National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

THE FUTURE OF US/CANADIAN COOPERATION IN THE SURVEILLANCE OF NORTH AMERICA

Lieutenant-Colonel J.D. Godefroy

JCSP 39

Master of Defence Studies

PCEMI 39

Maîtrise en études de la défense

Canada

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

MASTER OF DEFENCE STUDIES – MAÎTRISE EN ÉTUDES DE LA DÉFENSE

THE FUTURE OF US/CANADIAN COOPERATION IN THE SURVEILLANCE OF NORTH AMERICA

By Lieutenant-Colonel J.D. Godefroy
Par le lieutenant-colonel J.D. Godfrey

Word Count: 14 876

Compte de mots : 14 876

ABSTRACT

Recent military experience in Iraq and Afghanistan has caused both the United States (US) and Canada to look increasingly to unmanned aerial systems (UAS) as a flexible and low cost alternative to manned flights for domestic aerial surveillance. As a result, it is expected that intelligence, surveillance and reconnaissance (ISR) coverage of North America will expand exponentially over the next 10 to 30 years. Ongoing cooperation in continental defence, which has its roots in the North American Air Defence Agreement, has been deepened in recent years, and this shared purpose suggests that even greater cooperation will be likely in the future. This paper examines each state's current ISR enterprises, in both the military and civilian security domains, and surveys US and Canadian plans for future collection capability and exploitation infrastructure acquisitions. The legal and regulatory frameworks that govern the operation of UAS in each country are reviewed, and impediments to UAS use and international sharing of data are identified. Possible futures for the North American ISR environment are compared, using complex adaptive systems theory to identify possible challenges to proposed theoretical constructs which are driving planning and operating concept development on both sides of the border. Notwithstanding the great promise of increased collection represented by burgeoning UAS availability, the paper argues that limitations posed by national legal and political constraints will undermine the success of any move toward a self-synchronizing bi-national networked approach to shared surveillance of the North American continent. The paper concludes by arguing that notwithstanding these challenges, the nature and scope of the North American surveillance problem lends itself to increased adoption of UAS in the future, given their persistence and cost-effectiveness.

TABLE OF CONTENTS

LIST OF FIGURES

INTRODUCTION

Recent military experience in Iraq and Afghanistan has caused both the United States (US) and Canada to look increasingly to unmanned aerial systems (UAS) as a flexible and low cost alternative to manned flights for domestic aerial surveillance. As a result, it is expected that intelligence, surveillance and reconnaissance (ISR) coverage of North America will expand exponentially over the next 10 to 30 years. The two countries have markedly different surveillance needs, however, and the political, legal and regulatory issues that surround this new technology are also significantly dissimilar on each side of the border. Nonetheless, ongoing cooperation in the defence of North America, which has its roots in the North American Air Defence Agreement (NORAD), has been deepened in recent years through interaction between the US Northern Command (NORTHCOM) and the Canadian equivalent Canada Command, now absorbed into the Combined Joint Operations Command (CJOC). This shared purpose suggests that even greater future cooperation in the surveillance of our continent will be likely, but what form will this cooperation take?

This paper will examine each state's current ISR enterprises, in both the military and civilian security domains, and survey US and Canadian plans for future collection capability and exploitation infrastructure acquisitions, seeking to identify what impact UAS acquisition will ultimately have on each nation's surveillance capabilities. The legal and regulatory framework that governs the operation of UAS in each country will also be reviewed, with a view to identifying impediments to UAS use and international sharing of data collected by both UAS and manned ISR platforms. The experience of the United Kingdom (UK), Australia and the North Atlantic Treaty Organization (NATO) will be

examined to identify any possible lessons. Finally, possible futures for a North American ISR environment will be proposed and compared, with the aim of identifying the potential impacts of UAS acquisition and employment in a domestic context. It will be demonstrated that notwithstanding the great promise of increased collection represented by burgeoning UAS availability, limitations posed by national legal and political constraints, and the inherent friction that affects networked systems, will undermine the success of any move toward a self-synchronizing bi-national networked approach to shared surveillance of the North American continent. Nonetheless, it will be argued that the nature and scope of the North American surveillance problem lends itself to increased adoption of UAS in the future, given their persistence and cost-effectiveness.

LITERATURE REVIEW

The subject of national surveillance in Canada and the US is discussed in a number of references, which include government, academic and open source media publications. For the purpose of this paper, the initial source documentation sought included government planning and policy documentation which describes the surveillance tasks of each state's respective services and agencies, both military and civilian. In Canada, the government's *Canada First Defence Strategy* (CFDS) was used as a start point to identify the surveillance task assigned to the Canadian Armed Forces (CF), which is further defined in the Department of National Defence (DND) Management, Resource and Results Structure (MRRS) Program Activity Architecture (PAA). Documentation outlining the roles and responsibilities of specific CF or bi-lateral allied organizations is not freely available in the unclassified realm, and reference was

made to departmental studies and operating concepts, such as DND's National Surveillance Working Group, in the Chief Force Development (CFD) "National Surveillance Study" published in 2011, and the September 2012 "Intelligence Surveillance and Reconnaissance Operating Concept" published by the Vice Chief of Defence Staff (VCDS). These documents provided greater insight into the specific surveillance zones each entity monitors, and shed light on the organizational accountabilities of both military and civilian agencies. Doctrine sources were further consulted to clarify definitions and practices. These included CF Joint Publication (CFJP) 2.0, *Intelligence*, and CFJP 3.0, *Operations*. Civilian government policy and regulations have also been consulted, specifically Transport Canada's *Designated Airspace Handbook* and regulations for the operation of unmanned aerial vehicles (UAV) in Canadian airspace. These documents have assisted in defining the surveillance problem further, and have highlighted current regulatory constraints to expanded UAS use.

The US Government has a generally richer documentary basis for its surveillance activity. Department of Defense (DoD) documentation on current military UAS capabilities and domestic use was consulted as a start point. An April 2012 DoD Report to Congress on Future Unmanned Aircraft Systems Training, Operations and Sustainability , produced for the Under Secretary of Defense for Acquisition, Technology and Logistics provides an overview of current and anticipated future UAS acquisitions and associated training for all of the services between now and 2017. The DoD Unmanned Systems Integrated Roadmap FY 2011-2036, produced by the same office in 2011, updated earlier 2007 and 2009 versions of the same report, and lays out a DoD

vision for the development, fielding and deployment of UAS over a 25 year horizon.[1] Specific service doctrine which captures some aspects of US military UAS use, particularly command and control concepts espoused by the US Army and the US Air Force (USAF), is available and was consulted in excerpted form in several scholarly articles. The *United States Air Force Unmanned Aircraft Systems Flight Plan 2009-2047* was consulted as a key document which examines present and anticipated future capabilities across the services, and outlines how they will be used, although it is important to note that the USAF has retrenched on much of the vision this document contains, opting to retain piloted aircraft capabilities at the expense of UAS programs, which have been scaled back or cut over the last year.[2]

In addition to DoD references, a number of civilian US government sources are available and were found to offer useful broad insight into current US policy and activity, as well as future considerations. The capstone US Government document for air surveillance of US territory is the November 2011 Joint Planning and Development Office *Integrated Air Surveillance Concept of Operations*, a multi-agency publication which includes input from DoD, the Department of Commerce/National Oceanic and Atmospheric Administration, the Department of Homeland Security (DHS), the Federal Aviation Agency (FAA), and the Office of the Director for National Intelligence (ODNI). This document represents an attempt to integrate the operating concepts of all contributors, and to offer an initial proposal for an Integrated Air Surveillance

---

[1]Department of Defense, *Unmanned Systems Integrated Roadmap FY2011-2036*, 11-S-3613, (Washington, DC : U.S. Government Printing Office, 2011), 1.

[2]Lt. Col. Lawrence Spinetta and M.L. Cummings, "Unloved Aerial Vehicles," *Armed Forces Journal*, November 2012, last modified [or accessed] 2 April 2013, http://www.armedforcesjournal.com/2012/11/11752540

Architecture (ISEA) and associated governance with a near-term ambition of optimizing existing coverage and information sharing, and a long-term vision of achieving coverage of all US airspace.[3] A similar multi-agency document, the *National Concept of Operations for Maritime Domain Awareness,* published in December 2007, seeks to help establish an effective national maritime domain awareness (MDA) enterprise and interagency governance structure that aligns the efforts of the maritime intelligence and situational awareness communities.[4]

A number of US Government offices and agencies have also published inspection reports, audits, and policy papers on domestic UAS use. The House Permanent Select Committee on Intelligence published a performance audit of DoD ISR capabilities in April 2012, which looks at existing capabilities and training and makes recommendations about future requirements.[5] The DHS's Office of the Inspector General produced a review of US Customs and Border Protection (CBP) UAS use in May 2012. The Congressional Budget Office's (CBO) June 2011 report, "Policy Options for Unmanned Aircraft Systems", examined all DoD planned UAS system acquisitions, seeking to compare the costs and capabilities of planned system purchases against those of alternative options.[6] Finally, the US Congressional Research Service is a prolific source of collated information on military UAS acquisition plans, legal implications of military

---

[3]Joint Planning and Development Office, *Integrated Air Surveillance Concept of Operations* (Washington, DC: US Government Printing Office, November 2011), i-ii.

[4]Office of Global Maritime Situational Awareness, *National Concept of Operations for Maritime Domain Awareness* (Washington, DC: US Government Printing Office, December 2007), i-iii, 1.

[5]House Permanent Select Committee on Intelligence, *Performance Audit of Department of Defense Intelligence, Surveillance, and Reconnaissance* (Washington, DC: US Government Printing Office, April 2012),ii.

[6]Congress of the United States, Congressional Budget Office. *Policy Options for Unmanned Aircraft Systems* (Washington, DC: US Government Printing Office, June 2011), vii-xv.

and civilian government UAS use in a domestic context, and regulatory concerns, particularly the FAA's obligation to ensure that UAS are safely integrated into the nation's national airspace. Civilian lobbying and public interest groups, such as the American Civil Liberties Union (ACLU), have also produced policy papers with recommendations on limitations to UAS use in a domestic context, which have been helpful in framing the legal and privacy concerns that increased use of this technology have elicited.

These official government publications have been supplemented by reference to previously published academic papers on the topics of domestic surveillance and UAS use in both the US and Canadian context. Essays on US issues include USAF Major Scott Walker's US Army Command and General Staff College Master's thesis on the subject of integration of DoD UAS into the US national airspace policy structure, and USAF Major David Buchanan's US Naval War College paper discussing the desirability of USAF/US Army collaboration on joint doctrine for UAS use. Two Master of Defence Studies papers written by CF officers on Joint Command and Staff Program (JCSP) Course 35 discuss CF surveillance capabilities with a focus on air force systems. A paper by Major Iain Huddleston examines Canada's future ISR system, and takes a holistic approach that examines the surveillance problem in both the air and maritime domains, while another by Maj R.J. Walker focuses on the shortcomings and possible future of Canada's ISR system. These papers, written in early 2009, are somewhat dated, but given the relative lack in progress on both the policy and capability acquisition fronts, their conclusions, which argue for an ISR system of systems that combines multiple integrated platforms, and that has been developed in a holistic way, remain relevant in the context of

this paper's discussion of a future greater integrated North American system that combines Canadian and US capabilities.[7] The burgeoning interest of the Government of Canada in ensuring our ability to maintain influence in the Arctic is another theme that this paper seeks to examine, and an article by Captain Levon Bond in the Autumn 2011 Canadian Military Journal examines planned Canadian ISR capabilities, such as the Joint Unmanned Surveillance Target Acquisition System (JUSTAS), which will impact the CF's ability to better monitor this region in the future.

Finally, printed books and academic articles have provided useful context about the use of ISR data for intelligence production and the creation of situational awareness. Specifically useful sources included Gary Marx's article on concepts for understanding the myriad forms of surveillance, which appears in L.V. Scott and Peter Jackson's *Understanding Intelligence in the Twenty-First Century*, and Antoine Bousquet's *The Scientific Way of Warfare*, which includes a detailed treatment of the subject of complex adaptive systems theory. These have been supplemented by media articles from both countries, which have provided commentary on current UAS capability development, government policy decisions, expanding domestic UAS use, and associated legal issues and privacy concerns.

While there are a broad array of sources available on the topic of UAS use and surveillance of both the US and Canada, none brings together the issues at play in each country to examine the broader impacts of current and future developments on further

---

[7]Major R.J. Walker, "What Happened to Air Force ISR?" (MDS Research Project Paper, Canadian Forces College, 2009), i. and Major Iain Huddleston, "Canada First?: Defence Strategy and the Future Aerospace ISR 'System of Systems," (MDS Research Project Paper, Canadian Forces College, 2009), 2.

future integration of the two countries' respective surveillance enterprises. This paper seeks to begin this discussion, and to fill a gap in the literature.

CHAPTER 1: THE SURVEILLANCE PROBLEM

The *Canada First* Defence Strategy (CFDS), published in June 2008, represents the Government of Canada's twenty year strategic plan to develop the necessary capabilities that will ensure the Canadian Armed Forces (CF) can perform a series of explicitly outlined missions. First among these is the safeguarding of Canadian citizens and sovereignty, which sees the military specifically tasked to, "…work closely with federal government partners to ensure the constant monitoring of Canada's territory and air and maritime approaches, including in the Arctic, in order to detect threats to Canadian security as early as possible."[8] This monitoring expectation is further described, and the document states that, "Specifically, it means that the military will maintain the capacity to…provide surveillance of Canadian territory and air and maritime approaches…" [9] It is allowed that responsibility for surveillance of this area is shared among multiple Government of Canada departments, and while these are not specifically mentioned in the document, they include the Canadian Security Intelligence Service (CSIS), Transport Canada (TC), Environment Canada (EC), and the Canadian Border Service Agency (CBSA). For example TC is responsible for the National Aerial Surveillance Program (NASP), which monitors ships transiting Canadian waters for pollution prevention purposes using a combination of surveillance from manned aircraft

---

[8]Department of National Defence, *Canada First Defence Strategy* (Ottawa: DND Canada, 18 June 2008), 7.

