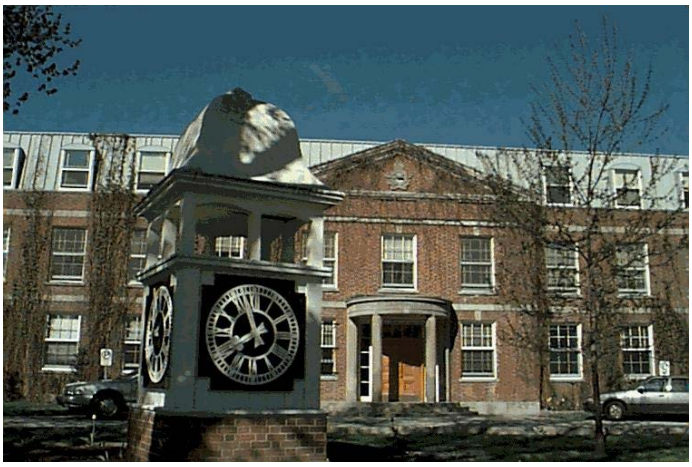
National Defence | Défense nationale

Canadian Forces College

Collège des Forces Canadiennes



# CROSSING THE RUBICON OF EVIDENCE AND INTELLIGENCE

Major C. Cotton

## JCSP 40

## 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 40

## 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 40 / PCEMI 40

MASTER OF DEFENSE STUDIES – MAÎTRISE EN ETUDES DE LA DÉFENSE

# I2: CROSSING THE RUBICON OF EVIDENCE AND INTELLIGENCE

By Major C. Cotton
Par le maj C. Cotton



Word Count: 18876

Compte de mots : 18876

## ABSTRACT

The military, like all of Canada's security agencies, is now immersed in a rapidly evolving security environment that is impacted by drastic changes in strategic expectations and technological potential. These changes, in turn, are being met by the cultural shields intrinsic to an open society that were put in place to assure the protection of individual agency against state overreach. Nowhere is this challenge more evident than in the rise of the sprawling discipline of Identity Intelligence (I2). I2 gives the military expansive collection capacity such that it is now faced with new, complex legal, ethical, philosophical and practical challenges particularly regarding its use as evidence in support to domestic security. Through the prism of the current Canadian and Allied designs, the following will argue that the military, in pursuit of comprehensive national security, can take practical steps to facilitate I2 as evidence and can do so without undermining society's official safeguards.

**TABLE OF CONTENTS**


i ……..... i

Table of Contents…… ii

List of Acronyms…… iii

Chapter 1

Primer……. 1
Aim and Methodology…… 4
Case Study……. 5
Literature Review……. 7

Chapter 2

Overview…… 11
Defining Intelligence……. 12
Defining Identity…… 15
Defining Identity Intelligence……. 17
Summary…… 21

Chapter 3

Overview…… 24
The United States Approach…….. 25
The United Kingdom Approach……. 29
The Australian Approach…… 31
Compare and Contrast…… 34
Summary…… 37

Chapter 4

Overview…… 39
The History……. 40
The Canadian Security Apparatus…….. 42
Interpretation of Existing Laws…….. 49
Military Specific Considerations…… 52
Summary…… 53

Chapter 5

Overview…… 56
Legal Risk…….. 59
Ethical Risk…… 64
Philosophical Risk……. 69
Practical Risk…… 73
Summary…… 77

Chapter 6

Review…… 79
Recommended Future Study……... 86

Bibliography…… 87

## LIST OF ACRONYMS

ii \ttorney General

AmI – Ambient Intelligence

ATA – *Anti-Terrorism Act*

ASIO – Australian Security Intelligence Organization

ASIS – Australian Security Intelligence Service

AUS – Australia

BATS – Biometrics Automated Toolset System

BEI – Biometric-Enabled Intelligence

CAF – Canadian Armed Forces

CBSA – Canadian Border Security Agency

CI – Counter-Intelligence

CIA – Central Intelligence Agency (US)

CIC – Customs and Immigration Canada

CSIS – Canadian Security Intelligence Service

CSEC – Communication Security Establishment Canada

CYINT – Cyber Intelligence

DFATD – Department of Foreign Affairs, Trade and Development

DI – Defence Intelligence

DIO – Defence Intelligence Organization (AUS)

DISG – Defense Intelligence and Security Group (AUS)

DNA - Deoxyribonucleic Acid

DND – Department of National Defense

DOMEX – Document and Media Explotation

iii Defense Signals Directorate (AUS)

FBI – Federal Bureau of Investigation

FEI – Forensic-Enabled Intelligence (US)

FININT – Financial Intelligence

FINTRAC – Financial Transactions and Reports Analysis Centre

FISA – *Foreign Intelligence and Surveillance Act* (US)

FLQ – Front de Libération du Québec

GCHQ – Government Communications Headquarters (UK)

GEOINT – Geospatial Intelligence

HUMINT – Human Intelligence

I2 – Identity Intelligence

IED – Improvised Explosive Device

IGIS – Inspector-General Intelligence Services (AUS)

INSET – Integrated National Security Enforcement Team

INSLM - Independent National Security Legislation Monitor

IRB – Immigration Review Board

IRPA – *Immigration and Refugee Protection Act*

ITAC – Integrated Terrorism Assessment Centre

JAG – Judge Advocate General

JIC – Joint Intelligence Committee

JTAC – Joint Threat Assessment Centre

MASINT – Measurements and Signatures Intelligence

MCE – Mapping and Charting Establishment

MEDINT – Medical Intelligence

iv – Minister of National Defense

MSOC – Maritime Security Operations Centre

NDA – *National Defense Act*

NSA – National Security Advisor

NTAC – National Threat Assessment Centre

ONA – Office of National Assessments (AUS)

OOTW – Operations Other Than War

OSINT – Open Source Intelligence

PCA – *Posse Comitatus Act*

PCO – Privy Council Office

RCMP – Royal Canadian Mounted Police

SIGINT – Signals Intelligence

SIRC – Security Intelligence Review Committee

SIS – Security Intelligence Service (SIS)

SME – Subject Matter Expert

SOCINT – Social and Cultural Intelligence

SS – Security Service (UK)

SOF – Special Operations Force

TCG – Tactical Coordination Group (UK)

TECHINT – Technical Intelligence

TTP – Tactics, Techniques and Procedures

## CHAPTER 1 – SETTING THE STAGE

> *Let us not deceive ourselves as to the nature of the threat that faces us; that it can be defeated easily or simply with one swift strike. We must be guided by a commitment to do what works in the long run not by what makes us feel better in the short run.*[1]
>
> - Prime Minister Jean Chretien

### PRIMER

One of the primary purposes for the creation of the state was to collectively generate security for its citizens. In recognizing this, the first line of *Securing an Open Society: Canada's National Security Policy* states, "There can be no greater role, no more important obligation for a government, than the protection and safety of its citizens."[2] One of the main challenges arising from this obligation, particularly in the modern social democratic state, is the tension inherent in the respect for a citizen's agency, and by extension privacy, with need for the state to generate information concerning both citizens and non-citizens such that it can best protect itself. The tension is reflected most acutely, in the post 9/11 environment, with the emergence of such legal instruments as surveillance and detention without declared foundation and the exponential growth of state intelligence agencies. This expansion of state security powers has been in parallel with the explosive evolution of technology that further enables state's capacity to collect information.

Nowhere is this tension more evident than in the state's division between evidence and intelligence. As described by American academics Gary Cordner and Kathryn Scarborough in their article 'Information Sharing: Exploring the Intersection of Policing with National and Military Intelligence' which states that, "the complexity of the inter-organizational environment

---

[1] Jean Chretien (Address by the Prime Minister on the occasion of a Special House of Commons Debate in response to 9/11, Ottawa, September 17, 2001).

[2] Canada. Public Safety Canada, *Securing an Open Society: Canada's National Security Policy* (Ottawa: Government of Canada, 2004), vii.

of law enforcement-related and homeland security-related information sharing is daunting…"[3] Evidence, by design, is meant to be transparent and respect for its writ inside a state's laws, is meant as a check against a state's power to prosecute without cause. Traditionally, it is the responsibility of law enforcement. Intelligence, on the other hand, is broader in scope and is meant to advise policy decisions rather than affirm law. Opaque by nature, it can be collected by all agencies of government in pursuit of both foreign and domestic interests.

Another pressure that arises in the dichotomies of state security is the conscious schism between a state's obligations to its citizens and its treatment of non-citizens. The foundational principles found in such instruments as the Canadian *Charter of Rights and Freedoms* or the American *Constitution*, reinforced by legislation governing privacy and intelligence collection, are the buttresses against omnipotent internal state power. However, in our present Westphalian system wherein states are the highest degree of independent executive authority, these defenses do not extend beyond individual borders and thus do not necessarily restrict a state's ability to treat non-citizens in other countries as different from its own.[4] This, in turn, allows a state a degree of flexibility in foreign intelligence collection and control of who may enter boundaries. As asserted by University of Toronto Professor Audrey Macklin,

> Geo-political borders serve many functions in public consciousness, both literal and symbolic; they demarcate the nation-state's essential territoriality, they assert and exert sovereignty; and finally, their selective permeability operates as a measure of the nation-state's security against external threat…[5]

---

[3] Cordner, Gary and Kathryn Scarborough, 'Information Sharing: Exploring the Intersection of Policing with National and Military Intelligence,' In *Homeland Security Affairs* Volume VI, no. 1 (January 2010): 15.

[4] However, a state may impose guiding principles upon its treatment of non-citizens when they are within a state's borders i.e. the *Canadian Charter of Rights and Freedoms* applies to visitors to Canada from the moment they arrive on Canadian soil.

The military, as one of the pillars of state security, has customarily been in the business of collecting intelligence rather than evidence. This is partly due the fact that unlike law enforcement operations, military operations were not a contest of individuals but capabilities and partly to the fact that, when unleashed, it did not have the time necessary for the detailed work of evidence gathering.[6] Additionally, due to a state's uneasiness with the use of the military in a law enforcement role, the conventional military has shied away from assuming any domestic, law enforcement responsibilities. Moreover, as the military is usually a tool for foreign policy and thus in the business of foreign intelligence, it was not historically held to the exacting requirements necessary for evidence collection. However, as stated by University of New Jersey Graduate Student Louise Stanton, the dynamic has altered and state strategy now relies on "the integration of civilian and military activities in a unity of [intelligence] effort."[7]

In particular, the alteration of this shibboleth is highlighted in the arrival of a new discipline known as Identity Intelligence (I2). An immensely powerful tool that is enabled by recent advancements in technological and analytical means, I2 is fundamentally changing the dynamic of military intelligence and evidence. It is giving the military the capacity to collect detailed information of an evidentiary nature hitherto denied it in the past thus putting the military squarely in the evidence versus intelligence debate in ways that the state never had to previously resolve. Though historic examples exist such as the use of military enabled evidence

---

[5] Audrey Macklin, "Borderline Security in Essays on Canada's Anti-Terrorism Bill," in *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*, ed. R.J. Daniels, P. Macklem and K. Roach, 383 (Toronto:University of Toronto Press, 2001).

[6] This, of course, does not include the very robust nature of the military police system who have the mandate to investigate and prosecute military members.

[7] Louise Stanton, "The Civilian-Military Divide: Obstacles to the Integration of Intelligence in the United States," Doctoral Thesis, State University of New Jersey, 2007), 7.

in the post-World War II Nuremburg trials and more recently during the *International Criminal Tribunal for the former Yugoslavia*, these are exceptions and represent the historical rather than the immediate forensic sphere of modern evidence.

## AIM AND METHODOLOGY

The following will be an in-depth exploration of the emergence of I2 and its implications on the future of military operations and responsibilities. In addition, using the prisms of current Allied and Canadian security apparatus, it will highlight the associated risks and substantiate the necessary steps that the Canadian state must take to legally permit this divide to be crossed in an efficient but plainly visible manner. By doing so, it will thus demonstrate that the importance of military enabled I2 in state security trumps the state's present aversions to sharing I2 as evidence.

Chapter 2 – *Identity Intelligence Defined*, will explore the component parts of intelligence and identity and their merger into this new and potent intelligence discipline. Chapter 3 – *The Allied Approaches* will compare and contrast relevant elements that enable and guide state security for our primary allies; the United States (US), the United Kingdom (UK) and Australia. It will draw out several key examples and structures that Canada can use as it seeks the appropriate balance between military intelligence and evidence. Chapter 4 – *The Canadian Approach* will investigate the restrictions and mechanisms for multi-agency information sharing to better understand the present form of Canadian state security and the associated legal parameters. Chapter 5 – *Risks and Remedies*, will study the four main hurdles that seemingly restrict this exchange of military enabled I2 as evidence: legal, ethical, philosophical and practical. It will also present several practical solutions to overcoming or mitigating these

apparent risks. Chapter 6 – *Conclusion*, will summarize this exploration as well as conclude with several recommendations for the Canadian state as it deliberates the role of I2 in the architecture of state security. It will also provide technological and training recommendations for future study.

## CASE STUDY – WHY I2 AS EVIDENCE?

In order to better understand the current environment and why it is important that Canada gets this right, the following hypothetical case study presents a short but realistic example of where I2 can play a role in domestic security. It highlights a situation that, if presented to the Canadian public, would appear reasonable and practical. The fact is that without changes in law, awareness and mechanisms for inter-agency information sharing, it cannot now happen.

*Future Area of Operation – July 2015*

Canada has been invited by a host nation government to assist in quelling internal unrest. A patrol is the victim of an Improvised Explosive Device (IED). Surviving soldiers quickly secure the area and, sensitive to their training that in the absence of direct threat this has become a crime scene, set up a cordon. They invite all locals still at the scene to submit to collection of fingerprints and facial scans which has been authorized by the local government. A Counter-IED Team is dispatched to assure that the location is safe and to collect information for future analysis. As part of their investigation, they find a second IED. Trained by the RCMP to the standards obligated by the *Canada Evidence Act*, the team carefully collects the component parts of the second device, bagging and tagging them accordingly. These parts are subsequently

returned, complete with all necessary paperwork to respect 'chain of evidence,' to the Task Force Level II Forensics Laboratory.

The laboratory personnel, also trained by the RCMP, have put in place a process that respects all evidentiary norms. This includes having their Commander declared as a Subject Matter Expert (SME) such that he would be accepted by a court of law if called upon to present any of the its findings. As part of their analysis, they pull a set of fingerprints from the device. These fingerprints are entered into a database, also to evidentiary standards, that permits no subsequent alternations. They are clearly caveated as collected on behalf of the Canadian state. The fingerprints become part of a case file that describes the incident and gives all the necessary contact information for follow-up. As there is no immediate connection made to a known individual, the file sits in the database unsolved but not forgotten.

The case file is honest to the Canadian Border Security Agency (CBSA)'s lookout information form that is the comprehensive tool used to inform their agents. The database, respecting strict guidelines on access, is shared with all of Canada's security agencies. Luckily, the fingerprints are clear enough that they can be compared against the information collected as part of Customs and Immigration Canada (CIC)'s *Temporary Resident Program* that, as of 2013, obligated all persons applying for a visa to submit biometric information.

*CBSA Border Control Kiosk, Ottawa – July 2020*

One individual, from the disputed region, has submitted a Canadian visa application complete with the necessary biometric information. After a positive connection is made inside the database between the fingerprints taken from the 2015 IED and those on the visa application, CIC flags his application as a concern and forwards it to CBSA. CBSA detains the individual

upon arrival using this positive connection. As the 'chain of evidence' is unbroken and the expertise of the military agents in the chain is respected, the Immigration and Refugee Board of Canada denies entry and any subsequent remedy to the individual. Based on this element of I2, he is returned to his home country to face possible prosecution.

## LITERATURE REVIEW

This thesis is persuasive and relies upon an existing literature review. It pulls from domestic and foreign sources, both from within and without government, that include legislation, doctrine and studied analysis. It covers topics such as identity, intelligence, I2, foreign state security instruments, concept of privacy and Canadian law. Though premised around the military much of the scrutiny and subsequent recommendations are equally applicable to associated information sharing and privacy concerns of other state security agencies.

Chapter 2 – *Identity Intelligence Defined*, draws mainly governmental and academic sources in order to best understand the contemporary definitions of identity and intelligence. Literature relating to intelligence and identity separately is very comprehensive as reflected in the expansive doctrine, philosophy and research available. However, literature specifically related to I2 as its own concept is less mature. There is some study of its impact in commercial spheres such as that found in Cristian Morosan's "Biometric Solutions for Today's Travel Security Problems" however it is focused mainly on identity as a means of authentication only. Of note, in security circles, only the US military as reflected in its Joint Publication 2.0 *Joint Intelligence* has formally captured I2 as its own discipline. Other sources make tangential but associated reference such as the description of the closely aligned Criminal Intelligence in Peter Gill's 'Making Sense of Police Intelligence?', the blossoming study of Ambient Intelligence

found in Philip Brey's "Freedom and Privacy in Ambient Intelligence" or the review of biometrics found in Anthony Iasso's "A Critical Time for Biometrics and Identity Intelligence."

For Chapter 3 – *The Allied Approach*, the preponderance of available information stems from US sources however there is also respectable UK and Australian literature. It mainly draws from existing US, UK and Australian legislation that governs their respective state security apparatus. This includes study of such instruments as the *USA PATRIOT Act*, the UK's *Terrorism Act 2000* and Australia's *Anti-Terrorism Act*. It also pulls from existing governmental and academic literature that has studied their respective approaches including British Professor Julian Richard's *A Guide to National Security: Threats, Responses & Strategies* and American Foreign Policy Professor Dr. Charles Stevenson's *America's Foreign Policy Toolkit: Key Institutions and Processes*. Of note, particular attention has been paid to law student Cedric Logan's article, 'The FISA Wall and Federal Investigations,' American graduate student, Nathan Sales' "Mending Walls: Information Sharing After the USA PATRIOT Act,' British academic Stevyn Gibson's 'Future roles of the UK Intelligence System' and Australian Professor George William's article 'A Decade of Australian Anti-Terror Laws.'

Chapter 4 – *The Canadian Approach* also draws mainly from the existing Canadian legislation policy that governs Canadian state security. Though not as broad as that found for the US or the UK, it is nevertheless quite comprehensive and nuanced. Two leading Canadian proponents in this field are University of Toronto Professors Kent Roach and Wesley Wark. Dr. Roach is a law professor and is focused on the evolution of the legislative response primarily as it pertains to the Criminal Code. Though his work is found in many places in the international academia, his perspectives can be found in his books *The 9/11 Effect: Comparative Counter-Terrorism* and *September 11: Consequences for Canada*. Dr. Wark is a history professor and is

focused on the particular intelligence elements that must be accounted for inside the legislative response. His perspectives can be found in the edited books *Twenty-First Century Intelligence* and *Essays on Canada's Anti-Terrorism Bill*. An alternate authority is the once Attorney General Irwin Cotler who was instrumental in the drafting of Canada's post 9/11 'human security' legislation. His perspective can be found in his article, "Thinking Outside the Box: Foundational Principles for a Counter-Terrorism Law and Policy.' This chapter also draws from such seminal analysis done on state interagency, information sharing such as the 1981 *Royal Commission of Inquiry into Certain Activities of the RCMP* and the 2010 *Report of the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.* From a military perspective, it draws upon academic literature such as retired Brigadier General James Cox's exhaustive doctoral thesis *Lighting the Shadows: An Evaluation of Theory and Practice in Canadian Defense Intelligence.*

The sources for Chapter 5 – *Risks and Remedies* are rich and various and draw namely from both academic and professional sources. The preponderance of the literature is focused on finding the equilibrium between privacy and the state's ability to demonstrate efficient security. However, much of it focuses on the use of identity as an internal means of security. For instance, *The Privacy Card: A Low Cost Strategy to Combat Terrorism* by Professor Joseph Eaton speaks to the case for a national ID card. Canadian specific examination, aside from some speaking to the RCMP/CSIS divide, has very little to yet say on the use of military intelligence as domestic evidence. The edited *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*, by Canadian Professors Colin Bennett and David Lyon, does contrast some, related Canadian issues with those of other countries namely UK and Australia. From a military perspective, the US Army is the leading proponent and its *Army Biometric Applications:*

*Identifying and Addressing Sociocultural Concerns* discusses and addresses the universal issues of collecting and sharing biometric information.

