority in maintaining strong links with close allied intelligence counterparts via a robust liaison process.

[202] Lieutenant Colonel Cody Sherman, J2 CANSOFCOM, conversation with author, 13 February 2013.

Finally, owing to the high attention paid in Canada to ensuring close scrutiny of intelligence agencies, the matter of intelligence oversight merits attention. The government and public take very seriously the importance of strategic oversight of national security and intelligence bodies. Canada's counter-terrorism strategy reflects this, emphasizing that "principles matter" and that agencies must not compromise democratic values while countering terrorist threats. As such, "adherence to the rule of law" is a fundamental principle of the national counter-terrorism strategy. Federal laws therefore govern Canadian counter-terrorism efforts to ensure they respect the Constitution, while oversight and review programs ensure that counter-terrorism programs do not erode the nation's cherished liberties or permit abusive practices.[203] For example, the Security Intelligence and Review Committee (SIRC) reviews CSIS operations to ensure Charter rights are upheld. The Auditor General and the Privacy Commissioner review RCMP operations, while the Commission for Public Complaints investigates grievances against the RCMP. The CSEC Commissioner reviews CSEC operations to ensure they comply with the law. The CF, however, has no external oversight body for its intelligence operations.[204]

But military intelligence is not without scrutiny, and CANSOFCOM's intelligence activities can come under close examination at any time from a number of groups. At the highest level, the Cabinet Committee on National Security (CCNS), chaired by the Prime Minister, addresses all national intelligence issues and annually approves national intelligence priorities. Below

[203] Ministry of Public Safety, *Building Resilience Against Terrorism*, 10-11.
[204] Shore, *Intelligence Review and Oversight in Post-9/11 Canada*, 456 and 463-466.

the CCNS, the Deputy Ministers' Intelligence Collection Committee reviews and directs federal intelligence efforts in support of government priorities. There is also a Deputy Ministers' Intelligence Assessment Committee which permits the Chief of Defence Staff and DND's Deputy Minister to discuss with their counterparts intelligence issues and policies. Within DND, the CDI leads the Defence Intelligence Management Committee (DIMC), which is attended by the Service and operational-level J2s (or equivalents) as well as appropriate Associate Deputy Ministers. The DIMC coordinates strategic direction to the military intelligence community and provides functional oversight of military intelligence operations.[205] And finally, as already emphasized, the CDI oversees CF intelligence activities as Functional Authority for military intelligence.[206]

It is essential that CANSOFCOM's intelligence leadership acknowledges the tremendous emphasis the government places on intelligence oversight, as there must be no risk that the Command's intelligence activities could be perceived as contravening laws or policies. Several factors, however, could result in such suspicion. The Command's operations and procedures generally remain secret and, like SOF activities in general, can be surrounded by an air of mystique that permits ill-informed and mistaken impressions to develop. And, as argued in this paper, the Command's intelligence function needs to employ a wide range of high-end intelligence capabilities, some of which—such as agent handling,

[205] Chief of Defence Intelligence staff, email correspondence with author, 19 November 2013.

[206] Department of National Defence, *Canadian Forces Joint Publication 01—Canadian Military Doctrine*, art 0540 page 5-9. At the time of writing, the CDI's staff was producing a suite of policies that will provide explicit direction to all levels of military intelligence activity down to the tactical level. The keystone document will be a Ministerial Directive for Defence Intelligence that will articulate the government's goals and objectives for military intelligence, laws and policies to be respected, and when the Minister and other authorities are to be consulted regarding military intelligence capabilities or activities. Chief of Defence Intelligence staff, email correspondence with author, 19 November 2013.

interrogation, and SIGINT—are potentially rather sensitive. In some cases, collection capabilities are governed by other agencies that will need to be confident that CANSOFCOM intelligence fully respects regulatory exigencies.[207] Furthermore, CANSOFCOM's domestic counter-terrorism mandate may necessitate from time to time that intelligence staff maintain situational awareness of potential threats that could result in a request for CANSOFCOM support to the RCMP, including sensitive domestic threats that would otherwise be beyond the concern of military authorities. For these reasons, CANSOFCOM intelligence should implement a proactive process of self-oversight that prevents perceptions from developing that the Command conducts intelligence activities outside the bounds of law or policy. The J2 is central to ensuring that CANSOFCOM intelligence activities are effectively self-policed and fully respect the letter and spirit of the law. Meanwhile, all CANSOFCOM intelligence professionals should at all times jealously guard the Command's credibility.