[9]*Ibid*.

and satellite imagery.[10] The scope of the surveillance task levied on the CF is not specifically defined, but military organizations generally include the latter in a holistically described information collection activity known as "Intelligence, Surveillance and Reconnaissance", or ISR. Reference to doctrine, specifically Canadian Forces Joint Publication 2.0, *Intelligence*, provides the following definition for ISR, which will be used for the purpose of this paper:

> ISR is the activity that synchronizes and integrates the planning and operation of all collection capabilities, with exploitation and processing, to disseminate the resulting information to the right person, at the right time, in the right format, in direct support of current and future operations.[11]

This definition draws out the fact that surveillance is more than simply collecting data. It also includes the analysis of the data collected to create useful intelligence, and the passage of this intelligence to all those who need it. While it describes an ideal construct seldom achieved, it provides a helpful explanation of the basic components that make up an ISR system. It is noteworthy that the definition includes both surveillance and reconnaissance, which *British Air and Space Power Doctrine* notes, "complements surveillance by using visual observation, or other detection methods, to obtain specific information about the activities and resources of an enemy or potential enemy."[12] The issue of whether the information sought is specific or not is generally not apparent to end users of the data, and the systemic nature of ISR as a conceptual paradigm is the most important issue for the purpose of this essay.

---

[10]Transport Canada, "Spill Prevention: National Aerial Surveillance Program," last modified [or accessed] 12 February 2013, http://www.tc.gc.ca/eng/marinesafety/oep-ers-nasp-2195.htm.

[11]Department of National Defence, CFJP 2-0, *Intelligence* (Ottawa: DND Canada, October 2011), 3-4.

[12]Air Staff, Ministry of Defence, *British Air and Space Power Doctrine*, AP 3000, 4th Edition, 2009, 49.

It is apparent that the task laid out in the CFDS is no small problem. Canada's land mass covers some 9,984,670 square kilometres[13], and the maritime approaches to the country include an additional 7,100,000 square kilometres of open water.[14] An area of this extent may be impossible to survey persistently, and it is not apparent, even if data could be collected that would allow for the detection of any penetration of Canadian territory, that it would be possible to analyze it in a timely way and produce useful intelligence. Indeed, the Department of National Defence's (DND) National Surveillance Working Group, in the Chief Force Development (CFD) "National Surveillance Study" published in 2011, notes that, " …"continuous" surveillance of the (sic) Canada's entire surveillance area of responsibility is neither practical nor necessary," and acknowledges that one method by which Canada, "has traditionally dealt with the vast scale of the military surveillance problem is to partner with our allies."[15]

The principal surveillance partnership between the two states is the NORAD agreement, which was signed on 12 May 1958, and updated to include a maritime warning task, among other modifications, on 28 April 2006. The primary missions of NORAD include aerospace warning, aerospace control, and maritime warning for North America. The aerospace warning and maritime warning tasks involve "processing, assessing and disseminating intelligence and information", and in the maritime warning task, explicit mention is made of the requirement to, "develop a comprehensive shared

---

[13]Statistics Canada, "Land and freshwater area, by province and territory," last modified [or accessed] 12 February 2013, http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/phys01-eng.htm.

[14]Department of Fisheries and Oceans, "Canada's Ocean Estate: A Description of Canada's Maritime Zones," last modified [or accessed] 12 February 2013, http://www.dfo-mpo.gc.ca/oceans/canadasoceans-oceansducanada/marinezones-zonesmarines-eng.htm#terr

[15]Department of National Defence, Chief of Force Development, *Canadian Forces National Surveillance Study 2010 (U)* (Ottawa: DND Canada, 15 January 2011), 8-9.

understanding".[16] The agreement also acknowledges the threat to national security posed by "non-military air and maritime activities associated with drug trafficking and other illegal transnational activities...", suggesting that surveillance of the continent must also take into account these non-traditional threats to both nations' security.[17] The specific surveillance responsibilities of each nation are not prescribed in the agreement, but can be assumed to include the national airspace and maritime approaches of each party.

Given this existing obligation, what is the specific ambition of the Government of Canada, and what is the CF's specific accountability for surveillance of Canadian territory? An attempt to provide a framework for the CF's development of a holistically integrated ISR enterprise was made in September 2012 through the publication of the "Intelligence Surveillance and Reconnaissance Operating Concept" by the Vice Chief of Defence Staff. The stated aim of this document is to, "to establish a framework for the efficient, flexible, adaptable development of ISR capabilities that deliver integrated information and intelligence to support CF Command and Control (C2)."[18] It outlines concepts and intent to govern the force employment, generation and development of ISR capabilities between now and 2032.[19] It explicitly notes the various shortcomings of the CF's current capability, which will be outlined further in Chapter 2. It does not, however, define the extent and nature of the surveillance problem. To identify this specific accountability, reference must be made to a patchwork of documentation. The capstone document that outlines DND's accountabilities in the delivery of its program is the

---

[16]*Agreement between the Government of the United States of America and the Government of Canada on the North American Aerospace Defense Command*, 28 April 2006, Article 1, a., c.

[17]*Ibid.*, Preamble.

[18]Department of National Defence, Vice Chief of Defence Staff, *Intelligence Surveillance and Reconnaissance Operating Concept* (Ottawa: DND Canada, 26 September 2012), i.

[19]*Ibid.* 7.

Management, Resource and Results Structure (MRRS). The latter documents DND's deliverables in a Program Activity Architecture (PAA), which contains 17 different program activities. These include ISR-related sub-programs under the Aerospace Readiness and Situational Awareness programs, while the Canadian Peace Stability and Security, Continental Peace Stability and Security and International Peace Stability and Security programs also have ISR-related components.[20] The PAA provides a performance measurement framework for each program, and identifies the specific organizations responsible for each activity. Responsibility for ISR activities is spread between the Canadian Army (CA), Royal Canadian Navy (RCN), Royal Canadian Air Force (RCAF), CJOC, and the Chief of Defence Intelligence.[21] These responsibilities are primarily discharged by the three services, under command of CJOC, NORAD or the 1st Canadian Air Division (1 CAD) as appropriate. On a day-to-day basis, the RCN, 1 CAD, and NORAD undertake specific continental surveillance activities in cooperation with OGD partners and Canada's US allies. The CF, specifically 1 CAD and the RCAF's NORAD contribution, partner with NAV Canada to monitor Canadian domestic airspace, which is divided into a Southern Domestic Airspace and a Northern Domestic Airspace zone, and includes an Air Defence Identification Zone.[22] Each of these zones includes all of the airspace above the described geographic area.

---

[20]Department of National Defence, Vice Chief of Defence Staff, *Program Activity Architecture*, last modified [or accessed] 13 February 2013, http://www.vcds.forces.gc.ca/sites/CProg/Resources/Internet/PAA-AAP/PAA%20Structure%20FINAL.pdf.

[21]*Ibid.*

[22]NAV Canada, *TP1820E Designated Airspace Handbook* (Ottawa, Minister of Transport, 2013), last modified [or accessed] 13 February 2013, http://www.navcanada.ca/ContentDefinitionFiles/Publications/AeronauticalInfoProducts/DAH/DAH_current_EN.pdf, 169, 174.

Another delineation of the North American surveillance problem is found in the North American Air Surveillance Plan (NAASP), a draft bi-national document which includes US and Canadian civilian and military input. The plan uses geographic and altitude dimensions to define six different airspace zones, five of which are relevant to the problem of continental surveillance. These include the North American Perimeter (NAP), the area from 100 nautical miles (nm) inland to 600 nm off the coast, and from the surface to 100,000 feet above mean sea level; the Interior High Altitude (IHA) airspace of each country, which resides inside the NAP and stretches from 30,000 feet to 100,000 feet above mean sea level; the Interior Medium Altitude (IMA) airspace, which consists of the area between 5,000 feet above ground level (AGL) to 30,000 feet above mean sea level; the Interior Low Altitude (ILA) airspace, which covers the area from the surface to 5,000 feet AGL; and special airspace, which is designated in cases where, "more stringent monitoring is required for special circumstances (i.e. protecting critical vital points)".[23] These zones are graphically depicted in Figure 1 below.

[23]*Canadian Forces National Surveillance Study…,* 11-12.

Figure 1: Canadian NAASP Zones

Source: *Canadian Forces National Surveillance Study…,* 12.

The CF's specific accountabilities with respect to surveillance of these zones are currently poorly defined. The CFD 2010 National Surveillance Study notes that specific Defence Tasks (DT) to conduct aerial surveillance are codified in the Defence Plan Online, but notes that the latter is "out of date and is currently being updated."[24] Regardless, given that the previously mentioned MRRS PAA, which has replaced the latter document, neglects to define the specific extent of the zones, the DTs remain the best source of a definition of the current aerial surveillance responsibilities of the CF, which are summarized as extending 600 nm from the perimeter of Canada's national coastlines/borders, and from the surface to 100,000 feet above median sea level (MSL).

[24] *Ibid.*,13.

Areas along the Canada/US border are an exception, and shared responsibility for these are outlined by the existing NORAD agreement. [25]

Responsibility for maritime surveillance is part of the domestic mandate of CJOC, and details of the conduct of this activity are covered in classified Canada Command Operation Order 10202/90 "LIMPID" Canadian Surveillance and Presence. The CF is not responsible for surveillance within the 12nm limit, with the exception of three DND/CF Controlled Access Zones in inshore waters off Halifax, Esquimalt and Nanoose harbours.[26] Notably, since 2006, the renewal of the NORAD Agreement has resulted in the corollary maritime warning mission becoming part of the latter organization's mandate.[27] The areas subject to maritime surveillance were defined in an internal 2002 CF ISR concept document produced by the Chief of the Maritime Staff, and consist of a series of four maritime surveillance zones. These are designated as an Inner Zone, which extends from the shore out to 50 nm; a Middle Zone which covers the area from the 50nm line out to 250 nm; an Outer Zone, which extends from 250 nm out to 1000 nm; and an Arctic Zone, which is less specifically defined.[28] These zones are graphically depicted in the diagram at Figure 2 below.

---

[25]*Agreement…on the North American Aerospace Defense Command…*, Article 1.
[26]*Canadian Forces National Surveillance Study...*, 14.
[27]*Ibid.*, 15.
[28]*Ibid.*, 14-15.

Figure 2 – Maritime Surveillance Zones

Source: Canada, *Canadian Forces National Surveillance Study…,* 15.

CF accountabilities are specifically focused on the continuous monitoring of the Middle Zone (50-250 nm), where there is an expectation that all vessels of interest (VoI) will be detected, tracked and identified. The CF is expected to detect and identify anomalous vessels in the Outer Zone (250-1000 nm), so as to designate VoI before they reach the outskirts of the Middle Zone, which is only 50 nm away from the start of Canada's Exclusive Economic Zone (EEZ). [29]

Canada's specific surveillance obligations for the Arctic, while included in an abstract way in the air and maritime zones described above, are the subject of increasing clarification as the area gains more GoC attention. At present, while there is limited capacity to conduct surveillance in the area, changing climatic conditions in recent years have made the area increasingly accessible, creating an imperative for more persistent monitoring of this region. Other regions or domains that are the subject of limited CF

[29] *Ibid.*, 15.

surveillance effort, while not specifically the focus of this paper, include outer space and cyber-space.

While the capability of the CF to conduct collection of surveillance data in its assigned areas will be discussed further in Chapter 2, it is appropriate at this time to examine the CF's capacity to manage the surveillance problem. Specifically, the CF's ability to coordinate the collection of specific surveillance data in assigned areas of responsibility, to exchange information with OGD partners and our US allies, and to federate the production of situational awareness and intelligence will be reviewed, with the intent of identifying shortfalls in current capability.

The issue of collection coordination is a key component in the effective functioning of an ISR system. Although airspace surveillance coordination, affected through Canada's participation in NORAD, is a mature activity, shortcomings exist in our ability to effectively monitor the maritime domain. Since collection resources are a scarce commodity, they must be focused in a way that assumes informed risk, given that there will inevitably be zones that are subject to gaps in persistent coverage, and some areas where no coverage will exist. At present, this collection coordination is performed primarily by human analysts, with a command role exercised in the establishment of priorities for both collection and analysis.[30] Notwithstanding collection limitations, the data that can be collected exceeds existing analytical capacity to review it, and further risk is regularly assumed as data is collected that is only superficially analyzed. For example, at the interdepartmental Maritime Security Operations Centres (MSOC) that have been established in Halifax, Esquimalt and Niagara to conduct collaborative

---

[30]*Ibid.*, 35.

detection and assessment, the integration of maritime surveillance data and the automated correlation of data collected by various sources remain limited.[31] The USAF *Air Force UAS Flight* Plan notes that, "The importance of solving the manpower shortfall is imperative as technology continues to outpace the USAF ability to source and train analysts." In the longer term, the USAF is seeking to automate labour intensive functions, such as processing, analysis and dissemination of derived threat detection information, as one mitigation measure to surmount this challenge.[32] Analytical capacity limitations are further exacerbated by the fact that differences exist in the computer systems and networks used to collect, analyze and share information. These differences create data "stovepipes" which prevent the sharing and correlation of data. While some of these limitations have been overcome within specific organizations, they persist between the services, and between the CF/DND and OGDs, and the result is that there is no one common operating picture (COP) that is shared within the CF, or between the CF and their partners. Some minor efforts, such as the MSOC that have been established on each coast, and in the Niagara region, have resulted in the creation of limited shared situational awareness between stakeholders. The centres seek to manage the collection of marine information and ISR data, and eventually, pending resolution of legislative issues, to store and analyze this data, creating marine information products and generating a Recognized Maritime Picture (RMP).[33] The fact that some 17 different Canadian Government departments and agencies participate in the Interdepartmental Maritime

---

[31]*Ibid., 35-36.*

[32]U.S. Air Force, *United States Air Force Unmanned Aircraft Systems Flight Plan 2009-2047,* Headquarters, United States Air Force, (Washington, DC: Department of the Air Force, 18 May 2009), 29.

[33]*Canadian Forces National Surveillance Study…,* 36.