## CHAPTER 2
## IDENTITY INTELLIGENCE DEFINED

> *And therefore only the enlightened sovereign and the worthy general who are able to use the most intelligent people as agents are certain to achieve great things. Secret operations are essential in war; upon them the army relies to make its every move.* [8]
>
> - Sun Tzu

### OVERVIEW

Identity Intelligence (I2) is an emerging intelligence discipline that results from the analysis of material from a variety of sources including but not limited to Human Intelligence (HUMINT), Signals Intelligence (SIGINT), Technical Intelligence (TECHINT), Measurements and Signature Intelligence (MASINT), Financial Intelligence (FININT) and the developing fields of Cyber and Ambient Intelligence. Its evolution stems from a state's increased need to identify and authenticate individuals and whether the driving force is "immigration control, anti-terrorism, electronic government or rising rates of identity theft," I2 is now being debated and matured in many countries.[9] In order to best understand I2, it must be translated through the contextual norms of its component parts; identity and intelligence.

In a speech given in 1991, US President George H. Bush envisioned its importance asserting that intelligence "is and always will be our first line of defense, enabling us to ward off emerging threats whenever possible before any damage is done."[10] Intelligence constitutes a contiguous family of objective terms and definitions and can best understood as the sum of its component families that include strategic, security, foreign, defense, criminal and economic

---

[8] Sun Tzu, *The Art of War*, ed. Samuel Griffith, 122 (Oxford: Oxford University Press, 1963), 149.

[9] David Lyon and Colin J. Bennett, "Playing the ID Card: Understanding the Significance of Identity Card Systems," in *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*, ed. Colin J. Bennett and David Lyon (London: Routledge Taylor & Francis Group, 2008), 3.

[10] George W. Bush (Speech quoted in David Alex Mastero II**,** "Cognitions of the Community: The Worldview of U.S. Intelligence" (Doctoral Thesis, West Virginia University, 2008), 1).

intelligence. Intelligence can also be divided into three segments along an ideally integrated continuum: an organization, a process and a product.

In comparison to intelligence, identity is both more and less subjected to overarching terms. The Canadian federal interdepartmental working group that studied the contentious National ID Card defined it as "a reference or designation used to distinguish a unique and particular individual."[11] At its essence, it is that which can be used to distinguish you as you. Normatively, it accounts for your cultural or societal identifiers whereas factually it accounts for your unchanging biological characteristics.

Taken together, I2 can be considered both a product and a process with the operationally useful characteristics of universality, uniqueness, measurability, longevity and neutrality.[12] It is the continuously evolving montage that can be used to filter, track, recognize and isolate an individual. It is a very powerful tool that, when applied, can pull a person out of the protective comfort of a crowd by making "nearly instantaneous verifications of claimed identity."[13]

**DEFINING INTELLIGENCE**

The Canadian Security Intelligence Service (CSIS) asserts that "intelligence conveys the story behind the story."[14] Like terrorism, it refuses to isolate itself inside one, fully inclusive universal definition. Depending on country or organization, intelligence can be raw data or

---

[11] Andrew Clement, Krista Boa, Simon Davies and Gus Hosein, "Towards a National ID Card for Canada? External Drivers and Internal Complexities" in *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*, ed. Colin J. Bennett and David Lyon (London: Routledge Taylor & Francis Group, 2008), 242.

[12] Joseph W. Eaton, *The Privacy Card: A Low Cost Strategy to Combat Terrorism* (New York: Rowman & Littlefield Publishers, Inc, 2003) xxiii.

[13] John D. Woodward, Katharine Webb, Elain Newton, Melissa Bradley and David Rubenson, *Army Biometrics Applications: Identifying and Addressing Sociocultural Concerns* (Pittsburgh: Rand, 2001) 2.

[14] Canadian Security Intelligence Agency, "What is Security Intelligence?," Last accessed 14 April 2014, https://www.csis-scrs.gc.ca/bts/fq-eng.asp#bm12.

completed analysis, it can be an activity, a report or an establishment, it can influence strategic policy or it can drive tactical decisions. Sherman Kent, an American academic and wartime intelligence specialist with the Central Intelligence Agency (CIA) described it as, "a particular kind of knowledge, the activity of obtaining such knowledge and the organization whose function is to acquire and utilize it."[15] The Department of National Defense (DND), via its Canadian Armed Forces (CAF) Joint Publication 2.0 *Intelligence*, takes this further stating that it is,

> the product resulting from the collection, processing, analysis, integration and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or the geography and the culture that contributes to the understanding of an actual or potential operations environment. The term is also applied to the process and activity which results in the product and to the organizations dedicated to such activity. [16]

However, intelligence must also inform decisions to be truly effective. Michael Herman, former chairman of the British joint intelligence committee asserted that intelligence, "is produced to influence government action." [17] Stuart Farson, a Canadian political science professor, echoes this stating that "the ultimate purpose of intelligence is to provide information that helps decision-makers make better policy choices."[18]

The intelligence family is made of up six general sub-families; strategic, foreign, security, defense, economic and criminal. Strategic Intelligence is that required for the

---

[15] Sherman Kent, Quoted in Bryce Offenberger, "The Way Forward: Reforming Canada's Foreign Intelligence Community," (Master's Thesis, University of Manitoba, 2012), 5.

[16] Canada, *Canadian Forces Joint Publication 2.0 Intelligence* (Ottawa: Department of National Defense, 2011), GL-7. This definition is very similar but slightly more holistic to that of NATO in that it includes analysis, integration and interpretation of information rather than strictly processing.

[17] Brad Cartier, "Certainty through Flexibility: Intelligence and Paramilitarization in Canadian Public Order Policing," (Doctoral Thesis, University of Ottawa, 2012), 7.

[18] Paul Robison, "The Viability of Canadian Foreign Intelligence," in International Journal (Summer 2009), 704.

formulation of policy whether at the national or international levels. Foreign Intelligence is collected to safeguard national interests and concerns, "the plans, capabilities, activities, or intentions of foreign states, organizations, or individuals."[19] The purpose of Defense Intelligence, which includes but is not limited to military intelligence, is "to achieve information superiority for the armed forces it serves" where in it provides decision makers with intelligence which allows for "the development of defense policies and plans, and the conduct of operations."[20] Economic Intelligence is the "monitoring and surveillance of commercial activity."[21] Criminal Intelligence is that which "supports decision making in the areas of law enforcement, crime reduction, and crime prevention."[22] Alternatively, Security Intelligence must have a direct threat component and results from,

> the collection, collation, evaluation and analysis of information regarding security threats. It provides government decision-makers with insight into activities and trends at national and international levels that can have an impact on [security].[23]

Serving each of these families are the seven traditional disciplines of intelligence; SIGINT, HUMINT, TECHINT, MASINT, Open Source Intelligence (OSINT), Geospatial Intelligence (GEOINT) and Counter-Intelligence (CI). SIGINT is that taken from the electro-magnetic spectrum and is primarily that of communications. HUMINT is that derived directly from human sources and may include media and document exploitation (DOMEX). TECHINT studies the practical applications of foreign technology. MASINT is the study of data obtained

---

[19] Barry Cooper, *CFIS: A Foreign Intelligence Service for Canada*, (Calgary: Canadian Defence and Foreign Affairs Institute, 2007), iv.

[20] Canada, *Canadian Forces Joint Publication 2.0 Intelligence* …2-4; and, Martin Rudner, "The Future of Canada's Defense Intelligence," in *International Journal of Intelligence and Counter-Intelligence* (2002), 542.

[21] Cooper, *CFIS: A Foreign Intelligence Service for Canada...* 51.

[22] Jerry Radcliffe, *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders, 2nd Edition* (Washington: US Department of Justice, 2007), 8.

[23] Canadian Security Intelligence Service, "What is Security Intelligence?" Last accessed 14 April 2014, https://www.csis-scrs.gc.ca/bts/fq-eng.asp#bm12.

from sensing instruments and the subsequent identification of unique identifiers. OSINT is that which is publically available such as TV or newspapers. GEOINT is that derived from, "topographical, imagery, geospatial, meteorological, and oceanographic information."[24] Finally, CI is the defense to the other six and is the mitigation of the threat posed by hostile intelligence services.

Other less traditional disciplines include Medical Intelligence (MEDINT) and Social and Cultural Intelligence (SOCINT). Emerging disciplines include Cyber-Intelligence (CYBINT), Ambient Intelligence (AmI) and, for the purposes of this discussion, I2. [25]

**DEFINING IDENTITY**

The complex and ever-changing topic of identity has been long debated in philosophy, psychology and sociology. Our current understanding is grounded in the seminal work of Aristotle, John Locke, Isaiah Berlin, Michel Foucault and Sigmund Freud. Foucault, in particular, is enlightening with his concept of identity as translated by *apparatus* or anything that has "the capacity to capture, orient, determine, intercept, model, control, or secure the gestures, behaviors, opinions, or discourses of living beings."[26] It can be further understood by French philosopher Paul Ricoeur's distinction between *idem-identity* or the relationary concept of What I Am and *ipse-identity* or the reflextionary concept of Who I Am. [27] Simply, identity is "a person's uniqueness as well as his or her similarity in relation to time or to others." [28]

---

[24] Canada, *Canadian Forces Joint Publication 2.0 Intelligence*…2-7.

[25] The US Joint Publication 2.0 *Joint Intelligence*, released in October 2013, has for the first time recognized Identity Intelligence as one of eight categories of intelligence production. Also included on the list are General Military Intelligence, Science&Technology Intelligence and Counter-Intelligence.

[26] Katja de Vries, "Identity, Profiling Algorithms and a World of Ambient Intelligence," in *Ethics and Information Technology* (Springer Science+Business Media, 2010), 73.

With this in mind, individual identity is composed of two components: personal identity and social identity. A personal identity is, "one's self-perception as an individual" and though subject to variance, is typically persistent. [29] It assumes that an individual can be identified as the same person at different instances in time. [30] It includes personal information given at birth (name), personal identifiers (social insurance number), physical descriptors (height, weight, eye color) and biometric information (DNA, fingerprints). [31] Social identity, on the other hand, is, "one's biographical history that builds up over time" and is a reflection of how an individual interacts with their society.[32] It has both the psychological element of self-identity as part of certain social groups and the sociological element of self-identity as inter-relational roles. When the two are integrated, social identity is a "a multi-level concept that involves understanding one's social groups at various scales."[33]

Together, personal and social identity, in the words of University of Illinois doctoral student Alice Filmer, have maintained a "dialectic between the culturalist emphasis on consciousness and the structuralist insistence on external conditions" in discussion of human agency. [34] However, for the purpose of this discussion, identity is more than just an existential reflection on self. In law, it is also used as a shibboleth or a device used to "decide who is in and

---

[27] Ibid, 74. *Idem-identity (*sameness or meˆmete´) is your identification in relation to others or as part of a group such as "I am a heterosexual, white, Catholic, Canadian" whereas *Ipse-identity* (selfhood or ipseity) is your individual grounding of self in time and place such as "What is it to be a heterosexual, white, Catholic, Canadian right now." *Ipse-identity* is thus the unique, individual experience of *idem-identity*.

[28] De Vries "Identity, Profiling Algorithms and a World of Ambient Intelligence"…74.

[29] Jiexun Li G. Alan Wang and Hsinchun Chen, "Identity Matching Using Personal and Social Identity Features," in *Information Systems Front* (Springer Science+Business Media, 2010), 2.

[30] Niels van Dijk, "Property, Privacy and Personhood in a World of Ambient Intelligence" in *Ethics Information Technology* (Springer Science+Business Media, 2009), 57.

[31] De Vries "Identity, Profiling Algorithms and a World of Ambient Intelligence"…73.

[32] Li,Wang and Chen, "Identity Matching Using Personal and Social Identity Features"…2.

[33] Ibid.

[34] Alice Filmer, "The Acoustics of Identity: Linguistic Passports Beyond Empire and Essentialism," (Doctoral Dissertation, University of Illinos, 2008), 13.

who is out; who is us and who is them; who is likely to be a good customer and who is not; who is allowed to pass the border and who is not."[35] This shibboleth can be served by I2.

**DEFINING IDENTITY INTELLIGENCE**

I2, at its essence, is the ability to verify "actual true identity" and provides a method of authentication as it is "based on something you are that cannot be lost or forgotten." [36] The US Joint Publication 2.0 *Joint Intelligence* defines I2 as intelligence resulting from, "the processing of identity attributes concerning individuals, groups, networks, or populations of interest."[37] It results from the holistic fusion of reputational, behavorial, biographic and or biologic identity features with any other associated information and results in "discovery of true identities, links identities to events, locations and networks, and reveals hostile intent."[38]

I2 is enabled by activities that are resident in all the other intelligence disciplines including HUMINT, MASINT, SIGINT, OSINT and TECHINT. It may also pull from FININT, CYBINT and AmI.[39] Its fundamental applications include biometric-enabled intelligence (BEI), forensic enabled intelligence (FEI) and document and media exploitation (DOMEX).

The present lodestone enabler to I2 is BEI. Biometrics is a term derived from the Greek words *bio* (life) and *metric* (to measure) and they are "unique human characteristics that rarely or never change." [40] CAF Joint Publication 2.0 *Intelligence* defines biometric intelligence as that, "derived from the exploitation of measurable anatomical, physiological, and behavioral

---

[35] De Vries "Identity, Profiling Algorithms and a World of Ambient Intelligence"…76.

[36] Li,Wang and Chen, "Identity Matching Using Personal and Social Identity Features"…1; and, Abhishek Nagar, "Biometric Template Security," (Doctoral Dissertation, Michigan State University, 2012), 3.

[37] United States, *US Joint Publication 2.0 Joint Intelligence* (Washington: US Joint Chiefs of Staff, 2013), GL-8.

[38] Ibid, B-9.

[39] Ibid, I-20.

[40]Cristian Morosan, "Biometric Solutions for Today's Travel Security Problems," in *Journal of Hospitality and Tourism Technology* Vol.3 No. 3 (2012), 178.

characteristics of human beings."[41] The current literature reflects the measurement of only two types of intrinsic characteristics: physiological and behavioral. Physiological traits are those less controllable by owners and include DNA, fingerprint, face, retina, iris, hand geometry, vein pattern, earlobe, and even odor.[42] Behavioral traits are those more controllable by its practitioners and includes voice, keystroke dynamics, signature pattern, handwriting and gait analysis.[43] By distinguishing based on innate attributes, it proposes a "natural and dependable solution to the difficulty of identity determination."[44]

The next application, the logical extension of BEI, is FEI. Forensic derives itself from the Latin *forēnsis*, meaning "of or before the forum." [45] It captures the modern intersection of law with science and according to the Online Merriam-Webster Dictionary, it means "relating to or dealing with the application of scientific knowledge to legal problems."[46] Taking this further, according to the US Joint Publication 2.0 *Intelligence*, FEI is that resulting from the integration of,

> scientifically examined materials and other information to establish full characterization, attribution, and the linkage of events, locations, items, signatures, nefarious intent, and persons of interest.[47]

The collection and study of biometric information as part of FEI is most critical to this debate as it can establish the bridge between an individual and their historic actions.

DOMEX is the "exploitation of captured enemy paper documents such as publications,

---

[41] Canada, *Canadian Forces Joint Publication 2.0 Intelligence*…2-7.
[42] Morosan, "Biometric Solutions for Today's Travel Security Problems"…178.
[43] Ibid.
[44] Cindy H. Dubin,"Biometrics Hands Down" in *Security Magazine* (February 2011), 54.
[45] Merriam-Webster Online Dictionary, "Forensic," Last accessed 16 April 14) http://www merriam-webster.com/dictionary/forensic. This is a legal reference to the Roman use of the forum as the main platform for its legal system.
[46] Ibid.
[47] United States, *US Joint Publication 2.0 Joint Intelligence* …GL-7.

marked maps, overlays, and other media capable of storing information."[48] As US Colonel J. Cox recently stated, DOMEX is a reflection of the growing "avalanche of harvested digital media that create a national security issue which merits a system that can reliably sift intelligence and quickly share it."[49] It is important because it may reveal such valuable information as plans, locations, capabilities or status. Though historically considered part of HUMINT with elements of TECHINT, the US Intelligence community has now situated it as an I2 application.[50]

FININT has its origins in the study of money laundering but it is the pursuit of post 9/11 terrorism financing that has brought it forward as an important intelligence discipline. It is responsible for,

> receiving (and, as permitted requesting), analyzing and disseminating to the competent authorities, disclosures of financial information: concerning suspected proceeds of crime and potential financing of terrorism.[51]

FINTRAC, Canada's federal FININT unit, must help "protect the integrity of Canada's financial system through the detection and deterrence of money laundering and terrorist financing."[52] It has a tangential connection to I2 as the study of individual financial transaction records can reveal behavioral traits that can assist in revealing true identity.[53]

---

[48] Canada, *Canadian Forces Joint Publication 2.0 Intelligence*…2-7.

[49] Joseph Cox, "DOMEX: The Birth of a New Intelligence Discipline," in *Military Intelligence* (April – June 2010), 22.

[50] The Canadian Intelligence Community, as demonstrated in the CAF Joint Publication 2.0 Intelligence, has it under HUMINT.

[51] Milind Sathye and Chris Patel, "Developing Financial Intelligence: An Assessment of the FIUs in Australia and India" in *Journal of Money Laundering Control* Vol. 10 No. 4 (2007), 391.

[52] Financial Transactions and Reports Analysis Centre of Canada, "Our Mandate," Last accessed 16 April 2014, http://www fintrac-canafe.gc.ca/fintrac-canafe/1-eng.asp.

[53] FININT is not practiced directly by the military and must be sought from other sources

Arising from the recognition of cyberspace as another operational environment, cyber-intelligence is one of four critical new cyber related defense activities. [54] However, though there are now some tentative references to CYBINT, it is still immature as a standalone discipline. The closest definition is that used in US Airforce doctrine of, "capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[55] It can be an authoritative I2 source on behavioral identity because it "collects information about people's searching and shopping habits, and this information can generate a detailed picture about that individual." [56]

AmI is emerging due to the almost universal interconnectedness of technology, primarily the internet. It arises from the artificial creation of "a world of traces beyond the individual life with which one identifies."[57] As stated by European Researchers David Wright, Serge Gutwirth and Michael Friedewald in their article, *Shining Light on the Dark Side of Ambient Intelligence*, people are surrounded by,

> easy-to-use interfaces embedded in all kinds of objects and by an everyday environment capable of recognizing and responding to individuals in a seamless, unobtrusive and invisible way.[58]

It is reflected in the Bayesian Logic algorithms built into such common applications as Google wherein probability values are repeatedly weighted and re-calculated in order to better

---

[54] Canada, *Canadian Forces Joint Publication 2.0 Intelligence*…4-4. The other four are cyber-analytics, cyber-forensics, cyber-logistics and cyber-security.

[55] Matthew Hurley, "For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance," in *Air & Space Power Journal (November – December 2012),* 14.

[56] Robert Ackerman, "Cyber Tasks Intelligence Community," in *Signal* (March 2010), 30.

[57] De Vries "Identity, Profiling Algorithms and a World of Ambient Intelligence"…79.

[58] David Wright, Serge Gutwirth and Michael Friedewald, "Shining Light on the Dark Side of Ambient Intelligence," in *Foresight* Vol. 9 No. 2 (2007), 46.

reflect or even project probable desires.[59] AmI is important to I2 because its goal is to become so pervasive as to be unnoticed but so powerful that it would capture elemental segments of individual identity. If tapped, AmI can provide a formidable echo of a person's true identity going so far as to acquire "a better understanding of people than people have themselves." [60]

**SUMMARY**

In summary, I2 is an emerging and authoritative intelligence discipline that is informed by elements drawn from across the traditional spectrum that includes security, defense, criminal, economic and strategic intelligence. When defined via its component parts of identity and intelligence, it reveals a nuanced but wide ranging characterization. Canadian graduate student Bryce Offenberger in his thesis *The Way Forward: Reforming Canada's Foreign Intelligence Community*, claimed that intelligence was "the activity of obtaining and processing […] knowledge and the specific organizations involved." [61] Retired Canadian Brigadier-General James Cox promoted the notion that intelligence is not just information but also "using that information to make decisions about future advantageous action."[62] It, as an organization, a process and a product, must encompass considered analysis and, in turn, inform decisions.

Identity is the delineation of an individual containing the exactness necessary to isolate a person as who they claim to be. It denotes both "a person's uniqueness as well as his or her

---

[59] For instance, an AI capable coffee machine, based on your use to date, would independently process a best guess as to the size, temperature, mixture and time you would like your coffee such that it would have it ready before you even thinking about it.

[60] Philip Brey, "Freedom and Privacy in Ambient Intelligence," in *Ethics and Information Technology* (Springer Science+Business Media, 2006), 162. The military's current connection comes through its nexus with cyber-intelligence.

[61] Bryce Offenberger, "The Way Forward: Reforming Canada's Foreign Intelligence Community," (Master's Thesis, University of Manitoba, 2012),7.