This chapter focused on potential investment areas in the domains of People, Structure, and Process that would contribute to optimization of the CANSOFCOM intelligence function, based on the likely future requirements deduced in chapter 3. The analysis presented here, however, should not be taken to suggest that CANSOFCOM intelligence is not currently focused on any of these areas. Rather, the aim has been to conduct a theoretical investigation of potential investment areas to inform the ongoing development of CANSOFCOM intelligence.

[207] Lieutenant Colonel Cody Sherman, J2 CANSOFCOM, conversation with author, 13 February 2013.

CONCLUSION

The future security environment is all but certain to include difficult challenges to international stability. Hybrid warfare, complex urban and littoral battlespaces and non-state combatants that hide within the civilian population are likely to present complicated military challenges. Terrorism will continue to be a tool of choice for extremists, some of whom are likely to seek WME to deal shocking, asymmetric blows against nation-states. Countering such threats will require forces capable of identifying, locating, tracking and targeting adversaries, using precision force to avoid harming innocent civilians. This is an environment for which CANSOFCOM is very well-suited. However, the Command's operations are dependent upon high-quality intelligence. As such, it is worthwhile to consider how the CANSOFCOM intelligence function can be optimized to deal with future threats and deliver the best possible intelligence support.

This paper began by examining the future security environment, based on projections made by the academic and military communities, focusing on those aspects of particular relevance to CANSOFCOM. By juxtaposing the Command's core tasks and roles with the future security environment, deductions emerged regarding the probable scope of future CANSOFCOM intelligence tasks. Key judgements included the need to operate jointly with other agencies in Whole of Government efforts, the likely requirement to support complex expeditionary missions that may include hostage rescue and counter-terrorism, and the requirement to be capable of locating and tracking elusive targets in complex urban and littoral battlespaces. Based on these overarching demands, this paper identified areas where CANSOFCOM intelligence could invest effort so as to

optimize itself for supporting future operations. For organizational purposes, these areas were grouped under the domains of People, Structure, and Process.

Major conclusions under the domain of People included emphasizing the importance of populating the Command's intelligence organization with high-calibre, professionally well-developed personnel, the intelligence function's core resource. It is necessary to recruit the right people using a tailored screening process. Those accepted for service should, on joining the Command, receive special training to provide them with the skills and knowledge necessary for succeeding in CANSOFCOM's demanding intelligence environment. They should also be inculcated with an organizational culture that is based on the Command's ethos and further emphasizes traits that are essential for the intelligence function.

In the domain of Structure, the bulk of the Command's intelligence personnel should be weighted towards the SOTF SOICs, as close as possible to the tactical commanders and operators who require intelligence support. Meanwhile, the J2 staff should invest resources towards satisfying the Commander's situation awareness and I&W requirements, in a substantial liaison program that keeps CANSOFCOM intelligence tightly integrated with appropriate national agencies and allied counterparts, and in Force Development activities that support the SOTF SOICs' requirements to keep abreast of leading edge intelligence technologies. The Command's intelligence structure also needs to be capable of accessing certain intelligence collection capabilities that have proven usefulness for fighting non-state actors in complex environments. Such capabilities include high-end ISR platforms, HUMINT, interrogation, and exploitation. However, this paper does not assess whether or not such services should be organic to the

Command. Further research is required to determine where these collection capabilities would best reside.

Finally, in the domain of Process, the Command's intelligence function should maintain expertise in targeting doctrine. The F3EAD cycle offers an ideal model for targeting elusive non-state actors. CANSOFCOM intelligence should also consider taking measures where possible to minimize the potential risk of intelligence failure that affects all intelligence organizations. Commitment to being a continuously improving organization by developing analytical measures of success and routinely conducting intelligence after-action reviews would do much to ensure that analysis is kept to the highest possible standard. Also, the Command's intelligence organization needs to be networked closely with each of the relevant national agencies that provide critical threat situational awareness, such as the RCMP and CSIS, or essential technical support, such as CSEC. Indeed, CANSOFCOM should be intimately familiar with each of these agencies, maintaining standing relationships with key personnel and understanding fully the capabilities, perspectives, cultures and potential friction points of each organization. Similarly, CANSOFCOM intelligence should invest effort towards maintaining standing liaison and collaboration as appropriate with allied counterparts with whom the Command may operate. After all, the globalized nature of future threats will require globalized responses. Moreover, such relationships would help CANSOFCOM intelligence maintain a reputation as a valuable and contributing partner while benefiting from others' hard-won expertise. Finally, the Command J2 should proactively exercise self-governance of the Command's intelligence function to ensure that activities remain

entirely consistent with policies set by the CDI, the Functional Authority for all CF intelligence activities. Figure 5.1 summarizes this paper's findings.