Security Working Group, which is working to develop the country's MDA Strategy, offers a sense of the scope of the challenges that exist in de-conflicting responsibilities and generating shared and timely situational awareness.[34]

It has been seen that the current CF mandate to conduct surveillance of Canadian territory has several areas of jurisdictional overlap, with lead responsibility subject to interpretation. It has been further identified that the CF lacks a holistic system of collection capabilities, de-conflicted analytical responsibilities, and dissemination mechanisms which would allow for the timely dissemination of intelligence developed through surveillance of Canada. Finally, it has been demonstrated that the CF's responsibilities, such as they are, are not well de-conflicted with those of the OGD or with the US. The US ISR approach will now be examined to provide a basis for comparison and initial analysis of the problem from a "whole-of-North America" perspective.

The United States surveillance problem is no less daunting than Canada's. In addition to a coastline of approximately 19,928 km, the US shares an 8,891 km border with Canada, and a 3,110 km border with Mexico.[35] Responsibility for surveillance of the US portion of the North American continent is shared between DoD and a number of civilian government agencies, which include the FAA, DHS, the Department of Commerce, specifically the National Oceanic and Atmospheric Administration (NOAA), and ODNI.[36] The DoD surveillance responsibilities are divided between NORAD, who

---

[34]*Ibid.*, 34.

[35]Department of Commerce, United States Census Bureau, *The 2012 Statistical Abstract: The National Data Book*, last modified [or accessed] 26 February 2013, http://www.census.gov/compendia/statab/2012/tables/12s0364.pdf

[36]*Integrated Air Surveillance Concept of Operations...*, 8.

are responsible for detecting aerospace threats to North America and providing maritime warning for the continent, and US Northern Command (USNORTHCOM), whose primary responsibilities explicitly include, "Monitoring Areas of Responsibility (AORs) that include air, land and sea approaches and encompass the continental United States, Alaska, Canada, Mexico and the surrounding water out to approximately 500 nautical miles."[37]These responsibilities are currently discharged in an incomplete way. The February 2010 US Quadrennial Defense Review notes that,

> The Department of Defense and its interagency partners must be able to more comprehensively monitor the air, land, maritime, space, and cyber domains for potential direct threats to the United States…. This effort includes enhanced coordination with Canada for the defense of North America as well as assisting Mexico and Caribbean partners in developing air and maritime domain awareness capacities. Special attention is required to develop domain awareness tools for the Arctic approaches as well.[38]

What are the specific shortcomings of the existing system, and why do they exist? The US faces challenges, much like those of Canada, because of the patchwork of conflicting authorities, accountabilities and priorities that undermine progress on building a system that shares data effectively in a timely way. A June 2011 GAO examination of DoD's ISR enterprise noted that, "until DOD develops an integrated ISR investment strategy, the defense and intelligence communities may continue to use resources that are not necessarily based on strategic priorities, which could lead to gaps in some areas of intelligence operations and redundancies in others."[39] The bottom line is that acquisition

---

[37]*Ibid*, 11.

[38]Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: US Government Printing Office, February 2010), 19.

[39]Government Accountability Office, *Intelligence, Surveillance, And Reconnaissance: Actions Are Needed to Increase Integration and Efficiencies of DOD's ISR Enterprise*, GAO 11-465 (Washington, DC: US Government Printing Office, June 2011), 21.

programs are conceived of and implemented independently in various departments and across the services, which causes inefficiencies.

NORAD shares its responsibility for surveillance of the NAS with the FAA and US CBP, a component of DHS, which is the main civilian agency responsible for the detection and identification of potential air threats to the United States.[40] While this combination of military and civilian authorities operates a reasonably mature system that provides comprehensive 24/7 coverage of the air domain, it does have some shortcomings. Specific current constraints mentioned in the November 2011 *Integrated Air Surveillance Concept of Operations* include the lack of a governance mechanism for a national integrated air surveillance capability, a shortage of well-developed legal and policy guidelines to enable information sharing between partners, and the absence of a network architecture to allow, "automated interagency processing, integration and dissemination of information, between interagency networks or across different levels of classification, ...". It is further acknowledged that "current data feeds from DoD and FAA surveillance systems are not uniformly integrated...", with the result being that surveillance-derived information is normally passed on through manual means.[41] The US is acutely aware of this fact, and has developed specific plans to address the shortcomings in their system. The March 2007 "Air Domain Surveillance and Intelligence Integration Plan", for example, highlights detection and prevention of threats, information sharing and integration, and unity of effort between the public and private sector, as well as

---

[40]Department of Homeland Security, *Air Domain Surveillance and Intelligence Integration Plan: Supporting Plan to the National Strategy for Aviation Security* (Washington, DC: US Government Printing Office, March 26, 2007), 11.

[41]*Integrated Air Surveillance Concept of Operations*..., 21.

international partners, as guiding principles for the further development of air domain awareness.[42] The US is seeking to develop a "next generation" integrated system between now and 2025, and the long-term intent, outlined in the plan, is that,

> To maximize Air Domain awareness, we must transform, and integrate capabilities that collect, analyze, and disseminate surveillance, intelligence and information to create an operational picture that is tailorable to the needs of users across the United States Government, as well as at State, local, and tribal levels, and with private entities and our foreign partners.[43]

The maritime domain is also perceived to be particularly problematic to address in a comprehensive way. The US DoD December 2007 National Concept of Operations for Maritime Domain Awareness (MDA) notes a number of problems that persist to the present, including gaps in collection capability, incompatible software use by the various responsible departments and agencies, unconnected databases, and misunderstandings between organizations that affect communication and the free exchange of information.[44] A dissonance also exists between the needs of clients for unclassified information and classified intelligence data, and this has undermined agreement on assignment of accountabilities for MDA maintenance. This latter issue gets at the heart of the problem of discussing surveillance in a comprehensive way. The US, like Canada, has surveillance needs that are driven by border protection and trade regulatory requirements, such as those administered by CBP, and others that revolve around defence of the state, which are the purview of DoD. While each was historically disconnected, advances in technology and changes to the threats that states face has led to an increasing convergence in intelligence and situational awareness requirements. Current threat

---

[42] *Air Domain Surveillance and Intelligence Integration Plan…*, 3.
[43] *Ibid., 1.*
[44] *National Concept of Operations for Maritime Domain Awareness…*, 4-5.

organizations, which include terrorists and trans-national criminal organizations (TCO), plan attacks on the North American continent using weapons and tactics that were not considered when the various surveillance regimes were first established. Intelligence about these threats is not easily shared with non-intelligence community partners given the constraints imposed by the existing information sharing architecture. The *Integrated Air Surveillance Concept of Operations* notes that, "the lack of integrated shared data and an ”analysis architecture"... constrains intelligence integration and information sharing within the IC [intelligence community] and across the non-IC."[45]

The requirement for remediation of now-apparent gaps in the surveillance system is driven by a need to connect the border protection and defence surveillance tasks of each state, and to move beyond state-specific surveillance to a continental regime. Further, new collection capabilities, such as those represented by UAS, are creating an environment where the relevant data that is collected and available for analysis will likely further outstrip the ability of the various agencies to process and/or share it in a timely way. The issue of current and future collection capability, in both Canada and the United States, will be examined further in the next chapter.

CHAPTER 2: CURRENT NORTH AMERICAN SURVEILLANCE CAPABILITY

At present, domestic surveillance of the North American continent and its approaches is predominantly conducted using radars and other sensors, manned aircraft and satellite imaging systems. This chapter will examine the anticipated evolution of the capabilities available for collection of surveillance data in Canada and the United States,

---

[45]*Integrated Air Surveillance Concept of Operations*..., 15.

and assess the potential impacts that this will have on the surveillance problem. It will be argued that the lower cost and increased persistence of UAS will result in an exponential increase in monitoring capability, which will place significant pressure on each country to address existing processing shortfalls in their current air and maritime domain awareness systems.

The various descriptions of potential future systems for air and maritime domain awareness production that were outlined in the previous chapter represent aspirations that anticipate the increased availability of persistent surveillance capabilities which can monitor North American airspace and the approaches to the continent on a continual basis. Such capability does not currently exist, due to endurance issues associated with manned aircraft, and the cyclical nature of current satellite surveillance capacity, which is focused on traditional foreign problem areas rather than domestic surveillance. It is apparent, however, that anticipated growth in the availability of UAS in various forms represents an opportunity to achieve an unprecedented and previously impossible level of persistent surveillance of the continent.

The United States is currently experiencing a boom in the development of UAS technologies and the extension of these capabilities in spheres beyond the military. Police, rescue and commercial entities are all embracing the benefits that the technology offers, lured by the promise of real-time video and images that can be geographically referenced, analyzed and shared with a wide range of stakeholders through GIS applications. These systems, in addition to offering high-resolution still and motion imagery, provide many additional benefits, which include enhanced endurance well beyond what can be achieved with manned flight, and stealth derived from their ability to

operate at altitudes up to 60,000 feet.[46] The US military has led the way in bringing these systems into operation, although the approach used by the various services to acquire and develop UAS technologies has been far from consistent.[47] While UAS have been used by US military forces since the Vietnam War, they gained prominence only during the First Gulf War in 1990-91. Early efforts to manage defence UAV acquisition efforts began in 1993, with the creation of the Defense Airborne Reconnaissance Office (DARO).[48] A Deputy Secretary of Defense initiative, the role of DARO was described as, "unifying existing reconnaissance architectures and enhancing the management and acquisition of all joint Service and Defense-wide manned and unmanned airborne reconnaissance/ surveillance capabilities".[49] The agency was short lived, however, and was folded into the National Imagery and Mapping Agency (NIMA), now the National Geospatial-Intelligence Agency (NGA), in 1998, with its acquisition coordination responsibilities retained by DoD, under the leadership of the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.[50] While this effort at centralization of acquisition responsibilities within DoD might have been expected to promote efficiency, it has not been particularly successful. An April 2012 performance audit of DoD ISR conducted by the House Permanent Select Committee on Intelligence found that, "The speed of growth,

---

[46]*Unmanned Aircraft Systems Flight Plan…*, 27.

[47]Richard F. Grimmett and Rebecca S. Lange, *Intelligence, Surveillance and Reconnaissance (ISR) Acquisition: Issues for Congress* (Washington, DC : U.S. Government Printing Office, September 10, 2012), 10.

[48]Department of Defense, *Defense Airborne Reconnaissance Office (DARO) Unmanned Aerial Vehicles (UAV) Program Plan* (Washington, DC: US Government Printing Office, April 1994), last modified [or accessed] 21 January 2013, http://www.dod.gov/pubs/foi/International_security_affairs/other/892.pdf

[49]*Ibid., ES-1.*

[50]United States Statutes at Large Volume 111 Part 2 Public Law 105-85, *Sec. 905 Airborne Reconnaissance Management*, 18 November 1997, last modified [or accessed] 2 April 2013, http://en.wikisource.org/wiki/Page:United_States_Statutes_at_Large_Volume_111_Part_2.djvu/775

lack of central management within DoD, and insufficient Executive Branch and Congressional oversight have led to many inefficiencies in DoDs ISR portfolio."[51] Specific challenges include the fact that the services have built similar UAVs under separate programs, and have each developed their own independent training systems and infrastructure, forgoing savings that might have been realized through coordinated effort.[52] Unfortunately, the acquisition plans of civilian agencies also continue to be developed and pursued independently, and there are no indications that this will change in the foreseeable future.

While capability acquisition is relatively uncoordinated across the US government, there has been some movement toward an interagency approach to addressing issues with routine UAS access to US national airspace (NAS). At present, the FAA places significant limitations on UAS flights. UAS are only allowed to operate under special conditions through a certification of authorization (COA) process, and normally in controlled or restricted airspace.[53] This limitation did not cause undue hardship in the past, but the expansion of capabilities across the services and in civilian organizations has led to significant demand for COA approval.[54] The ongoing DoD requirement to train its personnel on use of these systems, and the return of UAS systems to the US from Afghanistan and Iraq as deployed operations wind down, is expected to drive demand for additional authorizations.[55] The bureaucratic process, which is considered necessary for the fulfillment of the FAA's mandate, is cumbersome and slow,

---

[51]*Performance Audit of Department of Defense Intelligence, Surveillance, and Reconnaissance…*, *v.*

[52]*Ibid.*

[53]Major Scott A. Walker, "Integrating Department of Defense Unmanned Aerial Systems into the National Airspace Structure" (master's thesis, U.S. Army Command and General Staff College, 2010), 2.

[54]*Ibid.*

[55]*Unmanned Systems Integrated Roadmap…*, 28.

with approvals taking as long as 60 days.[56] Active efforts are underway to address this challenge, however. An April 2012 US Department of Defense (DoD) report to Congress on the future of UAS training, operations and sustainability notes that, "DoD is actively engaged in coordinating efforts on behalf of the Military Departments and Combatant Commands to shorten and simplify the FAA COA process to allow greater unmanned access to the NAS, with direct engagement through the interagency UAS Executive Committee (ExCom)."[57] The latter committee is made up of senior representatives from DoD, FAA, the Department of Homeland Security (DHS) and the National Aeronautics and Space Administration (NASA).[58] Their mission is to, "enable increased and ultimately routine access of Federal UAS engaged in public aircraft operations into the NAS to support operational, training, development and research requirements…"[59] Lobbying efforts are seeking to amend the FAA's legacy requirement for aircraft to be able to 'see and avoid' other aircraft, which currently routinely obliges UAS to be escorted when not being flown in restricted airspace. The emerging concept that is being proffered to replace 'see and avoid' is one that involves using emerging technologies to allow UAS to sense the presence of other manned aircraft or UAS. Described as "sense and avoid", it would potentially meet the FAA's requirement that UAS operate with an "equivalent level of safety" (ELOS) to manned aircraft.[60] At present, while research and experimentation is ongoing, progress towards an eventual solution has been slow.

---

[56]Walker, "Integrating Department of Defense Unmanned Aerial Systems….", 2.

[57]Department of Defense, Under Secretary of Defense for Acquisition, Technology and Logisitics, *Department of Defense Report to Congress on Future Unmanned Aircraft Systems Training, Operations, and Sustainability* (Washington, DC: US Government Printing Office, April 2012), ii.

[58]*Ibid.*

[59]*Ibid.*

[60]Walker, "Integrating Department of Defense Unmanned Aerial Systems….", 29-31.