[62] James Cox, "Lighting the Shadows: An Evaluation of Theory and Practise in Canadian Defence Intelligence," (Doctoral Dissertation, Royal Military College of Canada, 2011), 4.

similarity in relation to time or to others."[63] It has psychological, biological, personal, sociological and behavioral components that, when amalgamated can provide a very effective means of clearly distinguishing one person from another.

United, I2 translates source material from HUMINT, TECHINT, OSINT, SIGINT, CYBINT and AmI, via its main applications of BEX, FEX and DOCEX, to authenticate and possibly isolate individuals. Its ability to verify persons as who they are can establish "an individual's identity with certitude and [link] the individual to past aliases or activities."[64] When analyzed and captured inside apparatus that can, in turn, be used by national security agents, it becomes a powerful tool in a state's protection against terrorism, false immigration and identity fraud. As articulated by leading US Intelligence Consultant Booz Allen Hamilton, I2 can answer such questions as,

> Can a person be matched to a place, activity, or device? Can a face in the crowd be linked to other intelligence information? Can persons, objects, or other entities be linked? Is the presence of multiple people in the same location an event of interest? Can movement patterns by anticipated and exploited? Can we predict the intent of a person or organization? How does biometric and identity intelligence impact our strategic execution? [65]

Harry Howe Ransom, a former member of the CIA and leading authority on the American intelligence community called for students of intelligence 'to know more about knowledge and power, information and actions.'[66] The study of I2 indicates that it is a rising but

---

[63] De Vries "Identity, Profiling Algorithms and a World of Ambient Intelligence"…73.

[64] Anthony Iasso, "A Critical Time for Biometrics and Identity Intelligence," in *Military Intelligence* (July – September 2013), 39.

[65] Booz Allen Hamilton, "Identity Biometric Enabled Intelligence," Last accessed 23 April 2014, https://www.boozallen.com/consulting/technology/cyber-security/identity/identity-biometric-enabled-intelligence.

[66] Harry Howe Ransom, Quoted in Peter Gill, "Making Sense of Police Intelligence? The Use of a Cybernetic Model in Analyzing Information and Power in Police Intelligence Processes" in *Policing and Society: An International Journal of Research and Policy* Vol. 8 (1998), 303.

relevant instrument in state security. However, it comes with institutional anxiety particularly that surrounding potential legal complications in its use as a discriminatory device or shibboleth. The next two chapters, Chapter 3 – *The Allied Approach* and Chapter 4 – *The Canadian Approach*, will explore further the associated laws and structures within Canada and its Allies, in particular, the mechanisms for the legal sharing of I2 amongst security agencies.

## CHAPTER 3
## THE ALLIED APPROACHES

*Every minutia should have a place in our collection, for things of a seemingly trifling nature when conjoined with others of a more serious cast may lead to very valuable conclusions.*[67]

– General George Washington

### OVERVIEW

To better understand the legal and structural environment surrounding Canada's pan-government information sharing, a comparison with germane national security elements of its three closest allies: the United States (US); the United Kingdom (UK); and Australia, is in order. Aside from shared history and language, this comparison is cogent due to similar values regarding privacy, the sovereignty of the individual and the role of the state. In addition, this comparison is made easier due to the shared underpinning of common law legal systems.[68] Rather than focus on I2 specifically, the contrast will instead be broad and encompass pertinent parts of the nations' existing instruments for sharing information amongst agencies.

The US, it appears at first with its *USA PATRIOT Act*, has the most robust existing mechanism for sharing information amongst its security agencies. However, it has four legal traps that act as a barriers to universal disclosure; pretext, firewall, republican and privacy.[69] The UK with a long history of managing both domestic and foreign terrorist threats seems to be the most comfortable with pan-government intelligence distribution. Nevertheless, it has in place robust legislative protections as well as tactical and strategic nodes for interagency information

---

[67] George Washington, Quoted in Nathan Sales, "Mending Walls: Information Sharing After the USA PATRIOT Act" in *Texas Law Review* (July 2010), 1852.

[68] Common law is based on the simple premise that it is unfair to treat similar facts differently on different occasions. This premise is then translated through case or *stare decisis* law that obligates judgment to be made that is genuine to previous judgments on the same issue. Case law is reinforced, codified or made whole by legislation.

[69] USA PATRIOT Act stands for ***U****niting and* ***S****trengthening* ***A****merica by* ***P****roviding* ***A****ppropriate* ***T****ools* ***R****equired to* ***I****ntercept and* ***O****bstruct* ***T****errorism.*

exchange. Australia, heavily influenced by both the UK and the US post 9/11, put in place 54 pieces of counter-terrorism related regulation in such that critics call its approach 'hyper-legislative.'[70] Australia was particularly concerned with having in place vigorous oversight.

Each of the three necessarily echo each other's approach. There are four main similarities and four main differences that offer Canada some considerations for the way forward on its interagency information exchange. The four similarities are the discomfort in using the military in a law enforcement role, the use of Crown Prerogative in national security, the structure of the state security apparatus and resonance in legislation. The four main differences are, unlike the others, Canada does not have: a separate foreign intelligence service; mature tactical interagency sharing nodes; an independent intelligence oversight body with multiagency authority; or a federal privacy registry.

**THE UNITED STATES APPROACH**

There are five keys Acts that provide the architecture and structure the debate surrounding information sharing in the US federal government; the 1876 *Posse Comitatus Act (PCA)*, the 1947 *National Security Act*, the 1974 *Privacy Act*, the 1978 *Foreign Intelligence and Surveillance Act* (FISA) and, the 2001 *USA PATRIOT Act*. Each was the direct result of political pressure arising from precipitous events in American history. Three are attempts to limit government overreach and two are attempts to increase or better translate government authority. Though conventional wisdom dictates that it is uncomplicated to pass along information within US government, there continues to exist various thresholds that serve as brakes to universal access; pretext, firewall, republican and privacy.

---

[70] Roach, *The 9/11 Effect: Comparative Counter-Terrorism* …309.

The *PCA* was a direct result of official discomfort with the existence of a powerful standing Army after the American Civil War.[71] This discomfort arose due to the military governorship of the Confederate States during the Reconstruction Era (1867 – 1877). The Act criminalized the actions of anyone who,

> willfully uses any part of the Army or Air Force as a *posse comitatus* or otherwise to execute the laws except in cases and under circumstances expressly authorized by the Constitution or Act of Congress.[72]

Though arguably created for explicitly racist reasons, it is unusually venerated in American law.[73] Unique to the US, it is of concern to this discussion as it is the Act that is most often cited when determining the legal boundaries of information sharing between law enforcement and the military. As it makes the use of the military in domestic law enforcement potentially a criminal act, US military leadership is always hesitant to support or be seen to support law enforcement even if it is just sharing intelligence.[74]

The *National Security Act* arose at the end of World War II and on the cusp of the Cold War. It created the Central Intelligence Agency (CIA) and enshrined it with certain foreign authorities. It also accepted the use of means not permitted in domestic law to achieve foreign

---

[71] The Civil War lasted from 1861 – 1865. The confederation of Canada can also be attributed to this same discomfort.

[72] Sales, "Mending Walls: Information Sharing After the USA PATRIOT Act"…1819. *Posse comitatus* refers to the common law authority of a local sheriff's to summon local assistance in aid of keeping the peace or arresting criminals. The Airforce was included in this Act by an amendment in 1956. Interestingly, it does not apply to National Guard under the authority of state government in their home states nor to the Navy or Marines. That said, Department of Defence, as a matter of policy, interprets its application to the Navy and Marines equal to that of the Army and Airforce.

[73] It was racist in that the American government in the Reconstruction Era, in response to pressure by the South, did not want the military used to protect black freemen's right to vote.

[74] Breaking said law can be punished by a fine of up to $10 000, two years imprisonment, or both. As a historical aside, no American has ever been convicted under the *Posse Comitatus* Act.

goals. However, the CIA was denied any "police, subpoena, or law enforcement powers or internal security functions."[75] This ambiguous regulation has since stymied CIA cooperation with law enforcement agencies.

The *Privacy Act* arose from political concern with the vague governance of federal surveillance exposed by the Watergate Scandal. Broadly, it is meant to provide "safeguards against invasion of personal privacy through the misuse of records by Federal Agencies." [76] While it imposes a ban on inter-agency information sharing without an individual's consent, its various loopholes do not completely limit inter-agency discourse. In particular, it permits sharing without consent as long as the information is for "routine use" and its release is disclosed on a Federal Register.[77]

The *Foreign Intelligence and Surveillance Act* (*FISA*), similar to the *Privacy Act*, arose from federal investigations into the legality of domestic surveillance. It prescribes the procedures for collection of intelligence against agents of foreign powers inside the US. Most pertinent to the Federal Bureau of Investigation (FBI), who have the domestic responsibility for counter-terrorism and counter-espionage, it enabled what is now known as the FISA Wall which prevented foreign intelligence from sharing information with law enforcement due to the concept of 'primary purpose.'[78]

---

[75] Nathan Sales, "Mending Walls: Information Sharing After the USA PATRIOT Act" in *Texas Law Review* (July 2010), 1813. It is thought that Congress banned the CIA from internal security in order to prevent it reflecting the authoritarian Nazi and Soviet systems.

[76] United States Department of State, "The Privacy Act," Last Accessed 03 May 2014, http://foia.state.gov/Learn/PrivacyAct.aspx.

[77] Routine use by another agency in that it must be compatible with the purpose for its collection by the parent agency.

[78] The 'primary purpose' restriction meant that surveillance conducted against foreign agents for security reasons could not in turn be used for criminal prosecution.[78]

The *USA PATRIOT Act* was in direct response to the perceived security deficiencies that led to 9/11. It was truly an omnibus legislation that adjusted governance of such issues as border security, terrorism investigation, and surveillance. As 9/11 was regarded as primarily an intelligence sharing failure, the *USA PATROIT Act* meant to increase the data flow and better help security agencies 'connect the dots.'[79] In particular, it actively strove to break down the FISA Wall and legally encouraged the foreign intelligence community to make and maintain relationships with the law enforcement community. It directed the Department of Justice and the CIA to determine a comprehensive process by which foreign intelligence could tip off domestic criminal investigation and vice versa.[80]

However, the *USA PATRIOT Act* did not remove all existing barriers to unrestricted common access to information. The laws of the four preceding Acts still exist and, arguably, balance the openness of the *USA PATRIOT Act* via four primary constraints. The first, pretext, is the concern that law enforcement would use the looser rules governing espionage in pursuit of domestic criminal surveillance. It is restricted by the rules of the *NSA* and *FISA*. The second, firewall, is the concern that law enforcement would use the accepted, though sometimes unsavory means permitted in foreign affairs. It is restricted in the rules of the *PSA, National Security Act* and *FISA*. The third, republican, is the concern that the military would act independently of civilian control and become a partisan political force of its own in the domestic sphere.[81] It is restricted in the rules of the *PCA*. Finally, the fourth, privacy, is the concern of

---

[79] Government of the United States, *The 9/11 Commission Report* (Washington: Government of the United States, 2004) 408.

[80] This legal instrument is considered watershed in US law.

[81] This distinctively and curiously American and is not legislatively reflected anywhere else in Canadian, British or Australian law.

individual loss of consent towards government observation and individual presentation to the world. It is restricted in the rules of the *Privacy Act*.

## THE UNITED KINGDOM APPROACH

The UK has an approach to national security more mature and nuanced than any of its occidental allies and some of its legal innovations have served as models to other countries. Distinguished British Judge Lord Alfred Stevens captured the British philosophy in the lecture series, *Freedom Under the Law*, stating,

> Every society must have the means to protect itself from marauders. It must have powers to arrest, to search and to imprison those who break the laws. So long as those powers are properly exercised, they are themselves the safeguards of freedom.[82]

Its current security architecture is due to a centuries old legacy of domestic terrorism and empire governance that resulted in the cultural recognition of the pragmatic need for inter-agency information sharing. Though the solutions that were enacted in response to the 'Irish Problem,' the 1988 Pan Am Flight 103 bombing and again in response to 9/11 still resound, it was the London Bombings of 07 July 2005 (7/7) that have served as the latest catalyst for present mechanisms.

The UK security apparatus is built around three main pillars; domestic security, foreign security, and strategic communications. Domestic Security is served by the Security Services and the police, most notably of which is the Special Branch of Scotland Yard.[83] Foreign security is

---

[82] Alfred Denning Stevens, *The Hamlyn Lectures First Series: Freedom Under the Law*, (Toronto: The Carswell Company Ltd., 1949), 5.

[83] Security Services were once known as MI5 and are often still referred to by that name.

served by the Security Intelligence Services and the Department of Defence.[84] Strategic communication, primarily electronic surveillance serving both domestic and foreign customers, is attended to by the Government Communications Headquarters (GCHQ). Legislatively, the apparatus is inflated by the 1989 *Secret Service Act*, the 1994 *Secret Intelligence Services Act*, the 1998 *Data Protection Act* of 1998, *Terrorism Act 2000*, the *Regulation of Investigatory Powers Act* 2000, the 2001 *Anti-Terrorism, Crime and Security Act*, the *Criminal Justice Act* of 2003, the 2011 *Terrorism Prevention and Investigation Act* and the quinquennial *Armed Forces Act*.

Of note, regarding national security and information sharing, Section 1 of the *Intelligence Services Act* authorizes SIS and GCHQ the three main functions of national security, protection of economic wellbeing and "in the support of the prevention or detection of serious crime."[85] In addition, Section 28 of the *Data Protection Act* declares that personal data are exempt any of the provisions data protection if the exemption "is required for the purpose of safeguarding national security."[86]

The UK challenge, as underscored by 7/7, was the demarcation as to when an individual went from being a foreign security threat (SIS responsibility) to being a domestic security threat (SS responsibility) to being a routine criminal (police responsibility). Tactically, these challenges are were overcome by the creation of Tactical Coordination Group (TCG)s that are the executive coordination node for SIS, SS, police and as necessary, Defence Intelligence (DI). Strategically, they were overcome by the existence of the Central Intelligence Machinery which includes the

---

[84] Security Intelligence Services were once known as M16 and are often still referred to by that name.

[85] United Kingdom, *Intelligence Services Act 1994* (London: Parliament of the United Kingdom, 1994), Section 1.

[86] United Kingdom, *Data Protection Act 1998* (London: Parliament of the United Kingdom, 1998), Section 28.

cabinet level National Security Council, the parliamentary level National Security Council Committee for Threats, Hazards, Resilience and Contingencies, the federal bureaucratic Intelligence and Security Committee and the professional Joint Intelligence Committee (JIC).

The UK's strategic investment was reiterated in its most recent Strategic Defense and Security Review which emphasized intelligence and "coordinated analysis and assessment."[87] Pan-government intelligence sharing is primarily managed via both the JIC and the Joint Threat Analysis Centre (JTAC) whose primary function is to be a multi-agency intersection for the analysis and dissemination of intelligence. Together, they play an important synergetic role in analyzing state security threats. JTAC determines "threat levels and issues timely threat warnings as well as more in-depth reports on trends, terrorist networks and capabilities" whereas JIC assessments are more strategic and situate JTAC assessments in "a broader geopolitical context for Ministers and senior officials." [88] As it can collect intelligence in support to SIS, SS and GCHQ operations and conduct "all-source intelligence analysis", UK DI is a key contributing member to the JIC and JTAC.

**THE AUSTRALIAN APPROACH**

Much like Canada, Australia had not taken domestic security and its associated means as seriously as the US and UK prior to their hosting of the Summer Olympics in 2000 and the subsequent events of 9/11. Australia then went into hyper-legislation mode enacting no less than 54 pieces of legislation at the federal level alone. Their new governance upset existing legal notions that individuals should not be detained, questioned or subjected to surveillance unless

---

[87] Julian Richards, *A Guide to National Security: Threats, Responses and Strategies* (Oxford: Oxford University Press, 2012), 92.

[88] United Kingdom. *National Intelligence Machinery* (London: Government of the United Kingdom, 2010), 25.

suspected of criminal activity. Prime Minister Kevin Rudd, in a 2008 Parliamentary statement asserted that Australian national security interests must be followed in an accountable manner which "meets the government's responsibility to protect Australia, its people and its interests while preserving our civil liberties and the rule of law." [89] Australian professor George Williams countered this alleging, "powers and sanctions once thought to lie outside the rules of a liberal democracy except during wartime have now become part of the Australian legal system."[90]

The Australian security apparatus is built around four federal agencies; the Australian Secret Intelligence Service (ASIS), the Australian Security Intelligence Organization (ASIO), the Australian Protective Services and the Defense Signals Directorate (DSD). ASIS deals with foreign intelligence, ASIO deals with domestic intelligence, DSD deals with strategic communications and APS is a federal police service.[91] The Defense contribution is the Defense Intelligence and Security Group (DISG) which includes the Defense Intelligence Organization (DIO) whose primary mission is to, "analyse foreign developments and produce intelligence assessments for the Australian Government and Defense." [92] Their apparatus is amplified by legislation including the *Defense Act*, the 1979 *National Australian Security Intelligence Organization Act*, the 1979 *Telecommunications (Interception and Access) Act*, the 2001 *Intelligence Services Act*, the 2004 *National Security Information (Criminal and Civil Proceedings) Act*, the 2005 *Anti-Terrorism Act* and the 2010 *Independent National Security Legislation Monitor Act*.

---

[89] George Williams, "A Decade of Australian Anti-Terrorism Laws" in *Melbourne University Law Review* Vol. 35 (2011), 1139.

[90] Williams, "A Decade of Australian Anti-Terrorism Laws" …1135.

[91] APS is roughly analogous to the FBI and to the federal responsibilities of the RCMP.

[92] A Australian Department of Defence, "What We Do," Last accessed 17 March 2014, http://www.defence.gov.au/dio/what-we-do.shtml. Aside from the DSD, who answers to the Minister of Defense but is in fact a Whole-of-Government (WoG) agency.

The Australian security intelligence community has very robust pan-agency executive and oversight. Strategically, there is the cabinet level National Security Committee and the National Counter-Terrorism Committee which includes representatives of both federal and state governments. There is the National Intelligence Coordination Committee and the Head of Intelligence Agencies Meeting both of which include Defense as a primary attendee. The cabinet level National Security and International Policy Group has a National Security Information Coordination Officer whose role is specifically to coordinate information sharing across the national security community. Finally, the government has in place the independent office of the Inspector-General of Intelligence and Security (IGIS) who has full access to all intelligence and assists the government in oversight and inquiry. This office is also now reinforced by an Independent National Security Legislation Monitor (INSLM) whose role is to,

> review the operation, effectiveness and implications of Australia's counter-terrorism and national security legislation on an ongoing basis. This includes considering whether the laws contain appropriate safeguards for protecting the rights of individuals, remain proportionate to any threat of terrorism or threat to national security or both, and remain necessary.[93]

There are two major focal points for intelligence analysis and dissemination across the Australian government. The first is the strategic Office of National Assessments (ONA) which provides all-source assessments on international issues to Prime Minster and Cabinet. The second is the National Threat Assessment Centre (NTAC) which is a multi-agency organization embedded in ASIO with the mandate to issues threat assessments that,

[93] Australian Department of the Prime Minister and Cabinet, "Independent National Security Legislation Monitor," Last accessed 17 March 2014, http://www.dpmc.gov.au/INSLM/index.cfm..

> inform the actions of the police and other agencies [including Defence] with a role in protecting Australians and Australian interests from threats to national security.[94]

As Australia, like the UK, deliberately separates its intelligence from its law enforcement agencies, the NTAC is the primary interface in government where tactical intelligence can cross this divide. Defence is represented inside the NTAC by DIO and DSD.

**COMPARE AND CONTRAST**

In evaluating the present security architecture of all four countries, there arises four main similarities: philosophy on the use of the military in law enforcement, the use of Crown Prerogative, the structure of national security and resonance in legislation. There also emerges four main differences that have grounds for future Canadian consideration; foreign intelligence capacity, tactical information coordination nodes, inter-agency intelligence oversight; and, privacy related federal registration.

The philosophy of all four countries behind limiting to the full extent possible the role of the military in law enforcement is driven by two factors. First, the military serves a very lethal role in the pursuit of foreign policy. This is at direct odds with the primary law enforcement mission to guarantee domestic order through peaceful means that may include lethal force.[95] As means of legitimacy, law enforcement must be at all times governed by the law and thus its actors are at all times law focused. The military, as the state's no fail option, are at all times results focused. Blending the two would undermine the military's effectiveness due to the difficulty in balancing this apparent contrast. The second reason is that a military's resources, be

---

[94] Australian Security Intelligence Organization, "About ASIO," Last accessed 17 March 14, http://www.asio.gov.au/asio-and-national-security/units/ntac.html.

[95] But only as an extreme exception to the norm.

they personnel, material or financial, are scarce and using them in non-traditional roles would divert them from their primary mission.