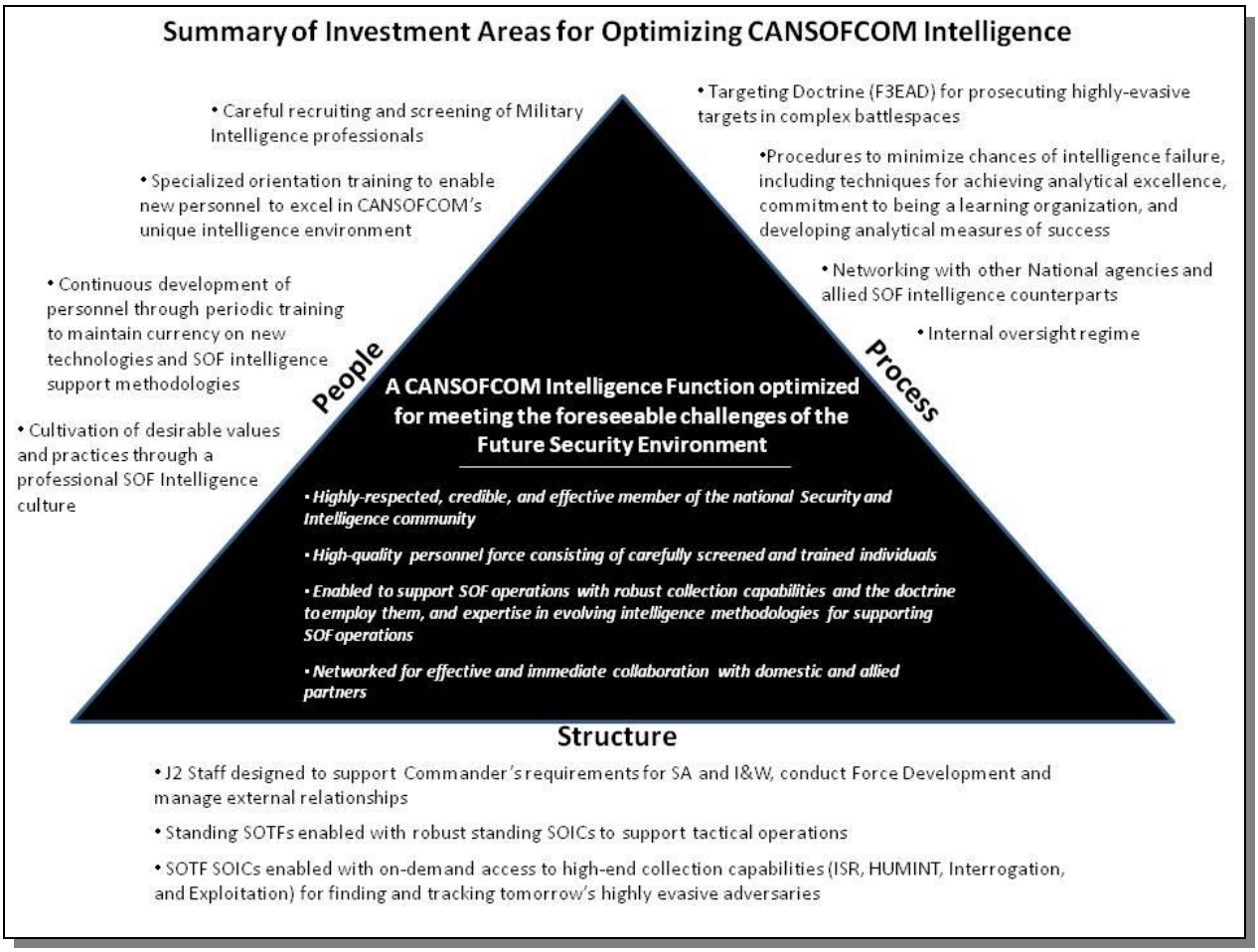

Figure 5.1

This paper is a forward-looking analysis that is in no way a critique of current practices or structure. It is, however, based on the premise that CANSOFCOM is a valuable military tool the nation is likely to use in the prosecution of future threats, and that intelligence plays a significant role in cueing the Command's operations. But high-

end intelligence does not come cheap. Just as SOF combat forces require carefully planned investments in personnel and capabilities, so too does SOF intelligence. In short, then, this paper argues that CANSOFCOM's intelligence function requires better-developed personnel and collection capabilities than Canadian military organizations normally possess.