Walker, in his U.S. Army Command and General Staff College master's thesis on the integration of DoD UAS into the NAS, notes that , "A significant amount of testing must still be done and the FAA is constrained by manpower in sifting through this data in an effort to reach a complete solution, which is still many years down the road."[61]

Regulatory limitations acknowledged, the US DoD is steadily building a UAS capability that is increasingly being used to support domestic surveillance activities. The US Air Force (USAF) currently operates a fleet of 256 UAS which includes the MQ-1B Predator (163 aircraft), MQ-9A Reaper (an armed version of the Predator - 70 aircraft), and RQ-4B Global Hawk (23 aircraft). Between now and 2017, they expect the number of MQ-1B Predator airframes to drop slightly to 110, and the MQ-9A Reaper inventory to increase substantially, from 70 to 256 aircraft. The RQ-4B Global Hawk inventory is expected to diminish slightly, from 23 to 15 airframes.[62] While the bulk of these systems are currently deployed on operations overseas, the USAF expects to have an ongoing requirement to train and conduct operational test activities with these aircraft in domestic airspace. An April 2012 US Department of Defense (DoD) report to Congress on the future of UAS training, operations and sustainability notes that, "As theatre forces return and the Military Departments' UAS fleets expand, DoD will require comprehensive continuation and Joint force training in the peacetime environment."[63]

Notwithstanding planned increases outlined in the latter document, recent open source reporting in the November 2012 edition of *Armed Forces Journal* suggests that the USAF is retrenching on its commitment to the expansion of UAS use, and has taken

---

[61]*Ibid*., 37.
[62]*Department of Defense Report to Congress on Future Unmanned Aircraft Systems…*, 2.
[63]*Ibid.,* 18.

steps to ground and mothball the RQ-4B Global Hawk fleet, in favour of continued use of manned U-2 surveillance aircraft with a shorter range. The USAF reportedly justified this decision by changing the surveillance orbit requirement from 1200 nm to 400 nm, which made the U-2 an acceptable compromise. Development of additional Global Hawk variants has been shelved, as has work on a medium-range UAS replacement for the MQ-1B Predator. Finally, acquisition plans for the MQ-9A Reaper have been halved, with only 24 systems per year to be added between 2013 and 2017, vice the 48 systems per year originally planned. The impetus for these cuts to planned UAS acquisitions is suggested to stem from the departure of US Secretary of Defense Robert Gates, and the retirement of the USAF Chief of Staff, General Norton Schwartz, who was replaced by General Mark Welsh in August 2012. Welsh, a fighter pilot, is alleged to favour manned aircraft systems.[64] While any assessment of the reasons behind the slowdown of USAF UAS adoption would be speculative, the change in momentum is noteworthy, and could undermine the anticipated greater availability of UAS systems between now and 2017.

The US Army has a larger fleet of UAS than the USAF, although the bulk of these are the RQ-11B Raven, a hand-launched short range platform, which can be operated using a simplified notification procedure over land owned or leased by the government.[65] Their larger UAS which require airfields for takeoff and landing include the MQ-5B Hunter (45 aircraft) and MQ-1C Gray Eagle (19 aircraft). While no growth in the Hunter fleet is expected, Gray Eagle holdings are expected to increase from 19 to 152

---

[64]Spinetta and Cummings, "Unloved Aerial Vehicles"
[65]*Department of Defense Report to Congress on Future Unmanned Aircraft Systems* …, 20.

platforms by 2017.[66] The implication is that greater numbers of platforms will increase demand for airspace access and place further pressure on FAA certification processes, barring progress in regulatory practices for access to the NAS.

The United States Navy (USN) and United States Marine Corps (USMC) also have small UAS fleets. . The USMC, in addition to their RQ-7B Shadow (52 aircraft), intend to increase their RQ-21A STUAS fleet from 8 to 100 by 2017. The USN currently has 5 RQ-4A Global Hawk systems, but intend to zero out their inventory in favour of the MQ-4C Broad-Area Maritime Search (BAMS) platform, which they will start acquiring in 2013. A fleet of 2 initial platforms will grow to 13 by 2017. Their MQ-8B Firescout /VTUAV holdings will grow from 5 to 37 by 2017, and they will eventually acquire 4 RQ-21A STUAS. Other systems include Scan Eagle (122 aircraft), and the X-47B UCAS-D fleet, which will eventually transition to UCLASS and grow from 2 to 4 platforms.[67] Increases in USN system numbers, particularly the BAMS, will improve their ability to persistently monitor the maritime approaches to North America.

It can be seen that the US services employ a wide variety of systems, some of which duplicate the capabilities of others. Of all the current systems in US military inventories, the long-range RQ-4B Global Hawk and medium-range MQ-1B Predator platforms of the USAF, and the USN's MQ-4C BAMS platform, are the most useful for domestic surveillance tasks. The broad areas involved lend themselves to the capability of systems such as the Global Hawk, which can fly up to 1200 nm to an area of interest, and then remain on station at altitudes up to 65,000 ft, providing surveillance for up to 28

---

[66]*Ibid*., 2.
[67]*Ibid.*

hours.[68] The platform can carry SAR, IR and electro-optical sensors, stream collected data in near-real time, and can search a 40,000 square nm area in 24 hours with 3 foot (~ 1 m) resolution.[69] This sort of broad area search capability, and the persistence it provides, is particularly useful for the surveillance of sparsely populated areas along each country's borders and along the coastlines of the North American continent. Future anticipated improvements to UAS capabilities include systems that are multi-mission and all-weather capable, increasingly net-centric or networked, and more capable of autonomous operations, including automated take off and landing.[70] Further expected improvements will include the ability to swarm multiple systems piloted by a single operator, the ability to accept requests for information and conduct collection management and prioritization autonomously, and the capability to detect and defend against threats.[71] The latter capacity, which would involve imparting machines with a level of artificial intelligence that raises legal and ethical questions, would be a step too far in the current legislative and regulatory environment, but the USAF's *Air Force UAS Flight Plan* notes that decisions about how far these systems will be empowered should be made sooner than later, in order to guide future development and acquisition.[72]

Of the systems in the current and planned DoD inventory, a number are already engaged in support to homeland security and other domestic surveillance tasks. The US began to fly DoD systems in February 2011 in support of the Mexican Government's

---

[68] *Air Force UAS Flight Plan...*,27.

[69] ---, RQ-4 Global Hawk Aircraft Factsheet, last modified [or accessed] 29 March 2013, http://air-attack.com/page/54/RQ-4-Global-Hawk.html

[70] *Air Force UAS Flight Plan...*, 33-34.

[71] *Ibid.*

[72] *Ibid., 41.*

efforts to fight transnational criminal organizations involved in drug trafficking.[73] A New York Times article published in March 2011 reported that, "… the Pentagon had flown a number of flights over the past month using the Global Hawk drones — a spy plane that can fly higher than 60,000 feet and survey about 40,000 square miles of territory in a day. They cannot be readily seen by drug traffickers...on the ground."[74] This cooperation was likely coordinated between US Northern Command and the Mexican military, and a Pentagon spokesman cited in the New York Times article noted that US DoD support was being provided in coordination with the State Department.[75] The US CBP also operates a fleet of UAS, currently consisting of 10 Predator B aircraft, which have provided coverage of the entire length of the US's border with Mexico since September 2010.[76] These CBP systems have also been used for domestic law enforcement purposes within the US. In June 2011, a sheriff in Nelson County, North Dakota requested CBP Predator B surveillance support to locate three fugitives suspected of stealing livestock. The CBP UAS was able to locate the suspects, who were found to be unarmed, and they were arrested by the authorities a short time later.[77] The US DoD, in support of CBP, also operates a fleet of Airborne and Tethered Aerostat Radar Systems (TARS), which provide what is described as, "low-level, "look-down" surveillance" along the United States' southern border, as well as some capability to monitor air approaches over the

---

[73]Ginger Thompson and Mark Mazzetti,"U.S. Drones fight Mexican Drug Trade," *New York Times*, March 15, 2011, last modified [or accessed] 5 February 2013, http://www.nytimes.com/2011/03/16/world/americas/16drug.html?_r=0&pagewanted=print

[74]*Ibid.*

[75]*Ibid*.

[76]Jay Stanley and Catherine Crump. *Protecting Privacy From Aerial Surveillance: Recommendations for Government Use of Drone Aircraft*. New York, NY: American Civil Liberties Union, December 2011. 7.

[77]Brian Bennet, "Police employ Predator drone spy planes on home front," *Los Angeles Times.* December 10, 2011, last modified [or accessed] 5 February 2013, http://articles.latimes.com/print/2011/dec/10/nation/la-na-drone-arrest-20111211

Caribbean.[78] The US DHS also uses DoD ground-based mobile radar systems for monitoring of threats on the borders, and for counter-narcotics operation in the Caribbean.[79]

These types of uses foreshadow the expectation of much broader uptake of UAS technology by civilian authorities in the US, which will have an impact on both the management of airspace as well as the useful integration of the collection from these systems, where desirable or warranted, into the air or maritime domain awareness picture. Several local police departments, small cities and towns in the US have already applied for FAA Certificates of Authorization (COA) in order to operate UAS[80], and the accessibility of the technology, which can cost as little as $300 for a hand-launched drone, has made it an attractive option for many organizations that would have previously been unable to afford it.[81] Uses for UAS in a domestic context include surveillance of suspects by police, search and rescue operations, and data gathering, both for routine purposes like pipeline monitoring, and natural disasters as well. Most civilian-use systems that exist at present are only equipped with imagery collection equipment, but experimentation is ongoing with other fittings, such as arms or claws that can be manipulated to pick up objects, and canisters that can be dropped with cargo. While many of these systems will operate in an essentially stand-alone capacity, and will not collect data relevant to the US Federal Government's surveillance needs, there is no doubt that

---

[78]*Integrated Air Surveillance Concept of Operations..., 8.*

[79]*Ibid.*

[80]Richard M. Thompson II, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses* (Washington, DC : U.S. Government Printing Office, September 6, 2012), 3.

[81]---, "The Dawning of Domestic Drones," *The New York Times.* December 25, 2012, last modified [or accessed] 9 March 2013, http://www.nytimes.com/2012/12/26/opinion/the-dawning-of-domestic-drones.html?_r=0

there will be an interest in being able to harness their feeds if required, for example, in the case of a domestic disaster or emergency. The US DHS is the likely department to ultimately oversee the integration of these new sensors over time, given their jurisdiction and the likely sort of events or issues, such as natural disasters or domestic emergencies that would generate data collection. One of the main challenges to integration will be the challenging array of different networks, software, data formats and technology employed by system users, which are difficult to de-conflict and harness, and which risk outstripping the capacity of processing systems. On the plus side, the growing civilian surveillance capability will complement military and CBP systems, creating redundancy and potential savings by allowing for federation of collection responsibility across multiple levels of government.

In addition to the challenge of sharing information, divergent or non-existent doctrine surrounding the command and control (C2) of UAS will also compromise effective operation of the web of UAS capabilities as a system in a domestic context. Efforts at de-confliction with allies, when conducting surveillance along borders, will complicate the task of collection coordination, as will divergent C2 practices amongst the US services. The USAF's doctrine, for example, emphasizes centralization of control and unity of command for air assets, under USAF personnel rather than supported elements, with the belief that this allows for the effective generation of air power effects.[82] Other organizations and services use their systems differently. The US Army has its UAS assets controlled at the divisional level, assigning them directly to commanders in a way that

---

[82]U.S Air Force, *Command and Control*, Air Force Doctrine Document (AFDD) 2-8 (Washington, DC: Department of the Air Force, 1 June 2007), 7.

enables local decision making but potentially sacrifices efficiency.[83] CBP and civilian agencies will also employ their UAS independently. Without centralized control of flight planning and collection objectives, a number of different organizations could potentially conduct surveillance that was duplicative or not analyzed and exploited to best effect.

The requirement to integrate US systems and surveillance management with that of Canada, while a longstanding problem, will further complicate the issue as new capabilities are introduced. At present, surveillance of Canada's airspace and maritime approaches is primarily conducted using a combination of radars, SIGINT, manned aircraft, naval vessels, and commercial satellite imagery.[84] Manned aircraft surveillance is generally conducted using the CP-140 Aurora long-range patrol aircraft. Canada has 18 CP-140, split between three squadrons. Greenwood, Nova Scotia, on the east coast, is home to 404 Squadron and 405 Squadron, and 407 Squadron is based in Comox, British Columbia. Approximately a quarter of the fleet is unavailable at any time, due to an ongoing life extension program which involves upgrades of some of the wing components.[85] The aircraft has a range of 5000 nautical miles and can routinely fly missions of 12 hours or more in duration. The Block 2 variant includes an MX-20 camera, which can capture electro-optical and infrared motion imagery.[86] Other CF aircraft, particularly fighters, can be used to respond to cuing from sensors and intercept

---

[83]Major David Buchanan, "Joint Doctrine for Unmanned Aircraft Systems: the Air Force *and* the Army Hold the Key to Success." Paper for Department of Joint Military Operations, US Naval War College, 3 May 2010, 5.

[84]*Canadian Forces National Surveillance Study...*, 25-27.

[85]Ken Pole, "Aurora's Appeal," *Canadian Skies*, 22 March 2012, last modified [or accessed] 1 October 2012, http://skiesmag.com/news/articles/16087-aurora-s-appeal.html.

[86]*Ibid.*

any detected threats. These aircraft have radar and other tactical sensors, as well as aircrew, who can assist in identifying the threat.

Naval vessels also augment the surveillance picture with their integral sensors. The RCN's fleet of Halifax Class Canadian Patrol Frigates and Iroquois Class Destroyers house active and passive surveillance sensor suites, which include radar and SIGINT-based capabilities. While line-of-sight and sensor limitations, as well as serviceability and availability, all have an impact on how much coverage these ships provide, they can provide relatively detailed airspace surveillance of focused areas.[87] The RCN ships routinely deploy with CH-124A Sea King Maritime Helicopters, which have radar and Forward Looking Infrared (FLIR) sensors that also contribute to limited local area surveillance in their patrol areas. Non-military aircraft also conduct some surveillance of Canadian territory and waters. TC uses four Dash 7 and Dash 8 fixed wing manned aircraft to provide pollution detection as well as ice monitoring for Environment Canada. While their surveillance suite is robust, including sideways looking airborne radar (SLAR), EO and infrared cameras, as well as an ultraviolet line scanner (UVIR) and an AIS receiver, they have limited ability to share the information they collect, and only their AIS data is incorporated into common operating pictures shared by the MSOCs.[88]

Canada, perhaps predictably, is well behind the US in the use of UAS technology for domestic surveillance. The reasons for this include limited user-driven demand for the technology, and the nature of Canadian Forces project management and procurement. The RCAF signaled intent to create a UAV squadron through the Joint Uninhabited

---

[87] *Canadian Forces National Surveillance Study...*, 2.7
[88] *Ibid.*, 42-43.