The second main similarity is that of structure or the existence of respective domestic intelligence, foreign intelligence, domestic security, national defense and strategic communications organizations. [96] Each also has nodes for interagency information exchange such as the US Terrorist Threat Integration Centre, the UK JTAC and the Australian NTAC. Security agencies are also supervised by oversight mechanisms that are either embedded in government bureaucracy or detached as standalone entities such as the US' President's Intelligence Advisory Board, the UK's Intelligence Security Committee, the Australian IGIS and the Canadian Security Intelligence Review Committee (SIRC).[97] Finally, each has rigorous legislation in place that governs such concepts applicable to this discourse as privacy and intelligence collection authorities.

As with Canada, the UK and Australia act upon what is known as the Crown Prerogative which allows for customary authority and immunity that belong to the sovereign alone.[98] This entitlement stems from the origins of constitutional monarchy that claim that a state's authority comes from the top down.[99] This is of note because Crown Prerogative can be used, in the absence of binding legislation, as an accepted legal catalyst in the pursuit of national security. The US, on the other hand, does not have a similar overarching mechanism other than the

---

[96] One of the main differences between the three is that though Canada, the UK and Australia have domestic security intelligence agencies separate from law enforcement, the US does not

[97] The SIRC, however, only has a mandate to review the operations of CSIS. It is not inter-agency.

[98] In Canada, this prerogative is embodied in the Governor-General and provincial Lieutenant-Generals and acted upon by the Legislative Executive or Prime Minister and his/her Cabinet.

[99] It is focused almost exclusively on a state's actions in the international realm and include but are not limited to declaration of war, ratification of treaties, receiving ambassadors, issuing of passports and granting of mercy.

President's use of an 'Executive Order' which is not universal and has to be explicitly connected to an existing law.

Legislatively, aside from disparity in the margins which includes differences in opinion on the use of extra-legal mechanisms such as rendition and torture, the extent of preventative detention and the need for a "motive requirement", the four countries are very similar.[100] This is in part due to Canada and Australia's emulation of UK anti-terrorism laws in recognition of UK's history combating domestic terrorism as consolidated in its pre-9/11 *Terrorism Act 2000*. This is further reinforced by each countries use of respective Criminal Codes and immigration laws as a means of judicial prosecution.

The first main differences is that though the US, the UK and Australia have distinct foreign intelligence agencies such as the CIA, SIS and ASIS respectively, Canada does not and thus suffers from a responsibility that is spread inefficiently between multiple departments.[101] Unlike the UK, Canada does not have mature tactical information sharing nodes that are resourced similar to the TCGs and include DI as a pillar partner. Unlike Australia, aside from the Auditor-General, Canada also does not have an interagency oversight body with the authority to provide the check and remedy to all intelligence operations and exchange.[102] Finally, unlike the US, Canada does not have the safeguard of a Federal Registry linked to its *Privacy Act* that would facilitate routine interagency transfers of information.

---

[100] The 'motive requirement' is that under UK law, terrorism requires a political, religious or ideological motive in order to be terrorism and is thus treated differently from other crimes.

[101] The CIA, SIS and ASIS respectively.

[102] The Auditor-General does not have access nor authority over classified information thus cannot act as an interagency mediator or remedy on intelligence.

**SUMMARY**

Though resembling each other in many ways, Canada, the US, the UK and Australia have shades of difference in their overall approach to national security that are worth exploring. Each is harnessed by its common law heritage and its values of democracy, privacy and rule of law. Each is faced with "distinctions between intelligence and law enforcement, between foreign and domestic and between public and private."[103] Each thus has built organizational, legislative and oversight mechanisms that enable it to pursue national security in accordance with its own perspective and mandate. These include devices and obstacles for interagency sharing of information including military intelligence.

The US, though thought to have the most robust and comprehensive apparatus as defined in its *US PATRIOT Act* is still restricted by four obstacles found the *Posse Comitatus, Privacy, National Security* and *FISA Acts:* pretext; firewall; republican; and; privacy. *The USA PATRIOT Act* is in fact, not "as repressive as many on both the Left and Right in the US thought."[104] The UK, with its abundant history with domestic security issues, is most comfortable with interagency information sharing and, as such, has resourced it TCGs, JIC and JTAC as trusted nodes for legal transfer of intelligence. It can best "visualize intelligence […] as a single National Intelligence Service, divided for convenience into its separate components" each with different skills but common conditions.[105] Australia, aside from its leaning to hyper-legislation, has put in place a very vigorous oversight regime that includes both operational and legislative

---

[103] Treverton, "Terrorism, Intelligence and Law Enforcement: Learning the Right Lessons"…122.
[104] Roach, *The 9/11 Effect: Comparative Counter-Terrorism*…176.
[105] Michael Herman, "Counter-Terrorism, Information Technology and Intelligence Change," in *Twenty-First Century Intelligence: Studies in Intelligence*, ed. WesleyWark ( London: Routledge Taylor and Francis Group, 2005), 54.

review. The UK and Australia, like Canada, also retain the prevailing power of the Crown Prerogative to stitch together any gaps in binding legislation, as necessary.

Legislatively, Canada is on par with its Allies. Canada too confronts the tension between "consent and confusion" or "the blurred space between sanctioned opportunities for autonomy and contestation and zones of containment and repression."[106] Any future changes to Canadian law concerning internal military intelligence exchange would likely to be innovative rather than imitative. From each of its Allies, Canada can continue to mature its own approach to national security and intelligence distribution. In comparison, the immaturity of Canada's tactical intelligence sharing nodes as well as the absence of an independent interagency intelligence oversight authority, a foreign intelligence agency and a privacy related federal registry, are four key gaps that inhibit comprehensive information sharing.

If anything, however, Canada's approach has been more restrained with regards to putting in place such instruments as control order regimes. University of Toronto Professor Kent Roach attributes this to Canada being shaped "by the *Canadian Charter of Rights and Freedoms* and by concerns about preserving multicultural relations."[107] Further, Canada decided to pursue a distinctive strategy that interpreted terrorism as just one of the many threats faced by a state and thus should be countered in an integrated rather than focused manner. The existing Canadian methodology will be explored in greater detail in Chapter 4 – *The Canadian Approach*.

---

[106] Colleen Bell, The Freedom of Security: Governing Canada in the Age of Counter Terrorism, (Toronto: UBC Press, 2011), 148 - 149.

[107] Stanley Cohen, Review of *The 9/11 Effect: Comparative Counter-Terrorism* by Kent Roach, in *Canadian Criminal Law Review* Vol. 17 (2011), 285.

## CHAPTER 4
## THE CANADIAN APPROACH

*The Government of Canada recognizes the importance of information sharing, both domestically and internationally, in ensuring the safety and security of Canadians. Within the Government of Canada, each department and agency undertakes information sharing in accordance with Canadian laws and their respective legislation, mandates, and regulations.*[108]

- Government of Canada Response to Auditor-General Report 2009

### OVERVIEW

The current state of the Canadian security apparatus has been shaped by three primary events: the 1970 invocation of the *War Measures Act* against the Front de Liberation du Quebec (FLQ), the fallout from the 1985 Air India bombing and the response to the 9/11 attacks in 2001.[109] Each of these caused existential reviews of the Canadian national security approach that facilitated fundamental changes. These changes included such phenomena as the creation of the Canadian Security Intelligence Service (CSIS) and the recognition that national security is too broad to be stove-piped. The Special Senate Committee on Anti-Terrorism in its interim 2011 report reinforced this by stating that national security issues are, "are too important to be entrusted to a single department or agency." [110] They also catalyzed the recognition that the relationship between those that collect intelligence and those that pursue evidence must be legally and culturally clarified.

For the purposes of this discussion, the Canadian national security apparatus does not legally permit the sharing of military generated I2 with the other national security agencies via any mechanism other than that of Crown Prerogative. This is due to two factors: first, other than

---

[108] Office of the Auditor General of Canada, *Status Report of the Auditor General to the House of Commons – 2009* (Ottawa: Government of Canada, 2009), 18.

[109] The Air India Bombing was the worst air terrorism event in global history until 9/11.

[110] Senate of Canada, *Interim Report of the Special Senate Committee on Anti-Terrorism: Security, Freedom and the Complex Terrorist* (Ottawa: Government of Canada, 2011), 27.

in prosecution of its own members, the military is considered a producer of intelligence rather than evidence; and, second, the military has a uniquely expeditionary responsibility and a legal exclusion to independent domestic missions. Combined, they demonstrate that for the Canadian state, other than for niche purposes, military generated intelligence does not have a role to play in domestic evidence.[111] However, as demonstrated below, within its existing legislation, information sharing, intelligence coordination and oversight, Canada can, in fact, facilitate the transfer of military enabled I2 as evidence without significant legal hurdles.

**THE HISTORY**

The political reaction to the use of the *War Measures Act* in response to the 1970 FLQ crisis was harsh. The Right Honorable Tommy Douglas, then leader of the New Democratic Party, stated, "The government, I submit, is using a sledgehammer to crack a peanut."[112] Post-crisis evaluation resulted in the replacement of the *War Measures Act* by the 1988 *Emergencies Act*. One of the major differences between these statutes was that any temporary laws made under the Act were now subject to the Canadian *Charter of Rights and Freedoms*. This means that any temporary loss of expected civil rights must be reasonable and justified and that use of Crown Prerogative power has its limits. This event also led to the McDonald Commission which studied, in depth, the RCMP's methods while investigating the FLQ. It recommended a standalone domestic security spy agency and CSIS was thus created in 1984.

---

[111] These niche capabilities include CSEC (for signals intelligence), CANSOFCOM (for kinetic response to domestic terrorism) and the Military Police Branch (for security on all Department of National Defense properties and for Counter- Military Intelligence) all of which have explicit domestic mandates not reflected elsewhere inside the Canadian Armed Forces.

[112] Thomas Douglas, Quoted in John Gray, "Pierre Elliott Trudeau: 1919-2000," Globe and Mail, 30 September 2000. Last accessed 03 May 2014, http://v1.theglobeandmail.com/series/trudeau/jgray2_sep30.html.

It can be argued that the legacy of 1985's Air India Flight 182 bombing, within Canada, is as resonating in federal security policy as that of 9/11. This is countered by Maclean's magazine's assertion that the event, "snuffed out hundreds of innocent lives and altered the destinies of thousands more, but it neither shook the foundations of government, nor transformed its policies."[113] Though it took the federal government 20 years to commission a formal inquiry, retired Supreme Court Justice John Major, upon release of his findings in 2010, asserted that the incident was,

> a cascading series of errors contributed to the failure of our police and security forces to prevent this atrocity. The level of error, incompetence, and inattention which took place before the flight was sadly mirrored in many ways for many years, in how authorities, Governments, and institutions dealt with the aftermath of the murder of so many innocents: in the investigation [and] the legal proceedings.[114]

Highly comprehensive, the report focused on several key issues including threat assessment, interagency cooperation and the relationship between intelligence and evidence. In particular, it highlighted the institutional tension between the RCMP and CSIS and the need to enhance the role of the National Security Advisor (NSA) regarding authority to distinguish between evidence and intelligence.

The final event of consequence was the incidents of 9/11. In response to what was perceived as an existential threat, Canada had to, "…successfully negotiate a relatively safe passage between the Scylla of the terrorist threat and the Charybdis of American

---

[113] John Geddes and Ken McQueen, "Air India Inquiry Reveals Intelligence Faults," Macleans Magazine, 25 June 2007, Last accessed 03 May 2014, http://www.thecanadianencyclopedia.ca/en/article/air-india-inquiry-reveals-intelligence-faults/.

[114] John Major, *Opening Remarks On the release of the Report of the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182*, (Ottawa: Government of Canada, 2010), 2.

unilateralism."[115] It led directly to the expansion of state authorities in the broad 2001 *Anti-Terrorism Act (ATA)* and the thickening of Canadian border security. The legislative response has since been tested by the circumstances surrounding the rendition of Maher Arar. It resulted in the formal commission into the *Inquiry Into the Actions of Canadian Officials in Relation to Maher Arar* which highlighted difficulties surrounding inter-agency information sharing.[116] Faisal Kutty, a Canadian Human Rights lawyer claimed that the Arar saga, "brought into focus the unintended victims of draconian laws and policies hastily enacted post 9/11…"[117]

## THE CANADIAN SECURITY INTELLIGENCE APPARATUS

The Canadian approach is uniquely nuanced. University of Ottawa Law Professor Craig Forcese asserted that Canada has "a sound democratic model for national security, namely, effective intelligence; capable law enforcement appropriate, stable laws; good governance; [and,] accountability" [118] Like the UK and Australia, the Canadian state still retains the awesome use of Crown prerogative as the legal filler for national security. It is often invoked in the absence of legislative framework for any state action that is felt necessary for self-defence. Unlike the UK and Australia, however, Canada has been legally comfortable with the vagueness and versatility of Crown prerogative and has not put in place 'hyper-legislation' meant to translate all state security options. Canada, rather than focusing on terrorism as the exclusive national threat, has

---

[115] Stuart Farson and Reg Whitaker, 'Canada' in *PSI Handbook for Global Security and Intelligence National Approaches Volume 1: The Americas*, ed. Stuart Farson, Peter Gill, Mark Phythian and Shlomo Shpiro (Westport, Connecticut: Praeger Security International, 2008), 27.

[116] Otherwise known as the *O'Connor Report* after its head, Associate Chief Justice of Ontario, Judge David O'Connor.

[117] Verkata Online Encyclopedia, "Maher Arar," Last Acessed 03 May 2014, http://wiki.verkata.com/en/wiki/Maher_Arar?page=3.

[118] Craig Forcese, "Canada's National Security Complex: Assessing the Secrecy Rules," in *IRPP Choices* Vol. 15 No. 5 (June 2009), 1.

enveloped an 'all threats' approach that includes cyber-warfare, transnational organized crime, natural disasters and pandemics as equally likely dangers.[119] Finally, Canada has also used its immigration rather than criminal laws as means of obstructing undesirable individuals.

Professor Forcese also articulated the following tenants regarding national security intelligence,

> National-security-related information is protected at several levels in Canadian information law: laws limiting open government rules otherwise applicable to the executive branch; laws that constrain the open court concept and disclosure rules typically applied by Canada's courts; and statutes that criminalize the wrongful disclosure of particularly sensitive information.[120]

Collectively, it is held together by the statues that govern individual departments, governmental policy and the existence of the Crown's prerogative powers. The 2009 Auditor General (AG)'s Report on National Security stated that Canadians need,

> to have confidence that the decisions and activities of intelligence agencies are legal, consistent, and appropriate, and that they are subject to examination by independent review agencies for reporting to their minister or Parliament.[121]

With this in mind, legislatively, there are 13 core Canadian federal acts that that govern national security intelligence. These are re-enforced by three extant federal strategies.[122] For this discussion, the following take precedence:

- *Charter of Rights and Freedoms*. Ratified as part of the 1982 *Canada Act*, it is now a foundational premise upon which all Canadian federal laws are built. It guarantees the

---

[119] Interestingly, this 'all threats' approach has since been studied and emulated by its Allies.

[120] Ibid, 9.

[121] Office of the Auditor General of Canada, *Status Report of the Auditor General to the House of Commons – 2009…*2.

[122] Collectively, they also include the *War Measures Act*, the *Emergencies Act*, the *RCMP Act*, the *CSIS Act*, the *Canada Evidence Act*, the *Access to Information Act*, the *Security Offenses Act*, the *Criminal Code*, the *Canada First Defense Strategy* and the *Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy.*

rights set out in it are, "subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."[123] Regarding this discussion, this charter enshrines such fundamental precept as mobility and equality under the law. It also clarifies certain legal rights such as security against unreasonable search and *habeas corpus.*

- *Immigration and Refugee Protection Act (IRPA).* Passed originally in 1869 but amended most recently in 2012, it governs the movement for the purpose of residency by foreign individuals into Canada. Canada has used the *IRPA* as one of its primary federal tools to either remove or block unwanted foreigners as it allowed officials to use, "investigative detention, secret evidence, a lower standard of proof and wider liability rules" than that available under the *Criminal Code* and *ATA*.[124]

- *Anti-Terrorism Act (ATA)*. An omnibus bill passed in 2001 and updated in 2013 as the *Combatting Terrorism Act*, it was a direct response to 9/11. In particular, it amended the *Criminal Code*, *Official Secrets Act* and, *Canada Evidence Act.* To quote the *ATA* preamble,

> whereas these comprehensive measures must include legislation to prevent and suppress the financing, preparation, facilitation and commission of acts of terrorism, as well as to protect the political, social and economic security of Canada.[125]

- *Privacy Act*. Passed in 1983, this 'quasi-constitutional' Act governs two norms: federal government management of personal information on Canadian citizens,

[123] Canada. *Charter of Rights and Freedoms* (Ottawa: Parliament of Canada, 1982), Section 1.
[124] Roach, *The 9/11 Effect: Comparative Counter-Terrorism*…396.
[125] Canada. *Anti-Terrorism Act* (S.C. 2001, c. 41), (Ottawa: Parliament of Canada, 2001), Preamble.

permanent residents and foreign nationals; and, the privacy expectations of individuals during interactions with the federal government.[126] It restricts the free sharing of information between departments without explicit purpose or individual consent.[127] Of note, it does not have a Federal Registry similar to that found in US law.

- *National Defense Act (NDA)*. Passed in 1922, the NDA provides the legislative framework for the use of military forces by the Canadian state. Use of the military in a domestic, law enforcement role is illegal without the express request of provincial authorities in any case, "in which a riot or disturbance of the peace, beyond the powers of the civil authorities to suppress, prevent or deal with."[128] This statute can only be broken by the Parliament's invocation of the *Emergencies Act*. Of topical note, the NDA also houses the statues that regulate CSEC.
- *Public Safety Act*. Passed in 2004, it made significant amendments to the *Canadian Aviation Transport Security Act* and *IRPA* amongst others. It is important because it reinforced the legal sharing of information between RCMP, CBSA and CSIS for transportation or national security purposes.
- *Securing an Open Society: Canada's National Security Policy*. Approved in 2004 and the first of its kind, it articulates, "core national security interests and proposes a

[126] It is called 'quasi-constitutional' because though privacy is not enshrined in the Canadian *Charter of Rights and Freedoms*, it is absolutely essential to the preservation of a free, democratic state.

[127] Explicit purpose means that it can only be shared if it is directly connected to the purpose for which it was originally collected.

[128] Canada. *National Defense Act* (R.S.C., 1985, c. N-5), (Ottawa: Parliament of Canada, 2013), Section 275.

framework for addressing threats to Canadians."[129] It is unique, in part, because it counts terrorism as only one of the main threats to national security. It first announced the introduction of biometric technology to Canadian passports.

Like its Allies, Canada has divided its security tasks into foreign and domestic. Foreign security intelligence is provided by the Department of Foreign Affairs, Trade and Development (DFATD), CSIS and DND.[130] Domestic security intelligence is provided primarily by CSIS but is informed by the police, primarily the RCMP. Straddling both realms and in support to all agencies are the Communications Security Establishment Canada (CSEC) who provide SIGINT and FINTRAC. Domestically, only the police and, to a degree, CSIS and CSEC have the authority to covertly collect intelligence against Canadians in the pursuit of either criminal prosecution or advice to government on security issues.[131] However, overt intelligence collection can be done by FINTRAC, CBSA, CIC, and DND if it falls within the respective mandate of their agency.[132] Internationally, CSIS, CSEC, DND, FINTRAC and DFATD have authority to collect covert intelligence however, they are restricted in their ability to spy on Canadians abroad. [133]

Each agency has its own analysis capacity, most notably DND's Intelligence Group, however there are also several inter-agency elements that merge information from multiple

---

[129] Canada. Public Safety Canada, *Securing an Open Society: Canada's National Security Policy* (Ottawa: Government of Canada, 2004), 4.

[130] Canada is unique in that it does not have a standalone agency similar to the US CIA that is responsible for the exclusive collection of foreign intelligence.[130]

[131] CSEC is only permitted to collect in Canada at the express request of the Minister of Foreign Affairs, Trade and Development or the Minister of National Defense.

[132] For DND this is for domestic counter-military intelligence or in the internal investigation of military members.

[133] As of its 2010 – 2011 Public Report, CSIS alone had 248 information sharing agreements with foreign entities in 151 countries. This is independent of intelligence generated through information sharing agreements with international peer organizations.

agencies. Strategically, the role of the office of the NSA is paramount. He/she ensures "effective coordination of Canada's security and intelligence community."[134] In this, they are supported by the Cabinet Secretariats of Security and Intelligence; Foreign Affairs and Defense; and, International Assessment Staff. As the NSA and these three secretariats are inside the Privy Council Office and work closely with both the Prime Minister and the Clerk of the Privy Council, they have full executive authority to be the lodestone inter-agency information bridge.