Some of the specific investment areas identified in this paper require further research if they are to be implemented. For example, additional study is necessary to develop comprehensive screening programs for those applying to serve with CANSOFCOM intelligence. Similarly, a detailed training regime designed to promote analytical best-practices and check analytical faults calls for further examination. Furthermore, exactly how CANSOFCOM intelligence should access high-end collection services in the domains of ISR, HUMINT, interrogation and exploitation requires consideration. Such services could be organic to the Command or accessed from external agencies.

At the end of the day, it is vital that CANSOFCOM intelligence be prepared for the future's challenges that are now visible on the horizon. CANSOFCOM is by design intended to conduct high-risk missions of strategic importance and is certain to be called upon to do so. Intelligence will play an important role in assisting CANSOFCOM to fight and win. As such, it is important to think now, and indeed to continue thinking, about how best to apply finite resources while avoiding the known pitfalls that undermine intelligence organizations. This is necessary so that the intelligence function is capable of meeting the future's predictably difficult challenges and that it achieves the true excellence in intelligence CANSOFCOM requires.

Bibliography

Books

Dowell, Lieutenant Colonel J.A.E.K. *Intelligence for the Canadian Army in the 21st Century*. Jadex Papers 5. Kingston, Ontario: Department of National Defence, Directorate of Land Concepts and Designs, 2011.

Gardner, Dan. *Future Babble: Why Expert Predictions Fail—and Why We Believe Them Anyway*. Toronto: McClelland and Stewart, 2010.

Heuer, Richards J. *Psychology of Intelligence Analysis.* Washington, DC: Center for the Study of Intelligence—Central Intelligence Agency, 1999.

Marrin, Stephen. *Improving Intelligence Analysis: Bridging the Gap Between Scholarship and Practice.* New York: Routledge, 2011.

Peritz, Aki and Rosenbach, Eric. *Find, Fix, Finish: Inside the Counterterrorism Campaigns that Killed Bin Laden and Devastated Al-Qaeda.* New York: PublicAffairs Books, 2012.

Schein, Edgar H. *Organizational Culture and Leadership (Third Edition).* San Francisco: Jossey-Bass, 2004.

Steele, Robert D. *The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats*. Carlisle, PA: Strategic Studies Institute, 2002.

Professional and Scholarly Articles

Balasevicius, Tony. "Finding the Right Stuff: Special Operations Forces Selection." In *Casting Light on the Shadows: Canadian Perspectives on Special Operations Forces*, edited by Colonel Bernd Horn and Major Tony Balasevicius, 37-58. Kingston, Ont: Canadian Defence Academy Press, 2007.

Bar-Joseph, Uri. "The Professional Ethics of Intelligence Analysis." *International Journal of Intelligence and Counterintelligence* 24, no. 1 (2011): 22-43.

Bar-Joseph, Uri and McDermott, Rose. "Change the Analyst and Not the System: A Different Approach to Intelligence Reform." *Foreign Policy Analysis* 4, no. 2 (2008): 127-145.

Betts, Robert K. "Fixing Intelligence." *Foreign Affairs* 81, no. 1 (2002): 43-59.

Brown, Jason M. "To Bomb or Not to Bomb? Counterinsurgency, Airpower, and Dynamic Targeting." *Air & Space Power Journal* 21, no. 4 (2007): 75-85.

Butler, Amy. "Intel Posturing." *Aviation Week & Space Technology* 172, no. 46 (2010): 28.

Butler, Mathew N. "A Few Good Men: Support Soldier Selection and Training." *Special Warfare* 23, no. 6 (2010): 6-9.

Charters, David A. "Canadian Military Intelligence in Afghanistan." *International Journal of Intelligence and Counterintelligence* 25, no. 4 (2012): 470-507.

Cline, Lawrence E. "Special Operations and the Intelligence System." *International Journal of Intelligence and Counterintelligence* 18, no. 4 (2005): 579-592.

Collier, Michael W. "A Pragmatic Approach to Developing Intelligence Analysts." *Defense Intelligence Journal* 14, no. 2 (2005): 17-35.