Surveillance and Target Acquisition System (JUSTAS) project as early as 2007, with an interim operating capability (IOC) to be place by 2010.[89] The involvement of the CF in the Afghan conflict was used as justification for a UAV capability, which was initially obtained between 2003-2009 through a contract which provided 7 CU-161 Sperwer tactical UAVs.[90] This system was upgraded in early 2009 through a three year contract with MacDonald, Dettweiler and Associates for the provision of 5 Heron UAV, acquired on an interim basis to allow for intelligence collection and force protection for Operation Athena, Canada's Joint Task Force-Afghanistan contribution, and employed as part of the Task Force Kandahar Air Wing as the Canadian Heron UAV Detachment (CHUD).[91] While the latter deployment created some institutional capacity to employ UAVs, the end of the combat mission in 2011 is expected to result in rapid skill fade for those personnel who worked with the system, either in flight operations and planning or analysis of the sensor imagery and data feeds. As of January 2013, the RCAF's planning documents suggest IOC for a UAV squadron is expected no earlier than 2017, and a CF spokesman indicated that options analysis is ongoing as the RCAF reviews its force structure requirements.[92]

Given this, it is likely that existing in-service UAS will make up the bulk of the CF's UAS capability for the near-term. Systems and capabilities currently being operated

---

[89]David Pugliese,"Canada's drone squadron still stalled, with neither planes nor troops," *Ottawa Citizen*, 27 December 2012, last modified [or accessed] 10 January 2013, http://www.ottawacitizen.com/technology/Canada+drone+squadron+still+stalled+with+neither+planes/7749650/story.html

[90]Royal Canadian Air Force, CU-161 Sperwer Overview, last modified [or accessed] 21 January 2013, http://www.rcaf-arc.forces.gc.ca/v2/equip/hst/cu161/specs-eng.asp

[91]Royal Canadian Air Force, CU-170 Heron Overview, last modified [or accessed] 21 January 2013, http://www.rcaf-arc.forces.gc.ca/v2/equip/hst/cu170/index-eng.asp

[92]Pugliese, "*Canada's drone squadron still stalled…"*

by the CF include the Boeing ScanEagle, which is provided on contract to the Royal Canadian Navy by Insitu Inc and ING Engineering of Ottawa.[93] The latter system was deployed to the Canadian Arctic with HMCS St. John's for the annual Operation NANOOK military exercise in 2012, and also flown most recently by HMCS Regina during its deployment to the Arabian Sea as part of Combined Task Force (CTF) 150 in the fall of 2012.[94] The ScanEagle is catapult launched, can stay aloft for up to 20 hours, and was used during the OP NANOOK exercise to support air and maritime disaster rescue efforts, while simultaneously testing its resilience and serviceability in cold weather conditions. In addition to the RCN's ScanEagle, the Canadian Army also maintains a limited UAV capability, having purchased 5 miniature UAVs, the Maveric system, from US-based Prioria Robotics.[95] These hand-launched UAS can be fitted with electro-optical or IR video cameras, and can fly for 45-75 minutes, at altitudes up to 16,000 ft.[96] Given the tactical nature of these systems, they would likely mainly be used in an expeditionary role, although scope would exist for their deployment in a domestic context on exercises or in aid to civil power scenarios. Besides this limited UAS capability, the main Arctic surveillance tool is the RADARSAT and RADARSAT-2 satellites operated by MacDonnell, Detweiller and Associates. These systems, which circle the Earth in a 101 minute sun-synchronous polar orbit, use a synthetic aperture

---

[93]David Pugliese, "ScanEagle Successful In Its Support to Canadian Forces in the Arctic Says Company," *Ottawa Citizen*, 8 October 2011, last modified [or accessed] 15 March 2013, http://blogs.ottawacitizen.com/2011/10/08/scaneagle-successful-in-its-support-to-canadian-forces-in-the-arctic-says-company/

[94]Lieutenant (Navy) Chris Walkinshaw, "HMCS Regina reports for duty," 17 September 2012, last modified [or accessed] 15 March 2013, http://www.cjoc-coic.forces.gc.ca/fs-ev/2012/09/17-eng.asp

[95]Kathy Staffa, "Prioria Awarded Canadian Defense Contract," *Prioria Robotics*, last modified [or accessed] 15 March 2013, http://www.prioria.com/media/documents/press/2010/Prioria_Canadian_Defence_Contract.pdf

[96]Prioria Robotics, *Maveric UAS* Configuration, last modified [or accessed] 15 March 2013, http://www.prioria.com/products/maveric-uas/configuration

radar (SAR) array with a resolution of approximately 10 metres, and provide relatively frequent over flight of the Arctic.[97] The capability they provide is the main data source for the Canadian Ice Service's monitoring of the Arctic's ice fields, and since 2012, the DND Polar Epsilon project has been delivering near-real-time MDA of Canada's maritime approaches, through contractor-operated ground stations that feed analyzed data to the MSOC in Halifax and Esquimalt.[98] The direction of this capability is controlled centrally in the former Canada Command (now CJOC-Continental), with a contractor-provided imagery analysis capability based in CJOC HQ in Ottawa.[99] The fact that direction of this capability is disconnected from the RCAF's Combined Air and Space Operations Centre's (CAOC) Intelligence Surveillance and Reconnaissance Division speaks to the ad-hoc nature of capabilities currently being fielded. The centralization of aerospace and maritime warning functions under NORAD suggests that 1 CAD, given its Canadian NORAD Region (CANR) responsibilities, would logically eventually assume responsibility for coordination of both maritime and aerospace surveillance for warning purposes of all approaches to Canada, including the Arctic.

The Arctic region surveillance problem is also the subject of experimental capability development. One Associate Deputy Minister (Science and Technology) (ADM (S&T) initiative that seeks to address existing shortfalls to collect surveillance data is the Northern Watch Technology Demonstration Project (TDP), which seeks to, "develop and demonstrate a capability to conduct up to 365 days, 24/7 persistent local

---

[97]Jeff Hurley, Presentation to SEASAR 2010, the 3rd Annual Workshop on Advances in SAR Oceanography from Envisat, ERS and ESA third party missions, 25-29 January 2010, last modified [or accessed] 15 March 2013, http://earth.eo.esa.int/workshops/seasar2010/8_Hurley.pdf

[98]*Ibid.*

[99]Captain Levon Bond, "JUSTAS and Project Epsilon: Integrated Intelligence, Surveillance, and Reconnaissance of the Canadian Arctic", Canadian Military Journal 11, no. 3 (Autumn 2011), 29.

area surveillance of air, maritime surface and sub-surface objects in the Canadian Arctic."[100] The timelines for this project, which began in 2007, include demonstrations of a remotely-operated capability which will conduct local surveillance in Gascoyne Inlet, Nunavut in 2014 and 2015. The initiative suggests that an explicit effort is being made to fill a shortfall in the CF's capability to conduct persistent surveillance, but also highlights the current limitations of the CF's existing platforms and systems, particularly in terms of persistence and scope. These acknowledged shortfalls have led to speculation that the CF might consider the purchase of 3 to 5 of Northrup Grumman's Arctic version of their Global Hawk UAS, dubbed the Arctic Hawk, for the purpose of northern surveillance. The Arctic Hawk UAS, which operates at 60,000 AGL, is capable of imaging the Northwest Passage four times during a standard mission, and can stay airborne for 24 to 35 hours.[101] It can stream its imagery as near real-time video to a ground station, and would provide coverage and persistence that would allow the CF to credibly discharge its existing surveillance responsibilities.[102]

While this overview of existing capabilities in both countries has focused specifically on current and projected future UAS acquisitions, it is apparent that the bulk of surveillance data collected at present is the product of radars and SIGINT sensors. The US has over 400 land-based radars, which include long-range, terminal and air defence

---

[100]Canada, Department of National Defence, ADM (S&T), *Technology Demonstration Program (TDP) Synopsis Sheet (TDP Project Approval) Northern Watch Technology Demonstration Project Version 2.04*, (Ottawa: DND Canada, 8 March 2012), 4.

[101]Carola Hoyos, "Canada looks to patrol Arctic with drone," *Financial Times*, 30 May 2012, last modified [or accessed] 12 January 2013, http://www.ft.com/intl/cms/s/0/0483a868-aa7a-11e1-9331-00144feabdc0.html#axzz2IfAo3SLG.

[102]Murray Brewster,"Ottawa considers high-altitude drones for Arctic Surveillance," *The Globe and Mail*, July 9, 2012, last modified [or accessed] 12 January 2013, http://www.theglobeandmail.com/news/politics/ottawa-considers-high-altitude-drones-for-arctic-surveillance/article4219537/.

systems, engaged in providing surveillance between ground level and 60,000 ft above MSL.[103] These types of systems provide a useful detection function, identifying anomalous targets for follow-on investigation by other collection sources, which currently consist almost exclusively of manned aircraft and maritime vessels. The fact that these secondary verifiers of the initial detections are manned by human crews, as previously noted, and lack the necessary endurance or persistence to provide more than a local and periodic look at any given area, is one shortcoming that UAS may be able to address in the longer term. *British Air and Space Power Doctrine* notes that, "Technology is also overcoming the lack of persistence that has been one of air power's traditional weaknesses: through space-based assets and high endurance UAVs, air and space power may now provide an unblinking eye."[104] There are several challenges that will need to be surmounted in order to develop this sort of capability, however. While the main technical issue is the design and ultimate construction of the networked system necessary for the development of shared situational awareness, which will be the focus of Chapter 4, the most significant policy issue is the combination of regulatory and legal concerns which threaten to limit the ultimate expansion of UAS use for domestic surveillance purposes. This policy issue is the subject of the next chapter.

CHAPTER 3: NATIONAL LEGAL CONSIDERATIONS

Legal and policy impediments in both Canada and the United States are currently preventing the full realization of the improved capability for continental surveillance that

---

[103]*Integrated Air Surveillance Concept of Operations..., 8.*
[104]*British Air and Space Power Doctrine…*, 47.

UAS offer. The chief impediments to rapid extension of UAS-enabled intelligence and information collection across the US are privacy concerns and dated Federal aviation legislation. In Canada, issues include dated Transport Canada policy documentation, and legal considerations associated with privacy rights that interfere with or prevent the collection and sharing of certain types of imagery and imagery-derived intelligence. Specific issues surrounding each state's current legal and policy frameworks, as well as initiatives underway and anticipated, will be examined with a view to identifying what progress can be expected towards the realization of each state's planned future ISR enterprise in the near-term.

Transport Canada currently requires anyone who wishes to use a UAS in Canadian airspace to apply for a Special Flight Operations Certificate (SFOC) at least four weeks before the intended flight, and to comply with a series of explicit conditions.[105] These include a detailed plan for the flight, which stipulates the boundaries of the area where it will take place, altitude and routes, and other data; details of the aircraft's technical specifications; as well as an emergency contingency plan and security plan for the flight, which addresses any hazards it might pose to persons or property on the ground. The Transport Canada website explains that, "while the ultimate goal is to "normalize" UAV operations within civil airspace, the industry technology is not mature enough, and the regulatory structure is not in place, to support routine operations."[106] The

---

[105]Graham McNaughton, "Halton police find $744K worth of drugs using high-tech pot-spotting drones," *National Post*, 13 September 2012, last modified [or accessed] 10 January 2013, http://news.nationalpost.com/2012/09/13/halton-police-find-744k-worth-of-drugs-using-high-tech-pot-spotting-drones/

[106]Transport Canada, "Personal Aviation, Special Flight Operations & Launch Safety: Unmanned Air Vehicle (UAV)," 3 May 2010, last modified [or accessed] 21 February 2013, http://www.tc.gc.ca/eng/civilaviation/standards/general-recavi-brochures-uav-2270.htm

website notes that the main factor which will allow for these flights to eventually become routine is the development of reliable detect, sense and avoid (DSA) technology, which will ensure collision avoidance capability for unmanned flights. The stated ambition is that the, "probability of a UAV colliding with another aircraft must be comparable to that for manned aircraft (i.e. an equivalent level of safety)."[107]

The US faces a similar policy hurdle to routine UAS flights, with the FAA COA process previously discussed creating the same sort of impediment as the Canadian SFOC requirement. The FAA's critics argue that the current COA process, which takes about 60 days to issue a waiver to fly a drone in US airspace, is not standardized, and is being overtaken by increasing demand which the agency is challenged to meet.[108] Where the US differs from Canada, however, is that there are active multi-agency efforts underway there to develop a workable way-ahead, with government legislative support. The US Federal Government, through the February 2012 *Federal Aviation Administration Modernization and Reform Act*, has mandated that the FAA resolve outstanding regulatory issues and open the NAS to UAS systems on a routine basis by September 2015.[109] The reason for this push in the US is primarily commercial; UAS manufacturing is expected to grow into a business worth more than $5 billion US, with demand for the systems anticipated across a variety of civilian sectors. No similar urgency to update legislation is being displayed in Canada, and it is likely that any Canadian amendment to

---

[107] *Ibid.*

[108] Jason Koebler, "Report: Regulatory Mess May Hold Up Domestic Drone Revolution," *U.S. News & World Report*, 17 December 2012, last modified [or accessed] 12 January 2013, http://www.usnews.com/news/articles/2012/12/17/report-regulatory-mess-may-hold-up-domestic-drone-revolution.

[109] *Ibid.*

Transport Canada policy will only come in the wake of capability advancements and changes to FAA regulations.