Tactically, the main node for inter-agency information sharing is the Integrated Terrorism Analysis Centre (ITAC). Described originally in 2004's *Securing an Open Society: Canada's National Security Policy* in recognition of the need to better facilitate inter-agency information sharing, it is housed by CSIS but manned by all security agencies including DND. Its role is to, "to help prevent and reduce the effects of terrorist incidents on Canadians and Canadian interests, both at home and abroad."[135] Alternate tactical nodes for information sharing are the Integrated National Security Enforcement Teams (INSETs) who include representation from the RCMP, CSIS and CBSA. Their role, in part, is to "enhance partner agencies collective ability to combat national security threats and meet all specific mandate responsibilities."[136] Finally, there are the Maritime Security Operational Centers (MSOCs) which have representation from RCMP, DND, and CBSA.[137] However, the 2009 AG's Report highlighted what is a universal challenge wherein these nodes,

---

[134] Privy Council Office, "National Security Advisor to the Prime Minister," Last accessed 03 April 2014, http://www.pco-bcp.gc.ca/index.asp?lang=eng&page=information&sub=publications&doc=Role/role2013-eng.htm#a3.

[135] Integrated Threat Assessment Centre, "ITAC's Role," Last accessed 03 April 2014, http://www.itac.gc.ca/bt/rl-eng.asp.

[136] Royal Canadian Mounted Police, "Integrated National Security Enforcement Teams," Last accessed 03 April 2014, http://www.rcmp-grc.gc.ca/secur/insets-eisn-eng.htm.

> [have] only a limited ability to combine and analyze data as departments do not have unrestricted access to each other's data due to legal constraints over information sharing.[138]

To quote Law Professor Lisa Austin, "a right without a remedy is no right."[139] With this in mind, there are four main review authorities, each of which, as a means of oversight, provide an annual Parliamentary report. CSIS is held to account by the Inspector General as well as the Security Intelligence Review Committee (SIRC).[140] The RCMP, aside from daily review by the courts, is appraised by the Commission for Public Complaints Against the RCMP. CSEC has its own independent Commissioner.[141] The oversight recommendations following the *Inquiry Into the Actions of Canadian Officials in Relation to Maher Arar* have taken this further in recommending that the SIRC mandate be expanded to review the national security activities of CBSA, CIC, FINTRAC and DFATD. It also recommended that there should be greater interaction between the review authorities to match the increasing inter-agency coordination.

**INTERPRETATION OF EXISTING LAW**

Legal boundaries constraining the sharing of military enabled intelligence with domestic agencies is as much perception as fact. Part of this perception is driven by the Canadian strategic culture wherein Canada,

---

[137] Their role is uniquely focused on maritime security. These were also created in the 2004's *Securing an Open Society: Canada's National Security Policy.*

[138] Office of the Auditor General of Canada, *Status Report of the Auditor General to the House of Commons – 2009…*14.

[139] Lisa Austin, "Is Privacy a Casualty of the War on Terrorism?," in *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*, ed. Ronald Daniels, Patrick Macklem and Kent Roach (Toronto: University of Toronto Press, 2001), 260.

[140] SIRC is considered independent and is typically staffed by retired Members of Parliament. Its current chair is the Honorable Deborah Grey.

[141] Of note, all other agencies that produce intelligence, including DND, have no separate review body though they can be held to account by the existing review authorities if they act in support to CSIS, RCMP or CSEC.

> has not built up an intelligence culture of innate political cultural acceptance of the role of intelligence in national security. Knowledge resources about intelligence matters are not widely available to Canadians: until recently the intelligence services themselves preferred reticence over publicity; parliamentarians had little scope or interest in probing the intelligence domain; the mass media seldom reported on intelligence and security matters except in sensationalist terms; intelligence studies were generally neglected in academe, with singular exceptions, even where there exist programs in security and defense studies. [142]

As Canada already consciously treats foreigners as legally different from Canadians, the obligation to protect their charter-like rights is not as restrictive as initially supposed. University of Toronto Professor Audrey Macklin stated in 2001 that, "laws that arouse deep concern about civil liberties when applied to citizens are standard fare in the immigration context."[143] This was highlighted by the Federal Court of Canada as part of their decision on *Amnesty International Canada v. Canada (Chief of the Defense Staff)* in which they held that Canadian law, including the Charter, could only be applied in another state with the consent of the other state.[144] This is also reflected in the authorities given to CSIS and CSEC to covertly collect intelligence on foreign nationals and to CBSA to explicitly deny foreign entry into Canada for security, criminality, health or financial reasons.[145]

Due to the lower bar governing immigration, Canada has not been hesitant to make use of the *IRPA* in the defense against unwanted foreigners. University of Toronto Professor Kent Roach declared that the government may often "rely on immigration proceedings to remove

---

[142] Forcese, "Canada's National Security Complex: Assessing the Secrecy Rules,"…9.
[143] Roach, *The 9/11 Effect: Comparative Counter-Terrorism*… 396.
[144] Office of the Commissioner for Federal Judicial Affairs Canada, *Amnesty International Canada v Canada, 2008 FCA 401 [2009] 4 F.C.R. 149* (Ottawa: Government of Canada, 2008).
[145] This goes directly against the mobility rights enshrined in the *Charter of Rights and Freedoms* Paragraph 6 (1) which states, "Every citizen of Canada has the right to enter, remain in and leave Canada."

people from Canada who have supported crimes of terrorism committed outside Canada."[146]. The *IRPA* also allows the use of security certificates which permit the Public Safety Minister and the Minister of Citizen and Immigration to co-declare foreigners as "inadmissible on grounds of security, violating human or international rights, serious criminality or organized criminality."[147] The legal remedy is the review of the certificate by a federal court judge to determine reasonableness.[148] Use of the *IRPA* as a counter-threat tool, however, has proven to be highly controversial as it lacks the "moral and denunciatory force of criminal prosecutions."[149]

The tension inherent in the 'intelligence as evidence' debate is most starkly emphasized in the relationship between CSIS and the RCMP. CSIS, with its national security mandate, has the responsibility to investigate national security threats. It needs to provide its sources with the security found in secrecy. The RCMP, however, has a responsibility to investigate security threats as a crime. It needs to pursue the transparency necessary for open court. Post-*ATA*, with its expansion of the definition of terrorism and associated crimes, the RCMP now must pursue investigations using sources once considered to be exclusively those of CSIS. The Supreme Court of Canada in a precedence setting ruling *Charkaoui v. Canada (Citizenship and Immigration)* recognized that the activities of the RCMP and CSIS were converging. [150]

---

[146] Kent Roach, *September 11: Consequences for Canada* (Kingston: McGill-Queen's University Press, 2003), 32.

[147]Canada. *Immigration and Refugee Protection Act* (S.C. 2001, c. 27), (Ottawa: Parliament of Canada, 2001), Section 77. The requirement for approval by two rather than one minister was meant as an added means of oversight and mitigates the power of one individual towards directing, in particular, detention without trial.

[148] However, this review often obligates the presentation of classified information that cannot be disclosed to defence counsel thereby inviting comparison to Frank Kafka's infamous, *The Trial*.

[149] Roach, *The 9/11 Effect: Comparative Counter-Terrorism*… 396.

[150] Supreme Court of Canada, *Charkaoui v. Canada (Citizenship and Immigration [2007] 1 S.C.R. 350, 2007 SCC 9* (Ottawa: Government of Canada, 2008). The irony is that the creation of CSIS, as an intelligence agency without the power of law enforcement, was, in part, a direct result of the overreach of the police during the FLQ crisis.

This same ruling also obligated CSIS to retain any 'raw intelligence' that resulted from their investigations to be used, potentially, as evidence.[151]

According to Roach, there will continue to be legal disputes between law enforcement and intelligence "over the exact location of this rather fuzzy line and whether prosecutions should be foregone in order to continue to collect intelligence."[152] This dichotomy remains unresolved in law though there have been several recent recommendations made via the 2009 AG Report, the Major Report and the O'Connor Report to relieve this tension.[153] They include the empowerment of the NSA with the discretion to balance the rights of the individual with the responsibilities of the state, the expansion of the security clearances for members of the legal community and the use of 'trusted agents' to enable 'parallel build' wherein intelligence can be used to steer investigations without expectation that it becomes evidence.[154]

## MILITARY SPECIFIC CONSIDERATIONS

The most recent prominent push to expand the military's role in domestic security was inside the 2004 *Public Safety Act* which included the contentious provision wherein in the Minister of National Defence (MND) would have the authority to declare temporary military security zones from which the public could be excluded. This provision has since been

---

[151] Prior to this, it was CSIS policy to destroy all raw intelligence, including case notes, interview notes and wire taps after the analysis of said intelligence was captured inside a report. This deliberate destruction was also contended in the Major Report that studied the Air India Bombing. This ruling resulted also in Richard Fadden, then the head of CSIS, to comment, "…within several years, someone will accuse us of acting like the Stasi because of the information we are now compelled to keep."

[152] Roach, *Consequences for Canada*…194

[153] Respectively, the 2009 *March Status Report of the Auditor General of Canada*, the 2010 *Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 Report,* and the 2006 *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar Report.*

[154] Investigators thus may know where the truth lies but have to pursue alternate forms of corroboration that can be presented in court. They are also prepared to give security classifications to defense lawyers.

abandoned due to an opposition to, "an increased domestic role for the military in security matters and feared that it might be used against legitimate dissent and protest."[155] It was, tangentially, tested again during the *Amnesty International Canada v. Canada (Chief of the Defence Staff)* Federal Court Case which sought resolution as to whether Canadian Charter rights extended extraterritorially to CAF detainees. This extraterritorial expansion of state responsibility via the CAF was ultimately dismissed as Canadian law could not be applied in another country, except for very explicit circumstances, without that country's consent.[156]

Domestic oriented, military enabled intelligence such as CSEC SIGINT and Mapping and Charting Establishment (MCE) GEOINT are already shared with partner national security agencies. Aside from the CSEC collection and oversight authorities in *NDA* Part V.1, the *NDA* has no statues that either allow or forbid the military to share intelligence with other security agencies. The closest applicable regulation is that contained in *NDA* Part VI which states that any CAF individual, element or unit may be called upon to,

> aid in the civil power are liable to be called out for service in aid of the civil power in any case in which a riot or disturbance of the peace, beyond the powers of the civil authorities to suppress, prevent or deal with…[157]

This presumably includes all elements of military intelligence however it is restrictive in that it must come as a request from another agency and then be beholden to the laws governing the requesting agency. This is unlike, for instance, the proscriptive disclosure authorities given to FINTRAC in Section 55 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*

---

[155] Roach, The 9/11 Effect: Comparative Counter-Terrorism…422.

[156] Circumstances include when Canada has territorial control in the absence of a functioning state government or when Canada has seized territory while in a state of war against another state.

[157] Canada. *National Defense Act* (R.S.C., 1985, c. N-5), (Ottawa: Parliament of Canada, 2013), Section 275.

or to CSIS in Section 19(2) of the *Canadian Security Intelligence Service Act*.[158] However, as asserted by Retired Canadian Brigadier General James Cox, "…in the world of intelligence, security and accountability requirements often trump rational structure and efficiency."[159]

**SUMMARY**

Catalyzed by the seminal events of the FLQ Crisis, the Air India bombing and 9/11, Canada is now representative of the axiom that the ability of the state to take security measures is proportional to "the threat posed in order to preserve itself and to ensure its continued survival is undoubted and is reflected in the doctrines of necessity and self-defense."[160] Though unique in comparison to the UK and Australia with the absence of 'hyper-legislation' and to the US with its use of the awesome binding powers of the Crown prerogative, nevertheless, Canada has a very robust architecture. It includes the national security legal and executive authority found in no less than 13 federal acts and three national strategies. The statues of primary national importance are the *Charter of Rights and Freedoms*, the *Privacy Act*, the *IRPA*, the *ATA,* the *Public Security Act* and, for the military, the *NDA*. Concerning national strategies, the 2004 *Securing an Open Society: Canada's National Security Policy* is paramount. It also includes the primarily foreign focused agencies such as DND and DFATD, the primarily domestic focused agencies such as RCMP and CBSA, and the dual-hatted agencies such as CSIS, CSEC and FINTRAC. Interagency information sharing nodes can be found strategically in the PCO and

---

[158] Canada. *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (S.C. 2000, c. 17), (Ottawa: Parliament of Canada, 2000) Section 55; and, Canada. *Canadian Security Intelligence Service Act* (R.S.C., 1985, c. C-23), (Ottawa: Parliament of Canada, 1985) Section 19.

[159] Cox, "Lighting the Shadows: An Evaluation of Theory and Practice in Canadian Defense Intelligence"…63.

[160] Stan Cohen, "Concluding Comments from the Department of Justice," in *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*, ed. Ronald Daniels, Patrick Macklem and Kent Roach (Toronto: University of Toronto Press, 2001), 442.

tactically in ITAC and MSOC. Oversight, aside from normal judicial, minister, cabinet and parliamentary supervision, is found with the Inspector-General, Attorney-General, SIRC, Commission for Public Complaints Against the RCMP and CSEC Commissioner.

For the purposes of this discussion, aside from those enacted to protect Canadian citizens, there is no explicit law restricting the military from sharing extra-territorial intelligence with its fellow national security agencies. Belief in the contrary is as much perception as reality and is driven by the existing legal tension between intelligence and evidence as well as whether the CAF has a mandate to judicially support domestic security. In fact, existing arrangements for the sharing of SIGINT and GEOINT already demonstrate that the divide between defense and domestic intelligence can be breached. Furthermore, in the national security architecture, there exists strategic and tactical oversight as well as information sharing nodes that would supervise and enable the interagency sharing of military intelligence and its rendition to evidence. However, like beauty, legal rights, "are in the eye of the beholder…"[161] The following chapter, *Risks and Remedies*, will outline the primary perceived obstacles towards the use of military enabled intelligence as evidence and provide possible mitigations to these perils.

[161] Ed Morgan, "A Thousand and One Rights," *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*, ed. Ronald Daniels, Patrick Macklem and Kent Roach (Toronto: University of Toronto Press, 2001), 412.

## CHAPTER 5
## RISKS AND REMEDIES

*Though the earth and all inferior creatures be common to all men, yet every man has a property in his own person. This nobody has any right to but himself.*[162]

- John Locke

### OVERVIEW

In his 2002 paper *The Future of Canada's Defense Intelligence*, University of Carleton Professor Martin Rudner claimed that the CAF was in the midst of another Revolution of Military Affairs (RMA).[163] Similar to the 18th century French *levee en masse*, the 19th invention of the machine gun and the 20th century adaptation of nuclear technology, the embrace of 21st century information technology denotes a,

> quantum leap in transforming military organizations, strategy, doctrine, equipment, training, operations, and tactics, so as to accommodate the adoption of new technologies.[164]

In particular, Dr. Rudner believed that the fusion of technology with HUMINT would be the intelligence game changer. This is reinforced by recognition that the traditional reliance on SIGINT was not enough to meet the evolutionary challenges of transnational security threats. In no discipline is this more apparent than in I2.

The rise of I2 and its associated implications has been in concert with quandary that the CAF is now faces as to its role, on behalf of the state, regarding national security. This is based on the seismic shifting of national security responsibilities and the "almost complete

---

[162] John Locke, Quoted in Niels van Dijk, "Property, Privacy and Personhood in a World of Ambient Intelligence" in *Ethics Information Technology* (Springer Science+Business Media, 2009), 58.

[163] Rudner, "The Future of Canada's Defense Intelligence," in *International Journal of Intelligence and Counter-Intelligence* (2002), 541.

[164] Ibid.

disappearance of distinctions between foreign and domestic threats." [165] In turn, this shifting has resulted in the "almost total integration of law enforcement, at all levels of governance, into national security work." [166] Strategically, the national intelligence community as a whole is moving from "response to prevention, aiming to develop knowledge supporting interventions at a far earlier stage."[167]

University of Ottawa Professor Paul Robinson asserted that that the distinction between foreign and domestic intelligence has become "irrelevant." [168] With this in mind, trans-national problems such as organized crime terrorism "cannot be adequately dealt with using domestically acquired intelligence only." [169] Intelligence to support the identification and defeat of these threats must often be gathered outside of Canada. Nationally, the intelligence community recognizes four resulting policy challenges that will impact their future effectiveness: the current weak capacity for coordination within the national intelligence community; the need to reconfigure the strategic approach to collection; and, the introduction of new, cooperative partners in international intelligence. For this discussion, the most important challenge is the fourth one; the accommodation of intelligence collection exigencies with "the principles of law enforcement, privacy rights and civil liberties."[170]

---

[165] Kevin O'Brien, "Managing National Security and Law Enforcement Intelligence in a Globalised World" in Review of International Studies (2009), 903.

[166] Ibid.

[167] Ibid, 904.

[168] Paul Robinson, "The Viability of a Canadian Foreign Intelligence Service," in *International Journal* (Summer 2009), 707.

[169] Ibid.

[170] Martin Rudner, "Contemporary Threats, Future Tasks: Canadian Intelligence and the Challenges of Global Security," in *Canada Among Nations 2002: A Fading Power,* ed. Norman Hillmer and Maureen Appel Molot (Toronto: Oxford University Press, 2002), 19.

**THE RISKS**

There is now a greater expectation that the military contribute to the national security obligations in a way not considered in the pre-modern terrorism era. As one of only two federal departments with an explicit foreign mandate, DND has a unique position towards the legal collection of foreign intelligence. However, the powerful intelligence collection capabilities now available to Canada have prompted valid concerns as to the acceptable balance between, "the requirements of national security and public safety, on the one hand, and privacy rights and civil liberties, on the other."[171] Regarding the use military enabled I2 in particular there arises four main risks: a legal risk, an ethical risk, a philosophical risk and a practical risk.

The legal risk is the perception that information sharing from military to law enforcement in pursuit of domestic judiciary ends is not allowed in Canadian law. The ethical risk, namely that of privacy, is the perception that military collection of identity related information on foreign nationals, without a remedy, is against social norms. The philosophical risk is that mandating and in some ways restricting the CAF to collect evidence rather than strictly intelligence opposes its operational focus and may undermine its treasured freedom of action. Finally, the practical risk is that regardless of the validity of the concept, it just cannot be done efficiently, securely or with available technology. The following will explore each of these risks. It will then answer them with practical remedies that would facilitate the DND's sharing of I2 within the national security community as a legal, ethical, philosophical and practical means of better protecting the state.

---

[171] Ibid, 20.

## LEGAL RISK

As highlighted in Chapter 2, *Identity Intelligence Defined*, the concept of identity is already recognized as a discriminatory device, or shibboleth, in law. As issue is the ongoing "constructive debate regarding the types of [shibboleths] allowed in a constitutional democracy."[172] As intelligence is often portrayed as "a secretive and sometimes subversive activity that is morally ambiguous" and takes its practitioners "close to legal and ethical boundaries," it becomes suspect as a valid evidentiary platform.[173]

There is a healthy tension in modern law regarding identity. Citizens, as independent agents wish often to exercise full control over issues that affect the "various aspects of what we (and others) see as our identities." [174] The tension arises between society's burden to justify identity-related regulation in the face of individual desires and the individual's burden to justify freedom of choice in the face of society's introduction of "identity-threatening […] interventions."[175] This tension becomes supercharged if society's intervention is in contention with something that is recognized as a fundamental right or liberty which at the outset encumbers "the government with justifying what it did, rather than to require the individual to demonstrate the worth of his claim."[176]

---

[172] De Vries, "Identity, Profiling Algorithms and a World of Ambient Intelligence,"...83.

[173] Jerry Radcliffe, *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders, 2nd Edition...*.8.

[174]Michael Shapiro, "The Identity of Identity: Moral and Legal Aspects of Technological Self-Transformation" In *University of Southern California Law Review* (2005), 361. This includes health factors (i.e. the choices in plastic surgery) and characteristics (i.e. the choice to change hair color).

[175] Shapiro, "The Identity of Identity: Moral and Legal Aspects of Technological Self-Transformation"… 361. Society, in this case, is embodied in its government. The two terms will thus be used inter-changeably.

[176] Shapiro, "The Identity of Identity: Moral and Legal Aspects of Technological Self-Transformation"… 363.