Cox, Colonel Joseph M. " DOMEX: The Birth of a New Intelligence Discipline." *American Intelligence Journal* 29, no. 1 (2010): 65-69.

Danskine, William B. "Aggressive ISR in the War on Terrorism: Breaking the Cold War Paradigm." *Air and Space Power Journal* 19, no. 2 (2005): 73-83.

Dearlove, Sir Richard and Quiggin, Tom. "Contemporary Terrorism and Intelligence." *Institute of Defence and Strategic Studies Commentaries* 78 (2006): 1-3.

Devine, Jack. "Tomorrow's Spygames." *World Policy Institute* 25, no. 3 (2008): 141-151.

Downs, Lt Col Michael L. "Rethinking the Combined Force Air Component Commander's Intelligence, Surveillance, and Reconnaissance Approach to Counterinsurgency." *Air & Space Power Journal* 22, no. 3 (2008): 67-76.

Duncan, Andrew J. "From Ethos to Culture: Shaping the Future of Army Intelligence." *Canadian Army Journal* 9, no. 3 (2006): 41-51.

Erwin, Michael. "Integrating Intelligence with Operations." *Special Warfare* 21, no. 1 (2008): 10-15.

Evans, Geraint. "Rethinking Military Intelligence Failure—Putting the Wheels Back on the Intelligence Cycle." *Defence Studies* 9, no. 1 (2009): 22-46.

Evans, Jacqueline R., Meissner, Christian A., Brandon, Susan E., Russano, Melissa B. and Kleinman, Steve M. "Criminal versus HUMINT Interrogations: the Importance of

Psychological Science to Improving Interrogative Practice." *The Journal of Psychiatry & Law* 38, no. 1/2 (2010): 215-249.

Faint, Major Charles D. " DOMEX: The Birth of a New Intelligence Discipline." *American Intelligence Journal* 29, no. 1 (2010): 65-69.

Faint, Major Charles D. "Exploitation Intelligence (EXINT): A New Intelligence Discipline?" *American Intelligence Journal* 29, no. 1 (2011): 65-69.

Faint, Major Charles D. and Harris, Michael. "F3EAD: Ops/Intel Fusion "Feeds" the SOF Targeting Process." *Small Wars Journal* 8, no. 1 (2012). Last accessed 10 October 2012. http://50.56.4.43/jrnl/art/f3ead-opsintel-fusion-%E2%80%9Cfeeds%E2%80%9D-the-sof-targeting-process.

Flynn, Michael T., Juergens, Rich and Cantrell, Thomas L. "Employing ISR: SOF Best Practices." *Joint Force Quarterly* 50, no. 3 (2008): 56-61.

Forest, James J.F. "Global Trends in Kidnapping by Terrorist Groups." *Global Change, Peace & Security* 24, no. 3 (2012): 311-330.

Frankel, Matt. "The ABCs of Targeting: Key Lessons from High Value Targeting Campaigns Against Insurgents and Terrorists." *Studies in Conflict and Terrorism* 34, no. 1 (2011): 17-30.

Fyffe, Greg. "The Canadian Intelligence Community After 9/11." *Journal of Military and Strategic Studies* 13, no. 3 (2011): 1-17.

Follis, Luca. "Laboratory of War: Abu Ghraib, the Human Intelligence Network and the Global War on Terror." *Constellations* 14, no. 4 (2007): 635-660.

George, Scott and Ehlers, Robert. "Air-Intelligence Operations and Training: the Decisive Edge for Effective Airpower Employment." *Air and Space Power Journal* 22, no. 2 (2008): 61-67.

Gill, Peter. "Security Intelligence and Human Rights: Illuminating the 'Heart of Darkness'". *Intelligence and National Security* 24, no. 1 (2009): 78-102.

Goodman, Glenn W. "ISR Now Synonymous with Operations." *Journal of Electronic Defence* 30, no. 7 (2007): 19-20.

Gomez, Jimmy A. "The Targeting Process: D3A and F3EAD." *Small Wars Journal* 7, no. 7 (2011).

Guiora, Amos N. and Page, Erin M. "The Unholy Trinity: Intelligence, Interrogation and Torture." *Case Western Reserve Journal of International Law* 37, no.2/3 (2006): 427-447.

Hammond, Thomas H. "Intelligence Organizations and the Organization of Intelligence." *International Journal of Intelligence and Counterintelligence* 23, no. 4 (2010): 680-724.