Notwithstanding the permit requirements for UAS flight in each country, demand for the systems has grown unabated, as they are perceived to provide a force-multiplying effect to agencies and organizations that are unable to afford manned air support of their operations. In the current absence of legislation proscribing UAS use, police departments across the US have begun to acquire them, and there is an expectation that they will be deployed in ever-increasing numbers. The US FAA has approved 348 applications for domestic use of UAS as of early January 2013, and of these, more than 50 percent belonged to the Defense Department. Law enforcement use remains limited, representing only 7 percent of the applications received to date, but the possibility of growth in this segment is a significant public privacy concern.[110] A 10 January 2013 *USA Today* article notes that 10 state legislatures, as well as the US Congress, are expected to consider legislation this year that would seek to limit the domestic use of UAS.[111] Legislation in Florida, for example, has received initial assent in the state legislature, and as of end-March 2013, was in committee with an expectation that it would come to the house for a vote in the near-term.[112] The issue of privacy concerns is currently being downplayed by the aircraft industry, which is working aggressively and lobbying Congress to ensure that its ability to sell systems is not undermined by restrictive legislation. The possibility of

---

[110]Judy Keen, "Citing privacy, critics target drones buzzing over USA," *USA Today*, 10 January 2013, last modified [or accessed] 12 January 2013, http://www.usatoday.com/story/news/politics/2013/01/10/domestic-drones-backlash/1566212/

[111]*Ibid.*

[112]Kyle Munzenrieder, "Florida Bill Would Limit Miami-Dade Police's Use of Drones," *Miami New Times*, 28 March 2013, last modified [or accessed] 30 March 2013, http://blogs.miaminewtimes.com/riptide/2013/03/florida_bill_would_limit_miami.php

legal limitations to UAS use on both sides of the border is of concern to military and civilian users alike. While there is no doubt that privacy and civil liberty concerns have some merit, there is doubtlessly scope to satisfy critics while still expanding UAS use. The challenge for lawmakers and system users on both side of the border is to reassure the public that their initiatives will not qualitatively alter current expectations of privacy.

What specific risks to privacy does domestic UAS use pose? Many of the concerns posed by US critics of these systems represent a fundamental opposition to surveillance in any form, even though a number of surveillance methods have been acknowledged to be constitutionally compliant through past jurisprudence. Examples of this include the right to monitor and track an individual when they are in public areas, and the right of police to conduct surveillance of individuals in their homes when those individuals are in public view from the outside.[113] The fact that surveillance of this sort could become persistent is what concerns privacy advocates, and any movement in the latter direction would cross the line from a constitutional perspective.[114] UAS offer this prospect of persistence, and the vision of the government, which involves aggregating data from various collection sources and making it available in real-time to multiple users, will further enable the former to achieve persistent surveillance of the sort the ACLU fears.[115] Notwithstanding this possibility, current technological constraints, as previously noted, make this apprehension an unlikely prospect in the near-term. Nonetheless, the vigour of public opposition to the prospect of persistent surveillance

---

[113]Richard M. Thompson II, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*. (Washington, DC: U.S. Government Printing Office, 6 September 2012), 4-6, 8-9.

[114]*Ibid.*, 9.

[115]Stanley and Crump, *Protecting Privacy From Aerial Surveillance…*, 1-2.

appears to be growing. Law enforcement agencies occasionally use loose language to describe surveillance capabilities, or to muse about possible uses for the latter, and this has further fuelled public concern. This concern has manifested itself in opposition to the acquisition of UAS by LEA, and in attempts to legislate restrictions, at both the state and federal level, to UAS use for domestic purposes.[116] In the US House of Representatives, for example, a bi-partisan bill proposed by Republican Representative Ted Poe (Texas) and Democratic Representative Zoe Lofgren (California) in February 2013, H.R. 637, titled "The Preserving American Privacy Act of 2013", seeks to prevent the use of weapons on domestic UAS, to limit the collection of imagery or voice intercepts where a reasonable expectation of individual privacy exists, and to prevent federal pre-emption of state laws limiting the use of UAS in their airspace.[117] The bill also explicitly seeks to minimize the amount of information collected, and limit both the time that it can be retained and how it can be shared. Further, it seeks to ensure that stringent oversight and collection approval processes are in place, to include public notification of the collection activity, and a process for public feedback on the proposed collection.[118] It is obvious that broad and detailed constraints of this sort run counter to many of the benefits of the sharing and aggregating of collected information that are envisaged in future domestic surveillance plans. If data cannot be collected once and used for multiple purposes, or

---

[116]Declan McCullagh, "Anti-drone revolt prompts push for new federal, state laws," CNET, 22 March 2013, last modified [or accessed] 28 March 2013, http://news.cnet.com/8301-13578_3-57575863-38/anti-drone-revolt-prompts-push-for-new-federal-state-laws/

[117]Congresswoman Zoe Lofgren, "Reps. Zoe Lofgren and Ted Poe Introduce Bipartisan Bill to Protect Americans' Privacy Rights from Domestic Drones," Congresswoman Zoe Lofgren US House of Representatives website, last modified [or accessed] 28 March 2013, http://lofgren.house.gov/index.php?option=com_content&view=article&id=785:reps-zoe-lofgren-and-ted-poe-introduce-bipartisan-bill-to-protect-americans-privacy-rights-from-domestic-drones&catid=22:112th-news&Itemid=161

[118]*Ibid.*

shared between agencies without constraints on its use, impacts will include less timeliness in the creation of shared situational awareness, and an undermining of the potential for self-synchronization that is inherent in networked enterprises. There is no doubt that current processes for inter-agency data sharing, based on data push, extensive liaison, and frequent inter-agency exercises and coordination meetings, will continue to surmount these types of challenges. Attempts to develop technological fixes, using measures such as network firewalls, meta-data tagging and caveats to regulate the flow of data between agencies through their networks, will also continue. These measures will doubtlessly have some positive impact, but they will not fully unfetter the data flow. While it is impossible to predict the eventual outcome of the political and legislative process currently underway, it is likely that the US system of political checks and balances, and constitutional considerations, will ensure that any legislation that is eventually passed will constrain the potential capability that UAS data collection offers. Further, it is likely that it will take both time, and demonstrated restraint on the part of UAS-equipped LEA, to convince the public that these systems can and will be used responsibly in a way that does not threaten the public interest.

Canadian legal issues concerning domestic surveillance activity also pose limitations on what can be collected, and how or if it can be shared either internally or with the US services and agencies. Within Canada, surveillance by the CF of Canadian citizens, permanent residents, or corporations incorporated in Canada is proscribed by law, and any surveillance data collected by police or other government agencies would also be subject to legal and privacy considerations.[119] While this limitation does not

interfere with surveillance of airspace and maritime approaches for sovereignty purposes, it places constraints similar to those in the US on the collection of imagery or video

One additional public concern, which goes beyond the issue of privacy, is the fear that persistent UAS surveillance will be coupled with the ability to take armed action remotely, using systems like the Hellfire missile-equipped MQ-9A Reaper for attacks on US soil. While there has been no specific mention in available US policy documents of any ambition to deploy armed UAS for domestic missions, the routine use of these systems for targeted assassinations abroad have created apprehension and spurred public debate. An ongoing ACLU legal challenge questioning the constitutionality of a US drone strike in Yemen in 2011, which killed three US citizens who were members of al-Qaeda, highlights the fear that actions of this sort could create a precedent for similar strikes inside the US.[120] Further, there is concern that the US use of UAS-delivered attacks on targeted individuals abroad is creating customary practices that may eventually be used by other states as justification for similar attacks, including attacks on US soil. Kurt Volker, a former US Ambassador to NATO, argued in a 26 October 1912 *Washington Post* opinion piece that the US monopoly on the use of UAS systems for targeted attacks will not last, and cautioned that when other states, such as China or Russia, also begin using these systems to kill terrorists in contested areas, it will be difficult to frame a rule-based response given the manner in which the practice has evolved.[121] Issues of this nature, while not specifically related to surveillance, are

---

[119]*Canadian Forces National Surveillance Study…*, 9-10.

[120]Ian Munroe, "Meet the Canadian challenging America's drone war," *CBC* News, 5 April 2013, last modified [or accessed] 5 April 2013, http://www.cbc.ca/news/world/story/2013/04/04/us-cia-drone-strikes-legal-challenge-jameel-jaffer.html

informing public debate in both Canada and the US, and will inevitably have an impact on the future of UAS use in each country.

In this chapter, we have seen that unresolved legal and regulatory issues in both Canada and the US threaten the near-term expansion of UAS use for domestic surveillance. The use of capabilities already in existence is being increasingly constrained by new legislation, while persistent regulatory hurdles to routine UAS use in the skies of both countries will take more time to surmount. It seems apparent that only the continued development of new technologies will perform the forcing function necessary to spur movement towards greater UAS use. The impact of the availability of new capabilities, however, will still be limited by the various factors discussed in the preceding chapters. The final chapter will examine the way-ahead for the North American surveillance regime, given the challenges already discussed, as well as the persistent impact of various sources of friction on any meaningful progress beyond the status quo.

CHAPTER 4: POSSIBLE MODELS FOR THE FUTURE NORTH AMERICAN SURVEILLANCE ENVIRONMENT

A look at the experience of some of the defence partners of Canada and the US may offer suggestions for a way-ahead in the North American context. The theme of holistic national UAS capability development is shared by Australia and the UK, and is reflected, as discussed in Chapter 1, in US and Canadian defence approaches to future capability development in the ISR domain. The need for interoperability with key allies is

---

[121]Kurt Volker, "What the U.S. risks by relying on drones," *Washington Post*, 26 October 2012, last modified [or accessed] 5 April 2013, http://articles.washingtonpost.com/2012-10-26/opinions/35500650_1_drone-strikes-drone-attacks-guantanamo-bay

another common stated objective. Australia's *Defence ISR Roadmap 2007-2017* posits a future paradigm that will see Australian forces able to move from sharing an ISR operating picture to operating "interdependently with Allies and partners."[122] Australian force development efforts acknowledge the desirability of having a holistically coordinated approach to acquisitions and capability management, and a "Coordinating Capability Manager" has been appointed to ensure coordination for capability development between the services and groups.[123] The UK is similarly mindful of the desirability of ensuring that future systems allow for the seamless exchange of data, and also allow for the possibility of development and acquisition of future UAS systems in concert with other allies.[124] NATO, in its *Strategic Concept of Employment for Unmanned Aircraft Systems in* NATO, seeks to break down potential barriers to interoperability among the NATO allies by codifying UAS categories, based on weight and employment. The document also noted the necessity of ensuring, "...full operational integration with respect to ... information collection and dissemination."[125] Canadian and US capstone documents also acknowledge the importance of being able to share data, but do not explicitly mention any intent to coordinate bi-national capability acquisitions, whether for collection, processing or networked sharing. This appears to be the result of a realist approach to policy development, which acknowledges that national imperatives will prevent broader integration. However, given the financial constraints that are

---

[122]Department of Defence, *Defence ISR Roadmap 2007-2017* (Australia: Australian Government, 30 August 2007), 6.

[123]*Ibid*., 11.

[124]Department of Defence, Joint Doctrine Note 2/11, *The UK Approach to Unmanned Aircraft Systems*, JDN 2-11, 30 March 2011, 1-2,1-4.

[125]Joint Air Power Competence Centre, *Strategic Concept of Employment for Unmanned Aircraft Systems in NATO*, January 2010, 17.

currently informing policy and acquisition decisions in both countries, and the likelihood that these constraints will remain a factor for some time, it is worthwhile to consider what greater integration might be possible.

One possible future for the North American surveillance environment would see independent Canadian and US approaches to collection and information management that are not integrated in a meaningful way, as a result of differing national legal frameworks that prevent collection and sharing in various contexts, and incompatible UAS that do not allow the near-real time population of an inter-agency bi-national information environment that provides shared situational awareness. While persistent legal limitations on the sharing of surveillance data between the two states will exist, the key impediments to broad progress in creating a surveillance regime involving shared responsibilities, such as an updated or enhanced NORAD, will include limited budgetary capacity to fund improved collection capabilities, and inability on both sides of the border to break down the walls between various agencies and their mandates. While it is anticipated that technological advancements will bring down the cost of persistent surveillance dramatically over time, and will allow for automated detection and prioritization of targets, legal and politically-motivated limitations to the leveraging of this technology, informed by both sovereignty concern and organizational mandates, will delay its widespread adoption. It is unlikely that anything other than a significant existential threat to North America, spawned by some as yet unforeseen technological advance, will provide the necessary impetus to overcome the friction that will impose all but halting progress beyond the status quo.

This said, what would an ideal future continental surveillance system look like? A review of the elements contained in the literature discussed in the preceding chapters suggests that it would consist of an improved formal surveillance partnership, based on an existing international agreement such as NORAD, that involves heavily integrated and complementary surveillance organizations, discrete national responsibilities, and routine sharing, supported by a legal framework that is de-conflicted and respectful of privacy concerns in both states. If the premise that a future integrated system can be developed is accepted, and it is acknowledged that the main impediments are related to information management and mandates, how can these limitations be overcome? The various CONOPS and plans put forward independently by both the US DoD and the CF to describe the future surveillance environment argue that improvements to sharing of information, networking of systems and meta-tagging of data will ultimately enable the vision of information dominance and persistent surveillance that they espouse. The challenge to this premise is that it is based on an imperfect understanding of the nature of complex adaptive systems (CAS), and how they ultimately function.

CAS theorists Alex and David Bennet argue that an organization seeking to develop CAS processes for their enterprise must embrace concepts such as organizational intelligence, unity and shared purpose, and knowledge centricity.[126] Organizational intelligence is defined as, "the ability of an organization to perceive, interpret and respond to its environment in a manner that meets its goals while satisfying multiple

---

[126]Alex Bennet and David Bennet. "Designing the Knowledge Organization of the Future: The Intelligent Complex Adaptive System," in Handbook on Knowledge Management 2: Knowledge Directions (Heidelberg: Springer-Verlag, 2003), 625.

stakeholders."[127] The idea is that the perceptions of various individuals, aggregated, are synergistic and offer more insight, while creating more knowledge and understanding, than the individuals would be able to create on their own. The challenge with this concept is that it ignores the friction inherent in organizations, which arises as a result of challenges of synchronization of understanding across a broad group in a timely way. Unity and shared purpose, and knowledge centricity, which is defined as, "the aggregation of relevant information derived from the knowledge of the organization's components that enables self-synchronization and increase collaborative opportunities...", are similarly undermined by the impact of friction.[128] This friction, which currently exists between each state's military and myriad domestic organizations, can only be potentially overcome through the amalgamation of the various constituent parts of the national surveillance enterprise into a single organization. The subsequent integration of each state's national organizations, in a construct similar to NORAD, may be the only way to further limit the impact of friction and enable the creation of the organizational intelligence that Bennet and Bennet discuss.