Post 9/11 state legislative responses highlighted trepidations from across the political spectrum wherein bolstering of the *Criminal Code*, in particular, did not demonstrate the Right's "confident faith in the traditional criminal law as a secure bulwark against disorder" or the Left's sense that criminal law has only "a limited role in responding to […] social, economic, and political injustices." [177] For both, it weakened society's belief in the importance of restraint in the use of what is the state's "strongest and most coercive instrument."[178] The legal anxiety is embodied in the perception that enhanced cooperation between "seemingly autonomous government structures […] tends to erode consent bases of modern liberal democracies."[179] For I2 and is bulwark, biometrics, this legal transfer of information is acutely sensitive because of the "intimate and irrevocable character of biometric information." [180] This sensitivity is further buttressed by the robust mechanisms for intelligence exchange between Canada and its Allies because "the full legal requirements for biometric information exchange are unknown, especially if the organizations performing the integration operate across borders from each other."[181]

As illustrated in Chapter 4, there exists no explicit restrictions against the use of military intelligence as evidence in Canadian law. In fact, the existence of the umbrella powers of Crown Prerogative permit this to occur in the pursuit of national security. In contrast, there is no explicit legal mechanism in place that articulates how this should occur in way that best protects the interests of military intelligence and law enforcement. The closest example that should govern

---

[177] Roach, *September 11: Consequences for Canada*…24.
[178] Ibid.
[179] Cartier, "Certainty through Flexibility: Intelligence and Paramilitarization in Canadian Public Order Policing,"…24.
[180] Morosan, "Biometric Solutions for Today's Travel Security Problems,"…191.
[181] Ibid.

this sensitive dichotomy is the legal relationship between the RCMP and CSIS. However, though the state has introduced mitigating measures such as privileged officers of the court with security clearances and, trusted agents that can translate intelligence into evidence, officially it remains unresolved in law. This is driven by the opinion that secret intelligence can be seen as "utterly incompatible with the demands of evidence, due process, the presumption of innocence and proof of guilt."[182] Thus, the primary legal challenge is ensuring that, for the use of I2 as evidence, those judicial demands can, in fact, be met.

**LEGAL REMEDY**

The legal use of military enabled I2 will likely be twofold; as part of a judicial prosecution for likely terrorism offenses and as a flag for stringent border security. 'Doing law' is not simply attaining judicial closure *simpliciter* but about

> illuminating the conflicting issues and clashing frameworks within a relevant body of rules, standards, and principles, and setting up at least rough templates for future guidance.[183]

Furthermore, laws governing intelligence collection should provide "the means by which the services are held accountable, including mechanisms of executive control, legislative oversight and judicial review." [184] Therefore, aside from the simple Crown Prerogative caveat, there is scope to further translate the necessary legal mechanism for sharing of military enabled I2 by future adjustments to the following three Parliament of Canada Acts:

---

[182] Kent Roach, "The Eroding Distinction Between Intelligence and Evidence in Terrorism Investigations," in *Counter-Terrorism and Beyond: The Culture of Law and Justice after 9/*11, ed. Nicola McGarrity, Andrew Lynch and George Williams (London: Routledge Taylor and Francis Group, 2010), 63.

[183] Shapiro, "The Identity of Identity: Moral and Legal Aspects of Technological Self-Transformation"… 360.

[184] Cox, "Lighting the Shadows: An Evaluation of Theory and Practise in Canadian Defence Intelligence"…130.

- The *NDA* should be adjusted to assure that the legal authorities and oversight given specifically to CSEC regarding their sharing of SIGINT to "federal law enforcement and security agencies in the performance of their lawful duties" are expanded to include DND's I2 capacity.[185]
- *Public Safety Act* should be adjusted to assure that DND is also included as one of the main agencies involved in the legal sharing of interdepartmental information for transportation or national security purposes.
- *Personal Information Protection and Electronic Documents Act* should be adjusted to assure that DND explicitly has the legal authority to share personal information without consent if it is for "reasons of law enforcement, national security, defense of Canada, [or] conduct of international affairs."[186]

Regarding I2 generated against foreign nationals, the legal remedy is simple. As demonstrated in Chapter 4, Canada already legally accepts that its treatment of foreign nationals will be different from that of its own citizens. Therefore, its national security agencies are not obligated to meet the exacting standards found in the foundational law of the *Canadian Charter of Rights and Freedoms*. Regarding the risk of I2 inadvertently generated against Canadian citizens outside of Canada, the government has gone to great lengths to demonstrate that its current national security legislation is consistent with the Charter as new offenses "did not

---

[185] Canada. *National Defense Act* (R.S.C., 1985, c. N-5), (Ottawa: Parliament of Canada, 2013), Section 273.64 (1) (c).

[186] Department of National Defense, "Highlights of the Public Safety Act, 2002," Last accessed 21 April 2014, http://www forces.gc.ca/en/news/article.page?doc=highlights-of-the-public-safety-act-2002/hnocfnla.

contain any reverse onuses and generally required high levels of subjective fault such as knowledge or purpose."[187]

Regarding the issue of due process, under the *IRPA*, CBSA can already arrest individuals if it "believes the person poses a risk to the public because of past crimes."[188] However, the existence of such entities as the Federal Court, which handles terrorism prosecution on behalf of Canada, and the independent Immigration and Refugee Board of Canada (IRB), which reviews the detention of individuals at the border, provides the necessary oversight to any submitted evidence. For both, individuals are provided with legal representation to assure that their rights are protected and that the state meets its obligations under the law. Further, the existence of these legal remedies assures that the Canadian basic value of presumption of innocence, which burdens the state with proof of guilt, is not waived in the process.

The main challenge, therefore, is meeting the necessary, rigorous demands of evidence. I2, due to the complexities surrounding biometrics in particular, already has evidentiary-esque requirements that are unique to it as an emerging discipline. The associated science is already taken mainly from the experience of forensics and law enforcement thus is institutionally already only slightly removed from the obligations of judicial scrutiny. This can be further remedied by deliberately building the collection of I2 source material around the standards that exist inside the *Canada Evidence Act*. It applies to "all criminal proceedings and to all civil proceedings and other matters" and already governs such legal devices as documentary evidence.[189] Working closely with the RCMP, the military can make best use of lessons learned by law enforcement

---

[187] Roach, *The 9/11 Effect: Comparative Counter-Terrorism*…381.
[188] Canadian Border Services Agency, "Fact Sheet," Last Accessed 21 April 2014, http://www.cbsa-asfc.gc.ca/media/facts-faits/007-eng html.
[189] Canada. *Canada Evidence Act* (R.S.C., 1985, c. C-5), (Ottawa: Parliament of Canada, 1985), Part 1.

with regards to standards for evidentiary collection of such elements as fingerprints or DNA. Further, it can use the standards already set in NDA Section 181, *Rules of Evidence*.[190]

Regarding the inherent tension of protecting secure sources, this can be easily remedied by an axiom that "transparency should be the default position." [191] The goal of transparency is "to open the possibility for the data subject to test the legitimacy of the grounds for decisions affecting him or her."[192] If the conventional military is trained in such legal necessities as the 'chain of evidence' and generation of court acceptable 'subject matter experts', transparency concerning biometric information collection resolves itself as there no longer will exist the military's need to protect its sources from judicial challenge. The limited elements of I2 generated by secure sources such as HUMINT, as long as they met evidentiary standards, would be protected by the remedies found in the *International Relations and National Defense and National Security* Section of the *Canada Evidence Act*.

**ETHICAL RISK - PRIVACY**

The State's careful balance between security and privacy is a difficult and often existential one. As Admiral James Hoy, then Head of the US Transportation Security Agency, said in 2003, "Don't be too quick to strike a balance between privacy and security. As Americans, we are entitled to a full measure of both".[193] Recognizing this pressure, the Federal Office of the Privacy Commissioner stated in a 2011 submission to the Federal *Beyond the*

---

[190] This concerns rules of evidence for the military prosecution in cases concerning military members in military courts.

[191] Wright, Gutwirth and Friedewald, "Shining Light on the Dark Side of Ambient Intelligence," ...56.

[192] Van Dijk, "Property, Privacy and Personhood in a World of AmbientIntelligence" … 67.

[193] Walter Scheirer, "Improving the Privacy, Security, and Performance of Biometric Systems" (Doctoral Dissertation, University of Colorado, 2009), 242.

*Border* Working Group that, "security measures established at both national and international levels have had widespread implications for privacy."[194]

The *Canadian Charter of Rights and Freedoms* takes a moral position as the authoritative text on certain basic values that include equal protection under the law, the security of our persons and, with regards to this discussion, privacy. The problem with modern national security is that in order to provide that security the state now impinges "more heavily on their citizens and require that individuals and groups cede a degree of their freedoms and right to privacy."[195] Furthermore, particularly with the growth of the Information Society, the state is obligated to protect the rights "for all citizens in all their roles (private and professional)" and to create attendant "safeguards and privacy-enhancing mechanisms."[196]

Privacy is viewed as "a selective disclosure of personal information founded on the equilibrium between one's private life and his/her accepted social identity".[197] Having a basis in society's understanding of property, it comes from comes from Latin *proprius* meaning ''one's own."[198] Its modern legal conception was coined by American legal scholars Samuel Warren and Louis Brandeis in their 1890 Harvard Law Review Article *The Right to Privacy* as the "right to be let alone."[199] Ethics and Law author Niels Van Dijk took this further claiming privacy to be the "claim of individuals, groups, or institutions to determine for themselves when, how, and to

---

[194] Canada. Office of the Privacy Commissioner of Canada, *Fundamental Privacy Rights within a Shared Vision for Perimeter Security and Economic Competitiveness* (Ottawa: Government of Canada, 2011), 1.

[195] Tami Jacoby, "Terrorism vs Liberal Democracy: Canadian Democracy and the Campaign Against Global Terrorism," in Canadian Foreign Policy (Spring 2004), 3.

[196] Wright, Gutwirth and Friedewald, "Shining Light on the Dark Side of Ambient Intelligence," ...46.

[197] Morosan, "Biometric Solutions for Today's Travel Security Problems,"…187.

[198] Van Dijk, "Property, Privacy and Personhood in a World of Ambient Intelligence"...58.

[199] Samuel Warren and Louis D. Brandeis, "The Right to Privacy," in the *Harvard Law Review* Vol IV (1890).

what extent information about themselves is communicated to others''[200] These, in turn, can be legally interpreted as "being shielded from the gaze of others" which includes, for the purposes of this discussion, the state. [201]

The privacy challenges in our information age are many: function creep, surveillance without consent, lack of awareness and lack of enforcement.[202] Privacy rights advocates seem most concerned about associated uncertainties about what to protect, lax security on the on the part of those who are supposed to be protecting the data and less than forthright explanations by the state "about the personal data they collect and/or how they use that data."[203] As noted in Chapter 2, this is especially alarming with the collection of the inadvertent or unsanctioned mosaic of ambient intelligence which, with the right analysis, can capture a fairly complete picture of an individual without that individual's explicit consent. In addition, regarding the biometric aspect of I2, concerns are "sometimes exacerbated by the novelty of biometric technology [and] are grounded in […] beliefs about biometric systems' functionality, privacy, trust, and technology anxiety."[204] Further, due to the permanent nature of biometric data, "its theft and misuse may be irreparable" and the unique strength of biometric information or "those unique traits that do not change significantly over a lifetime" are also their Achilles heel. [205]

---

[200] Van Dijk, "Property, Privacy and Personhood in a World of Ambient Intelligence"...63.

[201] Ibid.

[202] Function creep in this sense occurs when date collected for one purpose are used for another (i.e. if the personal information you have provided to a service provider for identity reasons is packaged and sold to another provider for marketing reasons.

[203] Wright, Gutwirth and Friedewald, "Shining Light on the Dark Side of Ambient Intelligence," ...49.

[204] Morosan, "Biometric Solutions for Today's Travel Security Problems,"…185.

[205] Walter Scheirer, "Improving the Privacy, Security, and Performance of Biometric Systems" …246; Abhishek Nagar, "Biometric Template Security" (Doctoral Dissertation, Michigan State University, 2012), 167; and, For instance, if a person's DNA or iris scans are linked to a chronic disease, they may be less able to find affordable medical insurance.

Regarding I2, the primary challenge then is having in place the necessary precautions that maximize protection of the individual from underserved attention and minimize any associated individual anxiety. Paradoxically, this must be done while respecting the state's Orwellian security obligation, "to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."[206] This is complicated by oft hyperbolic justifications such as those opposed are, 'indifferent to terrorism, murder and armed crime, drug smuggling, pedophilia, the plight of children, even plagues.'"[207] To be a success story, "all stakeholders must be cognizant of the threats and vulnerabilities and work together to ensure adequate safeguards exist."[208]

**ETHICAL REMEDY**

The explicit purpose of Canada's *Privacy Act* is to

> protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information.[209]

In order to respect this mandated individual right to privacy, military enabled I2 must be shared using "rules to govern the collection, use and disclosure of personal information."[210] At the same time, the military must respect the premise that intelligence collection is allowed if based on the principles of "fairness, finality, data quality, collection limitation, transparency,

---

[206] Paul Rivard and Joe Faragone, "Privacy and Retention Issues of Defense Intelligence" in Canadian Military Journal (Spring 2007), 86; and, Wright, Gutwirth and Friedewald, "Shining Light on the Dark Side of Ambient Intelligence," ...57.

[207] Roach, *September 11: Consequences for Canada*…10.

[208] Wright, Gutwirth and Friedewald, "Shining Light on the Dark Side of Ambient Intelligence," ...57.

[209] Canada. *Privacy Act* (R.S.C., 1985, c. P-21), (Ottawa: Parliament of Canada, 1983) Section 2.

[210] Rivard and Faragone, "Privacy and Retention Issues of Defense Intelligence"…86.

proportionality, security and accountability."[211] I2 sharing can thus be achieved through four proactive methods to contend with likely privacy issues: oversight, specific policy, training and awareness.[212]

As noted in Chapter 4, DND is currently not beholden to a standalone intelligence oversight body similar to CSIS' SIRC. The closest non-bureaucratic, non-executive oversight is CSEC's Commissioner whose primary responsibility is to "to review the activities of the Establishment to ensure that they are in compliance with the law."[213] Therefore, the state should mandate the creation of a DND Intelligence Review body that would act as the oversight and, if need be, remedy for the sharing of defense intelligence writ large. Its terms of reference could be similar to that of the CSEC Commissioner. In particular, and in respect to the *Security of Information Act*, this body would assure that "the public interest in disclosure outweighs the public interest in non-disclosure."[214]

Section 4 of the *Privacy Act* - Collection, Retention and Disposal of Personal Information, already stipulates that, "no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution."[215] With this in mind, regarding the associated administration and accounting, DND needs to capture in policy clear guidelines for two privacy related issues: types of I2 that can be retained and shared; and destruction of I2. Types of I2 must include both the sources (i.e. TECHINT) and the means of retention (i.e. electronic or hard copies). It must clearly articulate the necessary 'need-to-

---

[211] Van Dijk, "Property, Privacy and Personhood in a World of Ambient Intelligence"...64.
[212] Rivard and Faragone, "Privacy and Retention Issues of Defense Intelligence"…88.
[213] Canada. *National Defense Act* (R.S.C., 1985, c. N-5), (Ottawa: Parliament of Canada, 2013), Section 273.63 (2) (a).
[214] Canada. *Security of Information Act* (R.S.C., 1985, c. O-5), (Ottawa: Parliament of Canada, 1985), Section 15 (1) (b).
[215] Canada. *Privacy Act* (R.S.C., 1985, c. P-21), (Ottawa: Parliament of Canada, 1983) Section 4.

know' and 'authorization-to-know' caveats as well as put in place a transparent tracking mechanism complete with any dictated timelines for disposal or authorization for subsequent use. Ultimately, "…agreements or arrangements with other entities in regard to integrated national security operations should be reduced to writing."[216]

As the necessary extension to new policy and guidelines, DND will have to assure that a robust training apparatus is developed for all DND staff that will deal with I2. The training will have to include not only the practical aspects but also the legal ramifications of non-compliance. This will ensure that DND "prepares, at all levels of leadership, for the type of scrutiny that inevitably will arise."[217] To be truly effective, this internal training must also be paired with vigorous communication with partner agencies, both domestic and international, to assure that they understand DND specific concerns and restrictions. This would better assure that "pivotal importance of constraints, controls and caveats on information and intelligence sharing" is not defeated by inter-department and inter-agency incoherence on privacy.[218]

**PHILOSOPHICAL RISK**

The philosophical risk is in the military's elementary belief that it is not, cannot be in the business of evidence collection but only in the broader, traditional business of intelligence collection.[219] The exacting and time consuming standards of evidentiary proof in pursuit of prosecution go firmly against the rather more interpretive proof necessary for military targeting. This is contrary to the fact that the intelligence actions of our national security community are

---

[216] Cox, "Lighting the Shadows: An Evaluation of Theory and Practice in Canadian Defense Intelligence"…134.

[217] Rivard and Faragone, "Privacy and Retention Issues of Defense Intelligence"…87.

[218] Canada. Office of the Privacy Commissioner of Canada, *Fundamental Privacy Rights within a Shared Vision for Perimeter Security and Economic Competitiveness* (Ottawa: Government of Canada, 2011), 5.

[219] This is aside from the military's collection of evidence in the prosecution of its own members.

moving from response to early prevention. These interventions, through the leveraging of the international and domestic courts system, are in pursuit of judiciary solutions and thus require that the legal instruments such as 'chain of evidence' to be respected in order to be universally useful. Moreover, the development of precise, nonlethal tools such as I2 and its attendant technology for missions where "minimizing fatalities and civilian collateral damage is a priority goal" will facilitate further operational flexibility.[220] Finally, the close interface between the state's military and critical national infrastructure, means that in the modern environment of transnational threats, the military must be involved in the identification of potential violent, domestic threats as a basic means of self-defense.

With these factors in mind, DND can no longer eschew the role it has in comprehensive domestic intelligence and the fight against security threats at home. In fact, Professor Rudner asserted that DND must,

> achieve a more syncretic fusion between political intelligence and traditional military concerns, while also fostering a closer horizontal interoperability with CSIS, as well as other components of Canada's civilian intelligence community, if it is to contribute effectively to intelligence support against asymmetric threats.[221]

This need is further reinforced by the expectation that the military will continue to be involved in future Operations Other Than War (OOTW) that are by design more nuanced and complex that traditional war fighting. As exhibited in Afghanistan, soldiers will be ordered to fill that grey space between outright combat and maintenance of law and order in states without a functioning state authority. This means that they will be cyclically filling military, para-military and badged police functions and thus making dynamic transitions between the use of criminal

---

[220] Rudner, "The Future of Canada's Defense Intelligence," …545.
[221] Ibid, 559.

law and the use of violence as the primary means of coercion. By extension, in support to the national government of any given area of operations, the military may be asked to facilitate evidence collection and subsequent arrest in the absence of competent resident authorities in order to permit "command and control in an otherwise complex multilateral operating environment."[222]

As demonstrated by the mandates given to CSEC, the military is already involved in the collection and distribution of specific, niche intelligence in support to national security. However, the future security environment recognizes that to achieve information superiority, "the future development of Information and Intelligence capabilities for […] will have to promote a more balanced integration of technical and HUMINT sources." Holistic and comprehensive I2 as means of non-lethal, precise targeting, including the detailed effort towards evidence, will be a clear reflection of this balanced integration. The military must protect itself against an "inability to provide the highest value […] by acting alone" and join its "efforts into integrated value chain structures." [223]

**PHILOSOPHICAL REMEDY**

There are mutually reinforcing cultural and procedural remedies to this philosophical risk. Some of the solution is already resident inside the recommendations presented in the legal and ethical risks above, through changes to Canadian Law and by putting in place a demanding process for personal information sharing intra and inter-agency. They are further reinforced by

[222] Ibid, 544.
[223] Morosan, "Biometric Solutions for Today's Travel Security Problems,"…190.

military's prevailing recognition that there needs to be a "closer fusion of the strategic, tactical, and operational dimensions of Defense Intelligence."[224]

The first remedy, cultural, would be a demonstration by DND leadership that DND now is, in fact, in the business of collecting transparent, court acceptable evidence when on expeditionary operations. DND leadership must make it an overriding philosophy, standing order or accepted prerogative that unless there is an explicit time constraint or lethal risk, the CAF would build intervals into its entire future mission planning for evidence collection. Tactical commanders would be institutionally urged to embrace the associated tactical patience that evidence collection will require. Peer agencies will be notified that DND intended to meet a standing commitment to provide to them legally pertinent and sustainable identity intelligence for risks identified outside of Canada. This notification, ideally, will assist in overcoming bureaucratic friction that arises from intelligence bureaucracies "seeking to increase their stature relative to others, promote their interests, and to survive in the political marketplace" that results in miscommunication or no communication at all.[225]

The second remedy, procedural, will be the creation and enshrinement of related Tactics, Techniques and Procedures (TTPs) for the collection of evidence by the conventional forces.[226] Commanders and staff will be obligated to assure that selected CAF members had the training and tools to meet the demands of evidence collection. DND JAG would create a peer reviewed

---

[224] Rudner, "The Future of Canada's Defense Intelligence," …557.