Hedley, John Hollister. "Learning from Intelligence Failures." *International Journal of Intelligence and Counterintelligence* 18, no. 3 (2005): 435-450.

Hoffman, Frank. "Hybrid Warfare and Challenges." *Joint Force Quarterly* First Quarter, no. 52 (January 2009): 34-39.

Horn, Bernd. "Burn the Witch: A Case for Special Operations Forces." *The Army Doctrine and Training Bulletin* 2, no. 3 (August 1999).

Hubbard, Robert L. "Another Response to Terrorism: Reconstituting Intelligence Analysis for 21st Century Requirements." *Defense Intelligence Journal* 11, no. 1 (2002): 71-80.

Hull, Jeanne. "We're All Smarter than Any One of Us." *Journal of Public and International Affairs* 19, no. 1 (2008): 28-50.

Hulnick, Arthur S. "What's Wrong with the Intelligence Cycle?" *Intelligence and National Security* 21, no. 6 (2006): 959-979.

Hutchinson, H. Frederick. "The Risks of Conventional Wisdom." *International Journal of Intelligence and Counterintelligence* 23, no. 4 (2010): 786-792.

Kalugin, Oleg. "Terrorism and the Human Intelligence: the Soviet Experience." *The Brown Journal of World Affairs* 11, no. 1 (2004): 183-187.

Kauppi, Mark V. "Counterterrorism Analysis 101." *Defense Intelligence Journal* 11, no. 1 (2002): 39-53.

Lahneman, William J. "Is A Revolution in Intelligence Affairs Occurring?" *International Journal of Intelligence and Counterintelligence* 20, no. 1 (2007): 1-17.

Lahneman, William J. "The Need for a New Intelligence Paradigm." *International Journal of Intelligence and Counterintelligence* 23, no. 2 (2010): 201-225.

Lefebvre, Stéphane. "Canada's Legal Framework for Intelligence." *International Journal of Intelligence and Counterintelligence* 23, no. 2 (2010): 247-295.

Lindemann, Marc. "Laboratory of Asymmetry: The 2006 Lebanon War and the Evolution of Iranian Ground Tactics." *Military Review* 90, no. 3 (2010): 105-116.

Lowry, Richard. "Getting to the Truth." *National Review* 61, no. 17 (2009): 38-40.

Mackubin, Thomas Owens. "Reflections on Future War." *Naval War College Review* 61, no. 3 (2008): 61-76.

Mahnken, Thomas G. "Spies and Bureaucrats: Getting Intel Right." *Public Interest* 159, no.1 (2005): 22-42.

Marrin, Stephen. "Adding Value to the Intelligence Product." In *Handbook of Intelligence Studies,* edited by Lock K. Johnson, 199-210. New York: Routledge, 2007.

Marrin, Stephen. "Training and Educating U.S. Intelligence Analysts." *Journal of Intelligence and Counterintelligence* 22, no.1 (2008): 131-146.

Metz, Lieutenant General Thomas F., Tait, Colonel William J., and McNealy, Major J. Michael. "OIF II: Intelligence Leads Successful Counterinsurgency Operations." *Military Intelligence Professional Bulletin* 31, no. 3 (2005): 10-15.

Nolte, William M. "Ethics and Intelligence." *Joint Force Quarterly* 54 (July 2009): 22-29.

Rimsa, Kostas. "Very Special Forces." In *Inside Canadian Intelligence: Exposing the New Realities of Espionage and International Terrorism,* edited by Dwight Hamilton, 161-173. Toronto: Dundurn, 2011.

Rouleau, Mike. "Special Operations Forces: Shaping the Area of Operations." In *Special Operations Forces: A National Capability*, edited by Emily Spencer, 87-93. Kingston, Ontario: Canadian Defence Academy Press, 2011.

Rudner, Martin. "Canada's Communications Security Establishment, Signals Intelligence and Counter-Terrorism." *Intelligence and National Security* 22, no. 4 (2007): 473-490.

Scott, Len and Hughes, R. Gerald. "Intelligence in the Twenty-First Century: Change and Continuity or Crisis and Transformation." *Intelligence and National Security* 24, no. 1 (2009): 6-25.

Shore, Jacques J.M. "Intelligence Review and Oversight in Post-9/11 Canada." *International Journal of Intelligence and Counterintelligence* 19, no. 3 (2006): 456-479.