In addition to the general effects of friction, the system envisioned in the extant national CONOPS of each state will also suffer from specific challenges to the creation of shared purpose. An occasional lack of agreement or shared purpose will inevitably occur as a result of divergent national imperatives. While obvious threats to the North American continent, such as an inbound ballistic missile, can be easily detected and agreed by both states, less apparent asymmetric threats that require intelligence

---

[127]*Ibid*, 626.
[128]*Ibid*, 631.

collection, data aggregation and analysis, potentially conducted by multiple agencies over a longer duration of time, may challenge the development of shared purpose. Reasons for this include the fact that agencies may not agree on the urgency of the threat, or its potential impact. They may also disagree, as a corollary, over how many resources to allocate to its investigation or prosecution, further undermining the development of shared purpose. Efforts to develop shared purpose across intelligence collection and production agencies in a multi-agency and/or multi-national context, both in peacetime and in coalition operations, have been routinely challenged by disagreement on resource allocation, even in the face of an agreed threat, given that collection and analysis assets are always in short supply.[129] Given this, it seems apparent that shared purpose would be even more difficult to achieve if the threat was not broadly recognized and accepted. Another consideration which will also impact the achievement or maintenance of shared purpose is the unpredictability that is caused by interaction between the threat agent and the surveillance and response system. Any reaction on the part of the threat to its detection by the system, and any subsequent actions, will further challenge the maintenance of shared purpose, particularly if the action is unforeseen and requires coordination between the two states to decide a response.[130]

Finally, self-synchronization is another concept that a future bi-national surveillance enterprise will be challenged to achieve, both as a result of friction and imperfect shared purpose. The US *Integrated Air Surveillance Concept of Operations*,

---

[129]Keith Button, "As U.S, Navy Consolidates Spy Plane Units, Critics Say ISR Will Suffer," *Defense News*, 6 November 2012, last modified [or accessed] 5 April 2013, http://www.defensenews.com/article/20121106/C4ISR01/311060007/As-U-S-Navy-Consolidates-Spy-Plane-Units-Critics-Say-ISR-Will-Suffer

[130]Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 197.

among a list of desired operational capabilities for a future system, includes the ability of every air surveillance partner to, "...contribute to, access, analyze and share surveillance data and surveillance-related information in accordance with pre-established authorizations."[131] Self-synchronization, ostensibly a benefit that accrues from networked access to information, is dependent on the accuracy of the information that is shared. While unanalysed data, such as imagery and radar feeds, can be pooled and made available to multiple users with little fear of potential inaccuracy, any analyzed or assessed information, or intelligence, will be inaccurate to a certain degree by necessity if it is predictive and is disseminated in a timely way. This inaccuracy will defeat self-synchronization to some extent, as the potential for erroneous action, taken on the basis of misunderstood or untrustworthy intelligence, will oblige a degree of centralized control that will inhibit the impact of self-synchronization efforts. Self-synchronization is also arguably effective only if the organization's personnel are highly trained, and this requires a degree of consistency of staffing, and accrued experience, that often defies achievement in military organizations and their civilian governmental counterparts. As a result, the Canadian and US Governments, even if they are able to achieve the necessary levels of interconnectivity and timeliness in data exchange that would be necessary to permit self-synchronization, are unlikely to be able to surmount the latter's inherent conceptual limitations.

The conceptual limitations of the intelligent CAS that Bennet and Bennet propose are exacerbated by the fact that any networked operational concept will be obliged to follow one of two approaches, which are outlined in Yaneer Bar-Yam's paper on the

---

[131] *Integrated Air Surveillance Concept of Operations...*, 27.

complexity of military conflict, mentioned in Antoine Bousquet's *The Scientific Way of Warfare*. Bar-Yam explains that in the first approach, self-organizing networked agents take individual actions which lead to effective collective functioning of the organization. In the second approach, decision makers receive networked information from an array of sensors and control the operation of the organization.[132] As Bousquet notes, in the second approach, "there is no sense in which a true network has replaced a hierarchical structure."[133] Given the disparate nature of the entities involved in gathering information, making assessments, and ultimately taking decisions about how to react to any intelligence or detection gained from surveillance of the North American terrain of Canada and the US, it is highly unlikely, despite the conceptions offered in the various Canadian and US CONOPs and plans, that any self-organizing networked action will be enabled to occur in the near-term. As a result, increased networking of Canadian and US ISR enterprises is more likely to simply better enable decision makers at the top of each nation's political hierarchy over time.

Given these observations, are the long-term ISR plans and aspirations of the Canadian and US governments generally unachievable? To a certain extent, if the current national organizational paradigms persist, they are. To achieve more than simple improved networked support to the current hierarchical decision-making process, each state must be prepared to seek unprecedented levels of integration in their ISR enterprises if they are to make even limited progress in achieving their respective visions of future

---

[132]Yaneer Bar-Yam, "Complexity of Military Conflict: Multiscale Complex Systems Analysis of Littoral Warfare," New England Complex Systems Institute, 2003, 23-24, last modified [or accessed] 12April 2013, http://necsi.org/projects/yaneer/SSG_NECSI_3_Litt.pdf

[133]Bousquet, *The Scientific Way of Warfare...*, 227.

CAS-enabled surveillance and information management. Notwithstanding limitations to integration posed by sovereignty and legal constraints, any practical progress of acquisition programs that might begin to improve collection or networking is unlikely in the current fiscal and political environment. Despite the potential that UAS offer, Canada and the US each face financial constraints that will also adversely impact their ability to purchase new systems in the near-term. Consequently, while it is anticipated that there will be a significant increase in the availability of surveillance data over time, the acquisition horizons discussed in Chapter 2 suggest that new UAS will not become available in Canada before 2017, and likely much later, given ongoing constriction of the DND budget. In the US, similar financial challenges, particularly austerity measures involving sequestration of defence funds that could cut as much as US$500 Billion over the next 10 years, are forcing re-examination of acquisition planning and may lead to delay in the planned purchase of additional capability.[134] These realities will come into conflict with military aspirations on both sides of the border, and may also lead to friction between the two countries, as Canada may be asked to contribute more than it has in the past to the collective continental surveillance problem.

If aspirations for a radically improved North American surveillance regime are not achievable, what does the future hold? The most likely near-term outcome, when current political trends and anticipated future technological developments are taken into account, is a system that will be marginally more capable and better integrated than what

---

[134]William Welsh, "March sequester would degrade US defense forces, says Panetta," *Defense Systems*, 11 January 2013, last modified [or accessed] 28 March 2013, http://defensesystems.com/Articles/2013/01/11/panetta-sequestration-threat-briefing.aspx?Page=1

exists at present. Positively motivated US and Canadian government agents prepared to share, but not fully enabled as a result of less than compatible systems, will find ways to move data between the two countries, to coordinate collection responsibilities, and to improve the coverage that exists at present. UAS will be increasingly leveraged to conduct this collection, particularly on the Northern and maritime approaches to the continent, and on each state's borders. Data standards will be further harmonized to allow for tailored access and security to be applied, and more autonomous analysis and collation capabilities will be developed, which will improve the processing latency for data collected, and address the anticipated expansion of data collection. All of these improvements will occur in an iterative fashion, and change is expected to be evolutionary, vice revolutionary.

This change is not expected to occur simultaneously on both sides of the border. In Canada, financial constraints and the traditional reliance on geography and the US as the source of continental defence will cause any improvements to current surveillance activity to be slow. The most emphasis will likely occur in the Arctic, an area that is currently underserved by surveillance effort and one that will increasingly be at risk of incursion given ongoing climate-change induced effects on the region's waters. Canada can expect to receive some pressure from its US partners to improve surveillance of this region, and it will be in its national interest to do so. In the US, the threat of trans-national criminal activity, particularly smuggling of drugs and persons across its borders, will be the greatest driver for improvements to domestic surveillance capability. This threat will likely be used to sustain existing military UAS capabilities and skill sets, and to build on existing NORTHCOM relationships with its domestic partners. Legal and

political concerns will temper this effort, however, further ensuring that any change or growth in UAS use will be iterative and halting.

The picture painted by this analysis suggests that UAS may not have as significant an impact in the near-term, despite their potential, as would be expected. In fact, the specific qualities of UAS, particularly their cost-effectiveness and ability to conduct persistent surveillance, will ensure their continued development and integration into each country's surveillance regimes. The limited numbers of UAVs already in service will likely be supplemented over time by small additional purchases, and financial constraints on both sides of the border can be expected to lead to greater standardization of fleets. Domestic stakeholders in the US, particularly NORAD, NORTHCOM, DHS, and CBP, and their Canadian partners in CJOC, RCMP, CBSA and TC, will learn to integrate UAS into their operations, and will continue to develop useful processes for exploiting their capabilities in an iterative way. Influences on future UAV acquisition in Canada can be expected to mirror those that have driven past purchases and leases. The CF's Chief of Force Development organization can be expected to monitor new capabilities and technologies being developed, and to propose new UAS acquisitions which address potential threats or tasks that the Canadian Government has levied on the CF Acquisition projects will be launched to purchase these capabilities, and the CF will determine how to employ them and incorporate them into its enterprise once, and if, they are delivered. This is an important point; the CF's success in acquiring new UAS will ultimately depend on political interest, the economy, and a host of other factors that have little to do with actual needs, and Canada may, like the US, delay expanding into more aggressive UAS use, even if they are proven superior in cost-effectiveness to manned

surveillance flights. This delay, if it occurs, will likely be influenced by funding limitations, and by a CF preference to preserve its existing manned aircraft capability. The impact of these various limiting factors on future UAV capability acquisition and on employment of existing capabilities will be a delay to expansion of UAS use in the near-term, which can be expected to persist until major legislative, political and organizational challenges are addressed.

CONCLUSION

This paper has argued that the growth in the availability of UAS will have a significant impact on the North American surveillance environment, but that legal and political constraints will temper this impact. It has been seen that current regulatory frameworks for domestic airspace use pose a near-term obstacle to greater UAS employment for surveillance of US and Canadian territory before 2015. Further, fiscal constraints in both Canada and the US will delay acquisition and deployment of additional UAS, with Canadian military acquisition programs specifically expected to encounter significant delays out to at least 2017 and likely beyond. Privacy considerations, particularly in the US, are leading to a regulatory backlash and attempts by the ACLU and other lobby groups to sponsor legislation that will severely limit domestic surveillance, and these efforts will likely further undermine the ultimate growth of UAS-enabled domestic surveillance.

Against this backdrop, military planners in both Canada and the US have developed CONOPs and acquisition plans built around the desirability and promise of networked decision-making enabled by shared surveillance information. It has been

demonstrated that the premises behind these CONOPs are highly reliant on self-synchronization and automation of collection that can only occur in an environment where issues of regulation, accountability and authority are resolved. It has been shown, however, that the creation of an environment of this sort is unlikely. In fact, given national imperatives, the current paradigm, which sees highly hierarchical decision-making enabled by the availability of networked information, is likely to persist. There is no doubt that UAS use, over time, will continue to improve the persistence and the quality of surveillance data, but it is unlikely, barring a significant change to regulatory, legal and policy constraints in each country, that the technology will deliver the promise of networked self-synchronization that each country's military planners envision. Nonetheless, UAS use will inevitably increase, if only because the cost-effectiveness and persistence that these systems offer. Persistent threats to the sovereignty of both the United States and Canada, particularly in the Arctic, on international borders, and on the East and West coast maritime approaches to the continent, will cause each state to address the problem of surveillance in a more thorough way to meet the range of threats that they face. UAS will doubtlessly continue to be a part of this response, and their adoption can only be expected to grow over time.

BIBLIOGRAPHY

---, "The Dawning of Domestic Drones." *The New York Times. 25* December 2012. Last modified [or accessed] 9 March 2013, http://www.nytimes.com/2012/12/26/opinion/the-dawning-of-domestic-drones.html?_r=0

---, RQ-4 Global Hawk Aircraft Factsheet. Last modified [or accessed] 29 March 2013, http://air-attack.com/page/54/RQ-4-Global-Hawk.html

Australia. Department of Defence. *Defence ISR Roadmap 2007-2017.* Australia: Australian Government, 30 August 2007.

Bar-Yam, Yaneer. "Complexity of Military Conflict: Multiscale Complex Systems Analysis of Littoral Warfare." New England Complex Systems Institute, 2003. Last modified [or accessed] 12 April 2013, http://necsi.org/projects/yaneer/SSG_NECSI_3_Litt.pdf

Bennet, Alex and David Bennet. "Designing the Knowledge Organization of the Future: The Intelligent Complex Adaptive System." in *Handbook on Knowledge Management 2: Knowledge Directions.* Heidelberg: Springer-Verlag, 2003.

Bennet, Brian. "Police employ Predator drone spy planes on home front." *Los Angeles Times*, December 10, 2011. Last modified [or accessed] 5 February 2013, http://articles.latimes.com/print/2011/dec/10/nation/la-na-drone-arrest-20111211.

Bond, Captain Levon. "JUSTAS and Project Epsilon: Integrated Intelligence, Surveillance, and Reconnaissance of the Canadian Arctic", *Canadian Military Journal* 11, no. 3 (Autumn 2011): 24-29.

Bousquet, Antoine. *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. New York: Columbia University Press, 2009.

Button, Keith. "As U.S, Navy Consolidates Spy Plane Units, Critics Say ISR Will Suffer." *Defense News*, 6 November 2012. Last modified [or accessed] 5 April 2013, http://www.defensenews.com/article/20121106/C4ISR01/311060007/As-U-S-Navy-Consolidates-Spy-Plane-Units-Critics-Say-ISR-Will-Suffer

Brewster, Murray. "Ottawa considers high-altitude drones for Arctic Surveillance." *The Globe and Mail*, July 9, 2012. Last modified [or accessed] 12 January 2013, http://www.theglobeandmail.com/news/politics/ottawa-considers-high-altitude-drones-for-arctic-surveillance/article4219537/.