[225] David Mastro, "Cognitions of the Community: The Worldview of U.S. Intelligence" (Doctoral Dissertation, West Virginia University, 2008), 2.

[226] This is focused primarily on conventional forces such as dismounted infantry or a naval boarding party. The military police, by institutional design, and the Special Forces, by operational need, have already evolved robust evidence collection procedures.

aide-memoire for use at all levels the gives clear guidelines where legally acceptable and explicit instruction as to how to collect evidence that will stand up to basic judicial scrutiny.

**PRACTICAL RISK**

In the military's pursuit of information superiority, collected data , "must be synthesized so that they may be processed into actual intelligence, assessed, and delivered to intended users..."[227] The final risk, therefore, is that the production of effective, evidentiary I2 is beyond the scope of the military. Associated apprehension springs from three facets; information overload, interoperability and the absence of efficient and affordable technology. Regarding I2, the primary goal of "accurate authentication" is perceived to be not presently achievable with the ways and means available.[228]

Anecdotally, the weak link in I2 is "intelligence analysis, rather than collection failure."[229] This highlights a truism of intelligence in general that collection outweighs assessment.[230] This imbalance is only increasing in our information age as analysis is now required on "an ever-widening and – deepening data-set derived from a dramatic increase in community intelligence, from an expanded set of 'individuals of interest'..."[231] Identity matching in intelligence and law enforcement also "suffers greatly from the missing data problem" wherein inter and intra database referencing is weakened by an inability to compare 'same/same'

---

[227] Rudner, "The Future of Canada's Defense Intelligence," …543.
[228] Morosan, "Biometric Solutions for Today's Travel Security Problems,"…189.
[229] Robison, "The Viability of Canadian Foreign Intelligence,"…707.
[230] This is particularly true for modern, Western militaries where their vast technological capacity in such disciplines as SIGINT and IMINT produces endless raw data that goes consistently unevaluated due to a lack of analysis resources.
[231] O'Brien, "Managing National Security and Law Enforcement Intelligence in a Globalized World"…914.

components thus precluding easy correspondence. [232] Then CSIS Director, Jim Judd, expressed this concern in what he called the coming of the 'Information Tsunami.'[233]

This concern is bolstered by difficulties in associated system interoperability. Complete interfacing of DI is challenged by the complexity of the "data base and the multiplicity of types of sensors, storage, and retrieval systems available for information operations."[234] Protecting system confidentiality and integrity is made difficult in cross network programming necessary for interagency information sharing due to "possible conflict of interests between communicating entities; network convergence; [and], large number of ad hoc communications." [235] Though alluded to in the 2004 National Security Policy *Securing an Open Society*, Public Safety Canada has only recently begun to take steps to,

> consolidate the Government's information technology security architecture, in order to improve the security of Government networks and to work with partners to promote Canada's interest in a cyberspace that is open, interoperable, secure, and reliable.[236]

Thirdly, there is a perception that capable identity collection technology that has the ability gather information "accurately, rapidly, reliably, cost effectively, in a user friendly manner" do not yet exist.[237] This is particularly true for the unique needs of the military in that it wants technology that is easy to use, easy to maintain and can survive the demanding conditions

---

[232] Li,Wang and Chen, "Identity Matching Using Personal and Social Identity Features"…103. For instance, if one data base has a name that it matches to the same name in another database, it cannot affirm the match without additional personal information such as Date of Birth.

[233] O'Brien, "Managing National Security and Law Enforcement Intelligence in a Globalized World"…914.

[234] Rudner, "The Future of Canada's Defense Intelligence," …544.

[235] Wright, Gutwirth and Friedewald, "Shining Light on the Dark Side of Ambient Intelligence," ...50.

[236] Public Safety Canada, "Action Plan 2010-2015 for Canada's Cyber Security Strategy," Last accessed 21 April 2014, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx.

[237] Umut Uludag, "Secure Biometric Systems" (Doctoral Dissertation, Michigan State University, 2006), 1.

of military operations. Further, it must demonstrate intrinsic value to which the military can recognize, such as immediate identity authentication, or it gets left behind by otherwise frustrated soldiers.

**PRACTICAL REMEDY**

The remedy for this risk is also tied up with awareness and training. The analysis delta will be partly served by the consequential increase in "mass data crunching and analysis" that will result from the ubiquity of available communication technology and growth in such elements as Bayesian Logic expertise. [238] Further, similar to the evolution within in the US military intelligence community, DND's recognition of the emerging importance of I2 as its own discipline may obligate an increase in resourcing or, at least, prioritizing of I2 efforts. I2 needs to therefore be reflected in the next iterations of any DND intelligence doctrine.

Regarding interoperability and security of information systems, DND will need to continue to be a key partner in implementing Canada's Cyber Security Strategy and its associated Action Plans. In particular, DND must continue to assist in "securing Government systems [and] partnering to secure vital cyber systems."[239] Cyber security will continue to be a pressing issue of national importance for which "given the interconnected nature of our systems and networks, we have a shared responsibility and accountability."[240] DND, as an active partner, will then be able to assure that the DND systems that enable I2 storage will have the necessary secure

---

[238] O'Brien, "Managing National Security and Law Enforcement Intelligence in a Globalized World"…914.

[239] Canada. Public Safety Canada, *Action Plan 2010 – 2015 for Canada's Cyber Security Strategy*, (Ottawa: Government of Canada, 2013) 1.

[240] Ibid, 2.

interfacing with partner agencies such that the information sharing risk is mitigated if not eliminated.

The existence of supporting technology that meets the distinct collection requirements of the military is no longer a risk. The next generations of such instruments as the US Biometrics Automated Toolset System (BATS) that collects "fingerprints, iris scans, facial photos and biographical information of persons of interest" and includes technology to conduct standoff comparison to existing multiagency databases demonstrates that the tactical technology is already in use.[241] Similar user-friendly hand held devices, such as the Tactical Biometrics Collection and Matching System (TBCMS) are also in use by Naval Boarding Parties. This technology is, in turn, supported by the creation of the military's own deployable Level II Forensic Laboratories which house the most cutting edge expertise in fingerprint and DOMEX analysis along with lasers, gas chromatography and DNA extraction.[242] They can conduct "extensive scientific analysis and testing, often producing biometrically identifiable samples that will support positive matches for identification purposes."[243] These laboratories are also capable of producing analysis that would meet the burden of judiciary scrutiny and thereby would stand up if ever challenged.

A final, modest pragmatic solution is to determine the information parameters of CBSA requirements for its individual lookout information reports that flag its agents towards incoming

---

[241] United States, Department of the Army, *Biometrics Task Force Presentation - Biometric Automated Toolset (BAT) and Handheld Interagency Identity Detection Equipment (HIIDE),*19 September 2007. BATS and its technological sibling the Handheld Interagency Identity Detection Equipment (HIIDE) were omnipresent in Afghanistan from 2008 onwards. Canadian soldiers used them as a means of base security.

[242] In Afghanistan, the Canadian Level II Laboratory was called the Multi-Disciplinary Exploitation Capability (MDEC). American versions were called Combined Explosives Exploitation Cell or Joint Expeditionary Forensics Facility. At one point, Kandahar Airfield had no less than eight laboratories of similar style and capabilities.

[243] David Pendall and Cal Sieg, "Biometric-enabled Intelligence in Regional Command–East," in *Joint Force Quarterly* (1st Quarter 2014), 71.

security risks. CBSA uses intelligence from "various intelligence and law enforcement agencies, and is received in the form of either electronic transfers of data or other forms of communication."[244] As the primary means of apprising border security, these CBSA forms should then become the defacto template for military enabled I2. They should, in turn, inform the subsequent creation of all associated I2 hardware and software such that the military can deliver what its fellow domestic security customers require.

**SUMMARY**

American Professor, Walter Scheirer, in his doctorate thesis *Improving the Privacy, Security, and Performance of Biometric Systems*, stated the "The [identity] dilemma is a very real and dangerous threat facing the entire globe today." [245] This dilemma, also faced by DND as a key member of Canada's security community, is compounded by very real legal, ethical, philosophical and practical risks that challenge its ability to share its I2. Professor Robison reinforced these risks stating that,

> Successive governments have understandably spent hundreds of millions of dollars on bolstering our security, but they have spent little on protecting our rights from the potential abuses that may take place due to the expanding powers granted to our national security agencies.[246]

The legal risk lies in the fact the transfer of I2 between DND and other Canadian security agencies in the potential pursuit of judicial prosecution is not resolved in law and is only captured by the, umbrella permission allowed under the Crown's Prerogative. This can be

---

[244] Office of the Auditor General of Canada, *Status Report of the Auditor General to the House of Commons – 2009…*28. For example, CSIS data on long-term lookouts are electronically transmitted on a weekly basis to Citizenship and Immigration Canada (CIC) and CBSA. They are updated as new information is received and reviewed every two years for applicability.

[245] Walter Scheirer, "Improving the Privacy, Security, and Performance of Biometric Systems"…248.

[246] Robison, "The Viability of Canadian Foreign Intelligence,"…715.

remedied by legislative changes to the *NDA*, the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act.* The ethical risk lies in privacy concerns and whether the military should be sharing I2 gleaned from non-consensual sources. It is remedied by increases in oversight, policy, training and awareness to maximize transparency and minimize incoherence. The philosophical risk is in the military's longstanding belief that it collects only intelligence and is not in the business of collecting evidence. It can be remedied culturally by Senior DND leadership overcoming this conviction and making evidence collection a standing task on any future expeditionary operation. It can be remedied procedurally by changes to TTPs and training including a DND JAG endorsed aide-memoire. The practical risk is that, regardless of the hypothetical discussion, I2 cannot be collected or shared because our systems are not compatible, secure or mature enough to allow it. This risk is remedied by ongoing DND efforts to securely harmonize DND systems with those of the other national security agencies and by the existence of proven collection and analysis technology that can produce court acceptable effects.

The final issue is not a risk as much as a consideration. DND has to chase the difficult equilibrium that surrounds all intelligence collection and not just I2. Information gathering, as individuals or organizations, is universally prone to 'naïve empiricism' or the mistaken belief that "that more information will automatically lead to becoming better informed."[247] With this in mind, I2 done to judicial standards, within an accepted legal framework, on secure means and shared efficiently can reduce this empiricism and better inform Canada's declared intention of,

[247] Peter Gill, "Making Sense of Police Intelligence? The Use of a Cybernetic Model in Analysing Information and Power in Police Intelligence Processes" in *Policing and Society: An International Journal of Research and Policy* Vol. 8 (1998), 307.

delivering excellence at home, meeting its commitments as a reliable partner in the defense of North America, and projecting leadership abroad in support of international security.[248]

[248] Canada. Department of National Defense, *Canada First Defense Strategy* (Ottawa: Government of Canada, 2004), 21.

## CHAPTER 6 - CONCLUSION

> *It is important for peace and defense that those who have the responsibility to give just judgments of disputes, to detect the Designs of neighboring states, to conduct war prudently and to look out for the commonwealth's interests all around, should perform their duties properly*.[249]
>
> \- Thomas Hobbes

The Canadian state's biggest obligation and most complex responsibility is the provision of security to its citizens. This must be done while remaining honest to its fundamental principles of individual agency and rule of law. In doing this, it is faced with two distinct challenges. First, it must find the equilibrium between a citizen's right to privacy and the state's need for information. Second, it must determine the extent of its authority over the citizens of other countries in pursuit of its own national security. Noted legislator and academic Irwin Cotler in his article 'Thinking Outside the Box: Foundational Principles for a Counter-Terrorism Law and Policy' asserted that the required approach must seek to "protect both national security – or the security of democracy if not democracy itself – and civil liberties."[250] The focal peril in both is the danger of over-reach wherein it consciously uses its broader powers permissible against non-citizens outside of Canada against Canadian citizens who are protected against such broader powers. This creates a very difficult security paradox. This is most recently and glaringly represented in how Canada should now treat the Canadian nationals involved in a terrorist attack against an Algerian oil factory in April 2013.[251] As Canadian citizens, these individuals are entitled to all the protections inherent in Canadian law however, much like the tribulations

---

[249] Thomas Hobbes, *On the Citizen,* ed. and trans.R. Tuck and M. Silverthorne (Cambridge: Cambridge University Press, 1998), 78 – 80.

[250] Irwin Cotler, "Thinking Outside the Box: Foundational Principles for a Counter-Terrorism Law and Policy" in *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*, ed. R.J. Daniels, P. Macklem and K. Roach, 111 (Toronto:University of Toronto Press, 2001).

[251] Canadian Broadcasting Corporation, "Canadians in Algeria Attack Went Overseass With 3rd Man," Last accessed 30 April 2014, http://www.cbc.ca/news/canada/canadians-in-algeria-attack-went-overseas-with-3rd-man-1.1383022.

surrounding Omar Khadr's repatriation from American military imprisonment, their identification as terrorists makes them politically sensitive. This paradox may be further inflated if intelligence is unknowingly collected against innocent Canadians abroad that results in them suffering such future restrictions as inadmissibility into other countries or even back into Canada. This continues to be demonstrated by Canadian citizen Shahid Mahmood's unintended addition to the US No Fly List.[252] Therefore, the state must put in place as transparent a security structure as feasible within the confines of protecting state intelligence sources. It must "strike the right balance between security and liberty."[253] Further, it must also have in place legal remedies that permit Canadian citizens to challenge the state's use of its authority in both the domestic and foreign spheres.

The military, as one of the primary tools of foreign policy and therefore also a primary instrument of foreign intelligence collection, faces a unique challenge in assisting the state to meet its security tasks. Traditionally, the military held itself as only an intelligence collector and thus beholden only to the more expansive rules permitted for intelligence. However, technological and societal evolutions have now created the conditions where the military may be expected to collect evidence, to the detailed and rigid levels expected under Canadian evidentiary laws. The military, uniquely in its history, is now obligated to assist the state in producing the transparency referred above such that the state can best find solutions to its security paradox. This means it must be more tightly joined to the other mechanisms of state security particularly

---

[252] The Toronto Star, "Canada Refuses To Give Answers About Getting Off Of No Fly List," Last accessed 30 April 2014, http://www.thestar.com/opinion/commentary/2014/01/25/canada_refuses_to_give_answers_about_getting_off_nofly_list.html.

[253] Gregory Treverton, "Terrorism, Intelligence and Law Enforcement: Learning the Right Lessons"" in *Twenty-First Century Intelligence*, ed. Wesley Wark (New York: Routledge Taylor & Francis Group, 2005), 138.

regarding interagency information sharing. In essence, the military must now be prepared to cross the habitual Rubicon drawn between intelligence and evidence.

This historically distinctive situation is arising acutely in the domain of the new intelligence discipline known as Identity Intelligence (I2). Identity is primarily the contextual understanding of oneself as well as a means of separating one individual from another. Intelligence is primarily the collection and analysis of information in order to better inform policy. Taken together, I2 provides a means of authentication and a means of filtration. Through its sources in HUMINT, MASINT, OSINT and SIGINT and applications such as BEI, FEI and DOCEX, it gives the state, the extraordinary ability to effectively pull individuals out of a crowd. It can well assist modern state security policies and thus must be fully integrated as a viable but legal instrument to screen the good guys from the bad. However, this must be done in a manner that is candid to Canadian laws and does not undermine state legitimacy or citizen rights.

As it continues to refine its methodology in finding this balance, Canada can look to the example presented by its main Allies; the US, the UK and Australia. Like Canada, all three are open, democratic states beholden to fundamental principles and individual rights. Further, all three follow the doctrine of Common Law and thus legal lessons learned in one country can be referred to in Allied laws. In addition, Canada, the UK and Australia all make use of the awesome power of Crown Prerogative as a means of pursing state security in ways not reflected in binding legislation. Though the US, through the actions taken via its *USA PATRIOT* Act, appears to have robust integration powers across all of its security agencies, it still has legal and philosophical restrictions with the use of military enabled intelligence as evidence. The UK, often looked to by Canada as a leader on state security related legislation, appears to be most comfortable with interagency information sharing and the use of the military in domestic security

interests. This is due primarily to the lessons drawn by centuries of colonialism and by its residual domestic terrorist threat. Australia is very close to the Canadian perspective in that it saw a very rapid maturation of its state security policies post-9/11. The key lessons drawn from the study of all three include: the need for a standalone foreign security agency to better manage the line between foreign and domestic intelligence; the empowerment of a distinctive intelligence executive authority to better coordinate interagency information sharing; and, the reinforcement of an interagency intelligence oversight authority, including adding to privacy laws, to be the check on state over-reach.

The current Canadian approach to state security is "an all risks approach [that] has the potential to stress the common interest shared by all Canadians in responding to a wide range of threats."[254] It is driven by fallout following three seminal events: the FLQ crisis and its attendant rise of domestic security intelligence as separate from law enforcement; the Air India bombing and its attendant clarity on the intelligence and law enforcement information sharing divide; and, 9/11 and its attendant pressure for Canada to reinforce its state security in parallel with the US. These have resulted in various changes to the state security infrastructure including the creation of CSIS and the increased use of border control as a means of state security. Collectively, they pressurized the debate surrounding the state's reach on intelligence collection and interagency information sharing. However, after more than a decade of legislative expansion, the state's laws have only relatively recently been challenged in court to prove their worth. These challenges, most notably those surrounding the vexing circumstances of Canadian citizen Maher Arar, have forced the state to refine its approach. It has since put in place such remedies as the introduction

---

[254] Roach, *The 9/11 Effect: Comparative Counter-Terrorism* …425.

of trusted agents to translate the divide between intelligence and evidence and the permitting of classified information access to privileged representatives within the judicial system. In this legal environment, there are currently no legal restrictions to military intelligence to becoming evidence. However, aside from the broad authorities allowed under Crown Prerogative there are also no explicit legal mechanisms to transparently permit this to happen. With this in mind, the military continues to have reservations rendered through the perception of four main risks; legal, ethical, philosophical and practical.

The military's perceived legal risk is the belief that aside from the authorities already given in the *NDA* for niche DND capabilities to collect domestic intelligence against foreign nationals in support to other agencies, it is against Canadian law for military enabled intelligence to be shared as potential evidence. This is, in fact, not true however there are steps to remedy this apparent risk including simple adjustments to the *NDA*, *Public Safety Act* and *Personal Information Protection and Electronic Documents Act* in order to better reflect DND as one of the main agencies in domestic security and to encompass military enabled I2 as a source of domestic security intelligence. Also, in order to meet the demands of the *Canada Evidence Act*, all I2 should be collected in a transparent manner consistent with that of law enforcement including the respect for 'chain of evidence' caveat and nomination of court acceptable 'subject matter experts' to speak with authority on I2 evidence.

The ethical risk lies in the implicit Canadian right to privacy. Individuals should not be subject to inadvertent or direct collection of private information without their explicit consent and individual privacy is protected inside the *Privacy Act*. The challenge, from a state security perspective, is how to put in place the necessary measures that maximize protection from undeserved state attention without restricting access to necessary security related information.

For military enabled I2, the remedy would require four steps; oversight, specific policy, training and awareness. Oversight would be in the creation of a Defense Intelligence Review Board similar to CSIS' SIRC that would become the check and, if necessary, remedy to potential privacy infringement. Specific policy would be in the creation of I2 guidelines and procedures that cover the arcs of what can and cannot be collected and eventual I2 disposal. Training would be in the creation of a robust instructional apparatus that would follow from the introduction of new guidelines and procedures. Finally, to minimize privacy related incoherence, awareness arises in clearly demonstrating to domestic and international partner agencies, the military's specific I2 restrictions.

The philosophical risk arises from the customary belief that the conventional military does not collect evidence. It stems from a belief that the exhaustive detail and by extension time required would undermine military operations. Furthermore, the 'clean' aspect of evidence collection unnecessarily handcuffs the military in ways that its traditional intelligence collection does not. Though some of these concerns are answered elsewhere in remedies to the legal and ethical risks, the philosophical risk can be remedied by cultural and procedural changes. The cultural one would be a clear communication by DND leadership that it is now in the business of transparent evidence collection and thus, aside from situations of lethal danger, the military would make the time necessary to do the detailed work of evidence collection. The procedural one would be in the creation of related TTPs supported by a JAG blessed aide-memoire and a comprehensive training framework.

The practical risk is captured in the belief that a robust value chain does not yet exist that would enable a transition of military intelligence to court acceptable evidence. There are distinct hurdles, namely database interfacing, analytical capacity and user friendly technology. These can

be remedied through DND's continued, active participation in interagency systems harmonization, the DND acceptance of I2 as an analytical priority and the involvement of DND Research and Development in the ongoing evolution of I2 collection and examination tools such as those proven in Afghanistan. Additionally, all I2 input and output templates should be built in accordance with needs of partner agencies such as that required for CBSA's lookout information.