Simons, Anna. "The Evolution of the SOF Soldier: An Anthropological Perspective." In *Force of Choice: Perspectives on Special Operations*, edited by Bernd Horn, J. Paul de B. Taillon, and David Last, 79-91. Montreal and Kingston: McGill-Queen's University Press, 2004.

Sullivan, John P. and Wirtz, James J. "Terrorism Early Warning and Counterterrorism Intelligence." *International Journal of Intelligence and Counterintelligence* 21, no. 1 (2008): 13-25.

Taillon, J. Paul de B. "Canadian Special Operations Forces: Transforming Paradigms." *Canadian Military Journal* 6, no. 4 (2006): 67-76.

Taillon, J. Paul de B. "Coalition Special Operations Forces: Building Partner Capability." *The Canadian Military Journal* 8, no. 3 (2007), 54.

Wastell, Colin A. "Cognitive Predispositions and Intelligence Analyst Reasoning." *International Journal of Intelligence and Counterintelligence* 23, no. 3 (2010): 449-460.

Westhusing, Ted. "'Target Approval Delays Cost Air Force Key Hits': Targeting Terror: Killing Al Qaeda the Right Way." *Journal of Military Ethics* 1, no. 2 (2002): 128-135.

White, Ralph K. "Empathy as an Intelligence Tool." *International Journal of Intelligence and Counterintelligence* 1, no. 2 (1986): 57-75.

Wolfberg, Adrian. "To Transform into a More Capable Intelligence Community: A Paradigm Shift in the Analyst Selection Strategy." 22nd Annual Chairman of the Joint Chiefs of Staff Strategy Essay Competition paper, U.S. National War College, 2003.

Public Documents

Brookings Institution. *The Evolution of Joint Special Operations Command and the Pursuit of Al Qaeda in Iraq: A Conversation with General Stanley A. McChrystal.* Washington: the Brookings Institution, 2013.

Canada. Department of National Defence. *Canadian Special Operations Forces Command: An Overview.* Ottawa: Canadian Special Operations Forces Command, 2008.

Canada. Department of National Defence. *CANSOFCOM Capstone Concept for Special Operations*. Ottawa: Canadian Special Operations Forces Command, 2009.

Flynn, Major General Michael T., Pottinger, Captain Matt and Batchelor, Paul. *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan.* Washington: Center for a New American Security, 2010.

Granatstein, J.L., Smith, Gordon S. and Stairs, Denis. *A Threatened Future: Canada's Future Security Environment and its Security Implications.* Calgary: Canadian Defence and Foreign Affairs Institute, 2007.

Official Documents

Canada. Department of National Defence. *Canadian Forces Joint Publication 01—Canadian Military Doctrine.* Ottawa: Joint Doctrine Branch, 2011.

Canada. Department of National Defence. *Department of National Defence/Canadian Forces National Surveillance Study 2010.* Ottawa: Chief of Force Development, 2011.

Canada. Department of National Defence. *Joint Intelligence Doctrine.* Ottawa: National Defence Headquarters, 2003.

Canada. Department of National Defence. *The Future Security Environment 2008-2030.* Ottawa: Chief of Force Development, 2009.

Canada. Ministry of Public Safety. *Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy*. Ottawa: Government of Canada, 2011.

Great Britain. Ministry of Defence. *British Army Field Manual Volume 1 Part 10: Countering Insurgency*. Warminster: Land Warfare Centre, 2009.

Great Britain. Ministry of Defence. *Global Strategic Trends – Out to 2040 (Fourth Edition).* London: Development, Concepts and Doctrine Centre, 2010.

United States. Department of Defense. *Field Manual 3-05.102—Army Special Operations Forces Intelligence.* Washington: Department of the Army, 2001.

United States. Department of Defense. *Final Report of the Independent Panel to Review DoD Detention Operations.* Arlington, VA: Department of Defense, 2004.

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

Internet

The Associated Press. "U.S. Admiral Calls for Alliance of Special Forces." Last accessed 24 February 2013. http://www.cbc.ca/news/canada/story/2013/02/23/us-special-operations-command-us.html.

Department of National Defence. "CANSOFCOM Integrated Operating Concept." Last accessed 15 January 2013. http://www.cansofcom.forces.gc.ca/gi-ig/ioc-coi-eng.asp.

Royal Canadian Mounted Police. "Integrated National Security Enforcement Teams." Last accessed 25 January 2013. http://www.rcmp-grc.gc.ca/secur/insets-eisn-eng.htm.