Buchanan, Major David. "Joint Doctrine for Unmanned Aircraft Systems: the Air Force *and* the Army Hold the Key to Success." Paper for Department of Joint Military Operations, US Naval War College, 3 May 2010.

Canada. Department of Fisheries and Oceans. "Canada's Ocean Estate: A Description of Canada's Maritime Zones." Last modified [or accessed] 12 February 2013, http://www.dfo-mpo.gc.ca/oceans/canadasoceans-oceansducanada/marinezones-zonesmarines-eng.htm#terr

Canada. Department of National Defence. *Canada First Defence Strategy*. Ottawa: DND Canada, 18 June 2008.

Canada. Department of National Defence, CFJP 2.0, *Intelligence*. Ottawa: DND Canada, October 2011.

Canada. Department of National Defence, CFJP 3.0, *Operations.* Ottawa: DND Canada, July 2010.

Canada. Department of National Defence, Vice Chief of Defence Staff, *Intelligence Surveillance and Reconnaissance Operating Concept*. Ottawa: DND Canada, 26 September 2012.

Canada. Department of National Defence, Chief of Force Development. *Canadian Forces National Surveillance Study 2010 (U)*. Ottawa: DND Canada, 15 January 2011.

Canada. Department of National Defence, ADM (S&T). *Technology Demonstration Program (TDP) Synopsis Sheet (TDP Project Approval) Northern Watch Technology Demonstration Project Version 2.04*. Ottawa: DND Canada, 8 March 2012.

Canada. Department of National Defence, Vice Chief of Defence Staff. *Program Activity Architecture*. Last modified [or accessed] 13 February 2013, http://www.vcds.forces.gc.ca/sites/CProg/Resources/Internet/PAA-AAP/PAA%20Structure%20FINAL.pdf.

Canada. Royal Canadian Air Force. *CU-161 Sperwer Overview*. Last modified [or accessed] 21 January 2013, http://www.rcaf-arc.forces.gc.ca/v2/equip/hst/cu161/specs-eng.asp

Canada. Royal Canadian Air Force. *CU-170 Heron Overview*. Last modified [or accessed] 21 January 2013, http://www.rcaf-arc.forces.gc.ca/v2/equip/hst/cu170/index-eng.asp

Canada. NAV Canada, *TP1820E Designated Airspace Handbook*. Ottawa: Minister of Transport, 10 January 2013. Last modified [or accessed] 13 February 2013, http://www.navcanada.ca/ContentDefinitionFiles/Publications/AeronauticalInfoProducts/DAH/DAH_current_EN.pdf.

Canada and United States. *Agreement between the Government of the United States of America and the Government of Canada on the North American Aerospace Defense Command*, 28 April 2006.

Elias, Bart. *Pilotless Drones: Background and Considerations for Congress Regarding Unmanned Aircraft Operations in the National Airspace System.* Washington, DC: U.S. Government Printing Office, September 10, 2012.

Grimmett, Richard F. and Rebecca S. Lange. *Intelligence, Surveillance and Reconnaissance (ISR) Acquisition: Issues for Congress*. Washington, DC: U.S. Government Printing Office, September 10, 2012.

Huddleston, Major Iain. "Canada First?: Defence Strategy and the Future Aerospace ISR 'System of Systems", MDS Research Project Paper, Canadian Forces College, 2009.

Hoyos, Carola. "Canada looks to patrol Arctic with drone." *Financial Times*, 30 May 2012. Last modified [or accessed] 12 January 2013, http://www.ft.com/intl/cms/s/0/0483a868-aa7a-11e1-9331-00144feabdc0.html#axzz2IfAo3SLG.

Hurley, Jeff. Presentation to SEASAR 2010, the 3rd Annual Workshop on Advances in SAR Oceanography from Envisat, ERS and ESA third party missions, 25-29 January 2010. Last modified [or accessed] 15 March 2013, http://earth.eo.esa.int/workshops/seasar2010/8_Hurley.pdf

Keen, Judy. "Citing privacy, critics target drones buzzing over USA." *USA Today*, 10 January 2013. Last modified [or accessed] 12 January 2013, http://www.usatoday.com/story/news/politics/2013/01/10/domestic-drones-backlash/1566212/.

Koebler, Jason. "Report: Regulatory Mess May Hold Up Domestic Drone Revolution." *U.S. News & World Report*, 17 December 2012. Last modified [or accessed] 12 January 2013, http://www.usnews.com/news/articles/2012/12/17/report-regulatory-mess-may-hold-up-domestic-drone-revolution.

Lofgren, Congresswoman Zoe. "Reps. Zoe Lofgren and Ted Poe Introduce Bipartisan Bill to Protect Americans' Privacy Rights from Domestic Drones." Congresswoman Zoe Lofgren US House of Representatives website. Last modified [or accessed] 28 March 2013, http://lofgren.house.gov/index.php?option=com_content&view=article&id=785:reps-zoe-lofgren-and-ted-poe-introduce-bipartisan-bill-to-protect-americans-privacy-rights-from-domestic-drones&catid=22:112th-news&Itemid=161

Marx, Gary T. "Some Concepts that may be Useful in Understanding the Myriad Forms and Contexts of Surveillance." In *Understanding Intelligence in the Twenty-First*

Century: Journeys in Shadows, edited by Peter Jackson and L.V. Scott, 74-98, London: Routledge, 2004.

McCullagh, Declan. "Anti-drone revolt prompts push for new federal, state laws." *CNET*, 22 March 2013. Last modified [or accessed] 28 March 2013, http://news.cnet.com/8301-13578_3-57575863-38/anti-drone-revolt-prompts-push-for-new-federal-state-laws/

McNaughton, Graham. "Halton police find $744K worth of drugs using high-tech pot-spotting drones." *National Post*, 13 September 2012. Last modified [or accessed] 10 January 2013, http://news.nationalpost.com/2012/09/13/halton-police-find-744k-worth-of-drugs-using-high-tech-pot-spotting-drones/.

Munroe, Ian. "Meet the Canadian challenging America's drone war." *CBC* News, 5 April 2013. Last modified [or accessed] 5 April 2013, http://www.cbc.ca/news/world/story/2013/04/04/us-cia-drone-strikes-legal-challenge-jameel-jaffer.html

Munzenrieder, Kyle. "Florida Bill Would Limit Miami-Dade Police's Use of Drones." *Miami New Times*, 28 March 2013. Last modified [or accessed] 30 March 2013, http://blogs.miaminewtimes.com/riptide/2013/03/florida_bill_would_limit_miami.php

North Atlantic Treaty Organization. Joint Air Power Competence Centre. *Strategic Concept of Employment for Unmanned Aircraft Systems in NATO*. January 2010.

Pole, Ken. "Aurora's Appeal." *Canadian Skies*, 22 March 2012. Last modified [or accessed] 1 October 2012, http://skiesmag.com/news/articles/16087-aurora-s-appeal.html.

Prioria Robotics, *Maveric UAS Configuration*. Last modified [or accessed] 15 March 2013, http://www.prioria.com/products/maveric-uas/configuration

Pugliese, David. "Canada's drone squadron still stalled, with neither planes nor troops." *Ottawa Citizen*, December 27, 2012. Last modified [or accessed] 10 January 2013, http://www.ottawacitizen.com/technology/Canada+drone+squadron+still+stalled+with+neither+planes/7749650/story.html.

Pugliese, David. "ScanEagle Successful In Its Support to Canadian Forces in the Arctic Says Company." *Ottawa Citizen*, 8 October 2011. Last modified [or accessed] 15 March 2013, http://blogs.ottawacitizen.com/2011/10/08/scaneagle-successful-in-its-support-to-canadian-forces-in-the-arctic-says-company/

Spinetta, Lt. Col. Lawrence and M.L. Cummings, "Unloved Aerial Vehicles." *Armed Forces Journal*, November 2012. Last modified [or accessed] 2 April 2013, http://www.armedforcesjournal.com/2012/11/11752540

Staffa, Kathy. "Prioria Awarded Canadian Defense Contract." *Prioria Robotics.* Last modified [or accessed] 15 March 2013, http://www.prioria.com/media/documents/press/2010/Prioria_Canadian_Defence_Contract.pdf

Stanley, Jay and Catherine Crump. *Protecting Privacy From Aerial Surveillance: Recommendations for Government Use of Drone Aircraft*. New York, NY: American Civil Liberties Union, December 2011.

Statistics Canada. "Land and freshwater area, by province and territory." Last modified [or accessed] 12 February 2013. http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/phys01-eng.htm.

Thompson, Ginger and Mark Mazzetti. "U.S. Drones fight Mexican Drug Trade." *New York Times*, March 15, 2011. Last modified [or accessed] 5 February 2013, http://www.nytimes.com/2011/03/16/world/americas/16drug.html?_r=0&pagewanted=print.

Thompson II, Richard M. *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*. Washington, DC : U.S. Government Printing Office, September 6, 2012.

Transport Canada. "Spill Prevention: National Aerial Surveillance Program." Last modified [or accessed] 12 February 2013. http://www.tc.gc.ca/eng/marinesafety/oep-ers-nasp-2195.htm.

Transport Canada, "Personal Aviation, Special Flight Operations & Launch Safety: Unmanned Air Vehicle (UAV)." 3 May 2010. Last modified [or accessed] 21 February 2013, http://www.tc.gc.ca/eng/civilaviation/standards/general-recavi-brochures-uav-2270.htm

United Kingdom. Ministry of Defence, Joint Doctrine Note 2/11, *The UK Approach to Unmanned Aircraft Systems*, JDN 2-11, 30 March 2011.

United Kingdom. Air Staff, Ministry of Defence, *British Air and Space Power Doctrine.* AP 3000, 4th Edition, 2009.

United States. Congress of the United States, Congressional Budget Office. *Policy Options for Unmanned Aircraft Systems*. Washington, DC: US Government Printing Office, June 2011.

United States. Department of Defense, *Defense Airborne Reconnaissance Office (DARO) Unmanned Aerial Vehicles (UAV) Program Plan.* Washington, DC: US

Government Printing Office, April 1994. Last modified [or accessed] 21 January 2013, http://www.dod.gov/pubs/foi/International_security_affairs/other/892.pdf.

United States. Department of Defense, Under Secretary of Defense for Acquisition, Technology and Logistics, *Department of Defense Report to Congress on Future Unmanned Aircraft Systems Training, Operations, and Sustainability*. Washington, DC: US Government Printing Office, April 2012.

United States. Department of Defense, *Unmanned Systems Integrated Roadmap FY2011-2036*, 11-S-3613, Washington, DC: U.S. Government Printing Office, 2011.

United States, Department of Defense, *Quadrennial Defense Review Report*. Washington, DC: US Government Printing Office, February 2010.

United States. Department of Homeland Security, *Air Domain Surveillance and Intelligence Integration Plan: Supporting Plan to the National Strategy for Aviation Security*, Washington, DC: US Government Printing Office, March 26, 2007.

United States. House Permanent Select Committee on Intelligence, *Performance Audit of Department of Defense Intelligence, Surveillance, and Reconnaissance*, Washington, DC: US Government Printing Office, April 2012.

United States. Joint Planning and Development Office, *Integrated Air Surveillance Concept of Operations*, Washington, DC: US Government Printing Office, November 2011.

United States. Department of Commerce, United States Census Bureau, *The 2012 Statistical Abstract: The National Data Book*. Last modified [or accessed] 26 February 2013, http://www.census.gov/compendia/statab/2012/tables/12s0364.pdf

United States. Government Accountability Office. *Nonproliferation: Agencies Could Improve Information Sharing and End-Use Monitoring on Unmanned Aerial Vehicle Exports*. GAO-12-536, Washington, DC: US Government Printing Office, July 2012.

United States. Government Accountability Office. *Intelligence, Surveillance, And Reconnaissance: Actions Are Needed to Increase Integration and Efficiencies of DOD's ISR Enterprise*. GAO 11-465, Washington, DC: US Government Printing Office, June 2011.

United States. Office of Global Maritime Situational Awareness, *National Concept of Operations for Maritime Domain Awareness*. Washington, DC: US Government Printing Office, December 2007.

United States, U.S Air Force, *Command and Control*, Air Force Doctrine Document (AFDD) 2-8. Washington, DC: Department of the Air Force, 1 June 2007.

United States, U.S. Air Force, *United States Air Force Unmanned Aircraft Systems Flight Plan 2009-2047*, Headquarters, United States Air Force. Washington, DC: Department of the Air Force, 18 May 2009.

United States. United States Statutes at Large Volume 111 Part 2 Public Law 105-85, *Sec. 905 Airborne Reconnaissance Management*, 18 November 1997. Last modified [or accessed] 2 April 2013, http://en.wikisource.org/wiki/Page:United_States_Statutes_at_Large_Volume_111_Part_2.djvu/775

Volker, Kurt. "What the U.S. risks by relying on drones" *Washington Post*, 26 October 2012. Last modified [or accessed] 5 April 2013, http://articles.washingtonpost.com/2012-10-26/opinions/35500650_1_drone-strikes-drone-attacks-guantanamo-bay

Walker, Major Scott A. "Integrating Department of Defense Unmanned Aerial Systems into the National Airspace Structure," Master's thesis, U.S. Army Command and General Staff College, 2010.

Walker, Major R.J. "What Happened to Air Force ISR?" MDS Research Project Paper, Canadian Forces College, 2009.

Walkinshaw, Lieutenant (Navy) Chris "HMCS Regina reports for duty." 17 September 2012. Last modified [or accessed] 15 March 2013, http://www.cjoc-coic.forces.gc.ca/fs-ev/2012/09/17-eng.asp

Welsh, William. "March sequester would degrade US defense forces, says Panetta," *Defense Systems*, 11 January 2013. Last modified [or accessed] 28 March 2013, http://defensesystems.com/Articles/2013/01/11/panetta-sequestration-threat-briefing.aspx?Page=1