In short, military enabled I2 has the potential to become a powerful tool in national security especially in its ability to pull individuals from a crowd and as a means of border security. Its gradual but deliberate maturity would amplify the then PCO Executive Director of the International Assessment Staff, Greg Fyffe assertion that, "the building of an efficient, reliable and recognized [intelligence] community capability will be the on-going work of the coming decade—and more."[255] If its I2 capability is buttressed by adjustments to existing Canadian law, additional oversight, expansive guidelines, comprehensive training, and proactive merging of evolving technology, the military will be able to meet the demands of due diligence regarding transparency and court acceptability. In doing so, DND will reinforce the mandate set out in the Canada First Defense Strategy that first and foremost the military must "ensure the security of our citizens."[256]

## RECOMMENDED FUTURE STUDY

Though this analysis has touched already, at least tangentially, on the following two recommended topics for future study, there is still a wealth of work to be examined. Doing so

---

[255] Greg Fyffe, "The Canadian Intelligence Community After 9/11" in *Journal of Military and Strategic Studies*, Volume 13, Issue 3 (Spring 2011), 17.

[256] Canada. Department of National Defense, *Canada First Defense Strategy* (Ottawa: Government of Canada, 2004), 7.

would further synchronize the efforts of DND and its partner agencies regarding I2 and domestic security.

The first recommended topic is technology related and would involve a detailed analysis of the existing pan-government communications systems and databases with a view to recommending how to best harmonize I2 collection and interagency information sharing.

The second recommended topic is training related and would involve a detailed analysis of how law enforcement, including the Military Police, conducts evidence collection. This would then inform future conventional military training such that all the existing associated Canadian norms and standards are realized within the military when it conducts future operations.

## BIBLIOGRAPHY


Ackerman, Robert. "Cyber Tasks Intelligence Community." In *Signal*. (March 2010): 29 - 31.

Austin, Lisa. "Is Privacy a Casualty of the War on Terrorism?." In *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*. Edited by Ronald Daniels, Patrick Macklem and Kent Roach. Toronto: University of Toronto Press, 2001.

Bell, Collen. *The Freedom of Security: Governing Canada in the Age of Counter Terrorism*. Toronto: UBC Press, 2011.

Brey, Phillip. "Freedom and Privacy in Ambient Intelligence." In *Ethics and Information Technology* Springer Science+Business Media (2006): 161 – 163.

Bush, George W. Speech quoted in David Alex Mastero II**.** "Cognitions of the Community: The Worldview of U.S. Intelligence. Doctoral Dissertation, West Virginia University, 2008.

Cartier, Brad. "Certainty through Flexibility: Intelligence and Paramilitarization in Canadian Public Order Policing." Doctoral Thesis. University of Ottawa. 2012: 6 – 8.

Clement, Andrew, Krista Boa, Simon Davies and Gus Hosein. "Towards a National ID Card for Canada? External Drivers and Internal Complexities." In *Playing the Identity Card: Surveillance. Security and Identification in Global Perspective*. Edited by Colin J. Bennett and David Lyon. London: Routledge Taylor & Francis Group. 2008.

Cooper, Barry. *CFIS: A Foreign Intelligence Service for Canada.* Calgary: Canadian Defense and Foreign Affairs Institute. 2007: 50 - 52.

Cordner, Gary and Kathryn Scarborough. 'Information Sharing: Exploring the Intersection of Policing with National and Military Intelligence.'' In *Homeland Security Affairs* Volume VI, No. 1 ( January 2010): 14 – 16.

Cotler, Irwin. "Thinking Outside the Box: Foundational Principles for a Counter-Terrorism Law and Policy." In *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*. Edited by R.J. Daniels, P. Macklem and K. Roach. Toronto: University of Toronto Press, 2001.

Cohen, Stan. "Concluding Comments from the Department of Justice." In *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*. Edited by Ronald Daniels, Patrick Macklem and Kent Roach. Toronto: University of Toronto Press, 2001.

Cohen, Stanley. Review of *The 9/11 Effect: Comparative Counter-Terrorism* by Kent Roach. In *Canadian Criminal Law Review* Vol. 17 (2011).

Cox, James. "Lighting the Shadows: An Evaluation of Theory and Practise in Canadian Defense Intelligence." Doctoral Dissertation, Royal Military College of Canada, 2011.

Cox, Joseph. “DOMEX: The Birth of a New Intelligence Discipline.” In *Military Intelligence* (April – June 2010): 21 - 23.

De Vries, Katja. “Identity. Profiling Algorithms and a World of Ambient Intelligence.” In *Ethics and Information Technology* Springer Science+Business Media (2010): 73 – 83.

Dubin, Cindy.”Biometrics Hands Down.” In *Security Magazine,* February 2011: 53 – 55.

Eaton, Joseph. *The Privacy Card: A Low Cost Strategy to Combat Terrorism.* New York: Rowman & Littlefield Publishers. Inc., 2003: xxii – xxiv.

Farson, Stuart and Reg Whitaker. ‘Canada’ in *PSI Handbook for Global Security and Intelligence National Approaches Volume 1: The Americas*. Edited by Stuart Farson, Peter Gill, Mark Phythian and Shlomo Shpiro Westport. Connecticut: Praeger Security International, 2008.

Filmer, Alice. “The Acoustics of Identity: Linguistic Passports Beyond Empire and Essentialism.” Doctoral Dissertation. University of Illinois. 2008.

Forcese, Craig. “Canada’s National Security Complex: Assessing the Secrecy Rules.” In *IRPP Choices* Vol. 15 No. 5 June 2009: 1 - 9.

Fyffe, Greg. “The Canadian Intelligence Community After 9/11.” In *Journal of Military and Strategic Studies*, Volume 13, Issue 3 (Spring 2011): 16 - 18.

Gill, Peter. “Making Sense of Police Intelligence? The Use of a Cybernetic Model in Analysing Information and Power in Police Intelligence Processes.” In *Policing and Society: An International Journal of Research and Policy* Vol. 8 (1998): 303 – 307.

Herman, Michael. “Counter-Terrorism. Information Technology and Intelligence Change.” In *Twenty-First Century Intelligence: Studies in Intelligence*. Edited by Wesley Wark. London: Routledge Taylor and Francis Group, 2005: 53 - 55.

Hurley, Matthew. “For and from Cyberspace: Conceptualizing Cyber Intelligence. Surveillance. and Reconnaissance.” In *Air & Space Power Journal* (November – December 2012): 13 - 15.

Iasso, Anthony. “A Critical Time for Biometrics and Identity Intelligence.” In *Military Intelligence* (July – September 2013): 37 - 39.

Jacoby, Tami. “Terrorism vs Liberal Democracy: Canadian Democracy and the Campaign Against Global Terrorism.” In *Canadian Foreign Policy* (Spring 2004): 2 – 4.

Kent, Sherman. Quoted in Bryce Offenberger. “The Way Forward: Reforming Canada’s Foreign

Intelligence Community." Master's Thesis, University of Manitoba, 2012.

Li, Jiexun. Alan Wang and Hsinchun Chen. "Identity Matching Using Personal and Social Identity Features." in *Information Systems Front* Springer Science+Business Media, (2010) 1 - 2.

Locke, John. Quoted in Niels van Dijk. "Property. Privacy and Personhood in a World of Ambient Intelligence." In *Ethics and Information Technology.* Springer Science+Business Media (2009).

Lyon, David and Colin J. Bennett. "Playing the ID Card: Understanding the Significance of Identity Card Systems." In *Playing the Identity Card: Surveillance. Security and Identification in Global Perspective*. Edited by Colin J. Bennett and David Lyon London: Routledge Taylor & Francis Group, 2008.

Macklin, Audrey. "Borderline Security in Essays on Canada's Anti-Terrorism Bill." In *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*. Edited by R.J. Daniels. P. Macklem and K. Roach. Toronto: University of Toronto Press, 2001: 382 - 384.

Major, John. *Opening Remarks On the release of the Report of the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182*. Ottawa: Government of Canada, 2010.

Mastero, David Alex**.** "Cognitions of the Community: The Worldview of U.S. Intelligence" Doctoral Thesis, West Virginia University, 2008.

Morgan, Edited by by "A Thousand and One Rights." *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*. Edited by Ronald Daniels, Patrick Macklem and Kent Roach. Toronto: University of Toronto Press, 2001: 411 - 413.

Morosan, Cristian. "Biometric Solutions for Today's Travel Security Problems." In *Journal of Hospitality and Tourism Technology* Vol.3 No. 3, 2012: 178 – 191.

Nagar, Abhishek. "Biometric Template Security." Doctoral Dissertation, Michigan State University, 2012.

O'Brien, Kevin. "Managing National Security and Law Enforcement Intelligence in a Globalized World." In *Review of International Studies* (2009): 903 - 914.

Offenberger, Bryce. "The Way Forward: Reforming Canada's Foreign Intelligence Community." Master's Thesis, University of Manitoba, 2012.

Pendall, David and Cal Sieg. "Biometric-enabled Intelligence in Regional Command–East." In *Joint Force Quarterly (*1st Quarter 2014): 70 - 72.

Radcliffe, Jerry. *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders. 2nd Edition.* Washington: US Department of Justice, 2007: 7 - 9.

Ransom, Harry Howe. Quoted in Peter Gill. "Making Sense of Police Intelligence? The Use of a Cybernetic Model in Analyzing Information and Power in Police Intelligence Processes." In *Policing and Society: An International Journal of Research and Policy* Vol. 8 (1998).

Richards, Julian. *A Guide to National Security: Threats. Responses and Strategies.* Oxford: Oxford University Press, 2012.

Rivard, Paul and Joe Faragone. "Privacy and Retention Issues of Defence Intelligence." In *Canadian Military Journal* (Spring 2007): 86 - 88.

Roach, Kent. "The Eroding Distinction Between Intelligence and Evidence in Terrorism Investigations." In *Counter-Terrorism and Beyond: The Culture of Law and Justice after 9/11*. Edited by by Nicola McGarrity, Andrew Lynch and George Williams. London: Routledge Taylor and Francis Group, 2010.

Roach, Kent. *September 11: Consequences for Canada*. Kingston: McGill-Queen's University Press, 2003.

Roach, Kent. *The 9/11 Effect: Comparative Counter-Terrorism*. New York: Cambridge University Press, 2011.

Robinson, Paul. "The Viability of a Canadian Foreign Intelligence Service." In *International Journal* (Summer 2009): 706 – 708.

Rudner, Martin. "Contemporary Threats. Future Tasks: Canadian Intelligence and the Challenges of Global Security." In *Canada Among Nations 2002: A Fading Power.* Edited by Norman Hillmer and Maureen Appel Molot. Toronto: Oxford University Press, 2002.

Rudner, Martin. "The Future of Canada's Defense Intelligence." In *International Journal of Intelligence and Counter-Intelligence (*2002): 541- 557.

Sales, Nathan. "Mending Walls: Information Sharing After the USA PATRIOT Act." In *Texas Law Review* (July 2010): 1813 - 1819.

Sathye, Milind and Chris Patel. "Developing Financial Intelligence: An Assessment of the FIUs in Australia and India." In *Journal of Money Laundering Control* Vol. 10 No. 4 (2007): 390 - 392.

Scheirer, Walter. "Improving the Privacy. Security. and Performance of Biometric Systems" Doctoral Dissertation, University of Colorado, 2009: 242 - 248.

Shapiro, Michael. “The Identity of Identity: Moral and Legal Aspects of Technological Self-Transformation.” In *University of Southern California Law Review* (2005): 360 - 363.

Stanton, Louise. “The Civilian-Military Divide: Obstacles to the Integration of Intelligence in the United States.” Doctoral Thesis, State University of New Jersey, 2007.

Stevens, Alfred Denning. *The Hamlyn Lectures First Series: Freedom Under the Law*. Toronto: The Carswell Company Ltd, 1949.

Thomas Hobbes. *On the Citizen.* Edited by and translated R. Tuck and M. Silverthorne. Cambridge: Cambridge University Press, 1998.

Treverton Gregory, “Terrorism, Intelligence and Law Enforcement: Learning the Right Lesson.” In *Twenty-First Century Intelligence*. Edited by Wesley Wark. New York: Routledge Taylor & Francis Group, 2005.

Tzu, Sun. *The Art of War*. Edited by Samuel Griffith. 149. Oxford: Oxford University Press, 1963.

Uludag, Umut. “Secure Biometric Systems” Doctoral Dissertation, Michigan State University, 2006.

Van Dijk, Niels. “Property. Privacy and Personhood in a World of Ambient Intelligence.” In *Ethics and Information Technology* Springer Science+Business Media (2009): 57 - 67.

Warren, Samuel and Louis D. Brandeis. “The Right to Privacy.” In the *Harvard Law Review* Vol IV (1890).

Washington, George. Quoted in Nathan Sales. “Mending Walls: Information Sharing After the USA PATRIOT Act.” In *Texas Law Review* (July 2010): 1851 - 1853.

Williams, George. “A Decade of Australian Anti-Terrorism Laws” in *Melbourne University Law Review* Vol. 35 (2011): 1138 - 1140.

Wright, David, Serge Gutwirth and Michael Friedewald. “Shining Light on the Dark Side of Ambient Intelligence.” In *Foresight* Vol. 9 No. 2 (2007): 46 - 57.

Woodward, John, Katharine Webb, Elain Newton, Melissa Bradley and David Rubenson. *Army Biometrics Applications: Identifying and Addressing Sociocultural Concerns.* Pittsburgh: Rand, 2001.

**INTERNET SOURCES**


Australian Security Intelligence Organization. "About ASIO." Last accessed 17 March 14. http://www.asio.gov.au/asio-and-national-security/units/ntac.html.

Australian Department of Defence. "What We Do." Last accessed 17 March 2014. http://www.defence.gov.au/dio/what-we-do.shtml..

Australian Department of the Prime Minister and Cabinet. "Independent National Security Legislation Monitor." Last accessed 17 March 2014. http://www.dpmc.gov.au/INSLM/index.cfm.

Booz Allen Hamilton. "Identity Biometric Enabled Intelligence." Last accessed 23 April 2014. https://www.boozallen.com/consulting/technology/cyber-security/identity/identity-biometric-enabled-intelligence.

Canadian Border Services Agency. "Fact Sheet." Last Accessed 21 April 2014. http://www.cbsa-asfc.gc.ca/media/facts-faits/007-eng.html.

Canadian Broadcasting Corporation. "Canadians in Algeria Attack Went Overseas With 3rd Man." Last accessed 30 April 2014, http://www.cbc.ca/news/canada/canadians-in-algeria-attack-went-overseas-with-3rd-man-1.1383022.

Canadian Security Intelligence Agency. "What is Security Intelligence?" Last accessed 14 April 2014. https://www.csis-scrs.gc.ca/bts/fq-eng.asp#bm12.

Chretien, Jean. Address by the Prime Minister on the occasion of a Special House of Commons Debate in response to 9/11, Ottawa, September 17, 2001. Last accessed 03 May 2014. http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=653212&Language=E&Mode=1#SOB-47885

Department of National Defense. "Highlights of the Public Safety Act. 2002." Last accessed 21 April 2014. http://www.forces.gc.ca/en/news/article.page?doc=highlights-of-the-public-safety-act-2002/hnocfnla.

Douglas, Thomas. Quoted in John Gray. "Pierre Elliott Trudeau: 1919-2000." Globe and Mail. 30 September 2000. Last accessed 03 May 2014. http://v1.theglobeandmail.com/series/trudeau/jgray2_sep30.html.

Financial Transactions and Reports Analysis Centre of Canada. "Our Mandate." Last accessed 16 April 2014. http://www.fintrac-canafe.gc.ca/fintrac-canafe/1-eng.asp.

Geddes, John and Ken McQueen. "Air India Inquiry Reveals Intelligence Faults." Maclean's Magazine. 25 June 2007. Last accessed 03 May 2014. http://www.thecanadianencyclopedia.ca/en/article/air-india-inquiry-reveals-intelligence-faults/.

Integrated Threat Assessment Centre. "ITAC's Role." Last accessed 03 April 2014. http://www.itac.gc.ca/bt/rl-eng.asp.

Merriam-Webster Online Dictionary. "Forensic." Last accessed 16 April 2014. http://www.merriam-webster.com/dictionary/forensic.

Privy Council Office. "National Security Advisor to the Prime Minister." Last accessed 03 April 2014.http://www.pcobcp.gc.ca/index.asp?lang=eng&page=information&sub=publications&doc=Role/role2013-eng.htm#a3.

Public Safety Canada. "Action Plan 2010-2015 for Canada's Cyber Security Strategy." Last accessed 21 April 2014. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx.

Royal Canadian Mounted Police. "Integrated National Security Enforcement Teams." Last accessed 03 April 2014. http://www.rcmp-grc.gc.ca/secur/insets-eisn-eng.htm.

The Toronto Star. "Canada Refuses To Give Answers About Getting Off Of No Fly List." Last accessed 30 April 2014. http://www.thestar.com/opinion/commentary/2014/01/25/canada_refuses_to_give_answers_about_getting_off_nofly_list.html.

United States Department of State. "The Privacy Act." Last Accessed 03 May 2014. http://foia.state.gov/Learn/PrivacyAct.aspx.

Verkata Online Encyclopedia. "Maher Arar." Last Accessed 03 May 2014. http://wiki.verkata.com/en/wiki/Maher_Arar?page=3.

## OFFICIAL SOURCES

Canada. *Anti-Terrorism Act* (S.C. 2001, c. 41).Ottawa: Parliament of Canada. 2001.

Canada. *Canada Evidence Act* (R.S.C., 1985, c. C-5). Ottawa: Parliament of Canada, 1985.

Canada. *Canadian Security Intelligence Service Act* (R.S.C., 1985, c. C-23). Ottawa: Parliament of Canada, 1985.

Canada. Department of National Defense, *Canada First Defense Strategy.* Ottawa: Government

of Canada. 2004.

Canada. *Immigration and Refugee Protection Act*. (S.C. 2001, c. 27). Ottawa: Parliament of Canada, 2001.

Canada. *National Defense Act* (R.S.C., 1985, c. N-5). Ottawa: Parliament of Canada, 1985.

Canada. Office of the Privacy Commissioner of Canada. *Fundamental Privacy Rights within a Shared Vision for Perimeter Security and Economic Competitiveness.* Ottawa: Government of Canada, 2011.

Canada. *Privacy Act* (R.S.C., 1985, c. P-21). Ottawa: Parliament of Canada, 1983.

Canada. *Proceeds of Crime Money Laundering and Terrorist Financing Act* (S.C. 2000, c. 17). Ottawa: Parliament of Canada, 2000.

Canada. Public Safety Canada. *Action Plan 2010 – 2015 for Canada's Cyber Security Strategy*. Ottawa: Government of Canada, 2013.

Canada. Public Safety Canada. *Securing an Open Society: Canada's National Security Policy.* Ottawa: Government of Canada, 2004.

Canada. *Security of Information Act* (R.S.C., 1985, c. O-5). Ottawa: Parliament of Canada, 1985.

Department of National Defense. *Canadian Forces Joint Publication 2.0 Intelligence* Ottawa: Department of National Defense, 2011.

Office of the Auditor General of Canada. *Status Report of the Auditor General to the House of Commons – 2009.* Ottawa: Government of Canada, 2009.

Office of the Commissioner for Federal Judicial Affairs Canada. *Amnesty International Canada v Canada. 2008 FCA 401 [2009] 4 F.C.R. 149*. Ottawa: Government of Canada, 2008.

Senate of Canada. *Interim Report of the Special Senate Committee on Anti-Terrorism: Security. Freedom and the Complex Terrorist.* Ottawa: Government of Canada, 2011.

Supreme Court of Canada. *Charkaoui v. Canada Citizenship and Immigration [2007] 1 S.C.R. 350. 2007 SCC 9.* Ottawa: Government of Canada. 2008

United Kingdom. *Data Protection Act 1998.* London: Parliament of the United Kingdom, 1998.

United Kingdom. *National Intelligence Machinery.* London: Government of the United Kingdom, 2010.

United Kingdom. *Intelligence Services Act 1994*. London: Parliament of the United Kingdom, 1994.

United Kingdom. *Security Service Act 1996.* London: Parliament of the United Kingdom,1996.

United States. Department of the Army. *Biometrics Task Force Presentation - Biometric Automated Toolset BAT and Handheld Interagency Identity Detection Equipment HIIDE (*19 September 2007).

United States. *US Joint Publication 2.0 Joint Intelligence.* Washington: US Joint Chiefs of Staff, 2013.