ROYAL CANADIAN AIR FORCE
JOURNAL

AIR POWER THEORY AND FORCE CLASSIFICATIONS

2 CANADIAN AIR DIVISION

CAN UNMANNED AIRCRAFT SYSTEMS MEET CANADIAN AIR POWER NEEDS?

AND MORE!

CANADIAN ARMED FORCES

FORCES ARMÉES CANADIENNES

National Defence
Défense nationale

Canada

EDITORIAL TEAM

NOTE TO READERS

As a bilingual publication, readers should take note that where quotations are translated from their original language, we will use the term [Translation] at the end of the quote to indicate that readers can find the original text in the other language version of the *Journal*. Unless otherwise noted, photographs appearing in the *RCAFJ* are attributable to the public domain.

ROYAL CANADIAN AIR FORCE

JOURNAL

AIRPOWER
IN FORMATION

AGILE • INTEGRATED • REACH • POWER

SUBMISSION REQUIREMENTS

The *ROYAL CANADIAN AIR FORCE JOURNAL (RCAFJ)* welcomes the submission of articles, book reviews and shorter pieces (which will be published in the Letters to the Editor, Points of Interest, Pushing the Envelope and Point/Counterpoint sections) that cover the scope of air-force doctrine, training, leadership, lessons learned and air-force operations: past, present or future. Submissions on related subjects such as ethics, technology and air-force history are also invited.

JOURNAL SECTIONS

ITEM	WORD LIMIT*	DETAILS
LETTERS TO THE EDITOR	50–250	Commentary on any portion of a previous *RCAFJ*.
ARTICLES	3000–5000	Written in academic style.
BOOK REVIEWS	500–1000	Written in academic style and must include: • the book's complete title (including subtitle); • the complete names of all authors as presented on the title page; • the book's publisher, including where and when it was published; • the book's ISBN and number of pages; and • a high resolution .jpg file (at least 300 dpi and 5 by 7 inches) of the book's cover.
POINTS OF INTEREST	250–1000	Information on any topic (including operations, exercises and anniversaries) that is of interest to the broader aerospace audience.
PUSHING THE ENVELOPE	250–2000	Forum for commentary, opinions and rebuttal on *RCAFJ* articles and/or issues that are of interest to the broader aerospace audience.
POINT/COUNTERPOINT	1500–2000	Forum to permit a specific issue of interest to the RCAF to be examined from two contrasting points of view.

* Exclusive of endnotes

AUTHORS ARE ASKED TO NOTE THE FOLLOWING GUIDELINES:

- Submissions may be made in either official language.
- Authors must include a brief (one paragraph) biographical sketch which includes current appointment/position, telephone number and email address. Please include all professional and academic designations as well as military decorations.
- Selected articles that have been peer reviewed have a ✹ to the left of the title.
- The Senior Editor will notify contributors on the status of their submission. It may not be possible to publish all submissions.
- All text submissions must be digital, in Microsoft Word or rich text format. Files must not be password protected and must not contain macros. Files may be submitted by mail or email at the addresses provided below.
- All supporting tables, images and figures that accompany the text should be sent in separate files in the original file format (i.e., not imbedded in the text). Original vector files are preferred; high resolution (not less than 300 dpi) .psd or .jpg files may be submitted.
- Authors are now required to provide "alternate text" with detailed description for all figures. The alternate text is to be labelled as such and placed below the caption.
- Copyright permissions are required for all material that is not Department of National Defence or author originated. It is the author's responsibility to obtain and submit the necessary written permissions which must include the author's/artist's name as well as the publisher's name and location. Any material not meeting these requirements may be omitted from the article.
- The Senior Editor may select images or have graphics created to accompany submissions.
- Authors should use *Oxford English* or *Petit Robert* spelling. When required, reference notes should be endnotes rather than footnotes and formatted in Chicago style. For assistance refer to *The Chicago Manual of Style, 16th Edition*, *Le guide du rédacteur* or CFAWC Production Section at CFAWCProd@forces.gc.ca
- Acronyms and abbreviations should be used sparingly:
  - If they are required in the text, the term is to be written out in full the first time it is used and then followed by the abbreviated form in parentheses.
  - A list of all abbreviations (and their terms) used in the text will be included at the end of each submission.
- The Senior Editor reserves the right to edit submissions for style, grammar and length but will not make editorial changes that will affect the integrity of the argument without consulting the author.

FOR FURTHER INFORMATION OR TO MAKE A SUBMISSION PLEASE CONTACT THE SENIOR EDITOR AT:

Canadian Forces Aerospace Warfare Centre
8 Wing / CFB Trenton
Box 1000 Stn Forces
Astra, Ontario K0K 3W0

Attn: LCol Doug Moulton   Doug.Moulton@forces.gc.ca

CALL FOR SUBMISSIONS

For the Fall 2016 issue: **30 July 2016**

For the Winter 2017 issue: **30 October 2016**

For the Spring 2017 issue: **30 January 2017**

For the Summer 2017 issue: **30 April 2017**

DISCLAIMER

CONTENTS

SUMMER 2016

VOLUME 5 • NUMBER 3

Photo: DND

EDITOR'S MESSAGE

As we move forward into the annual posting season, there is the inevitable change that comes to Royal Canadian Air Force (RCAF) units around the country. In this, the *Royal Canadian Air Force Journal (RCAFJ)* is no different, as we now take the opportunity to say thank you to our Senior Editor, Major Bill March. It is hard to imagine an *RCAFJ* without Bill's hand at the rudder, as it has been since the Fall 2008 edition was published. Bill's dedication to developing the *RCAFJ* has always been impressive. His superb leadership has established the *RCAFJ* as a world-class publication, providing airpower enthusiasts a venue to further the development of airpower mastery within the RCAF.

This issue also provides an opportunity for all to peruse the award-winning "Cyber Warfare Schools of Thought: Bridging the Epistemological/Ontological Divide." One of the Commander RCAF Awards, the Carr Award (Lieutenant-General Bill Carr) is presented to a Joint Command and Staff Programme student at Canadian Forces Staff College for a pre-eminent paper on an innovative airpower topic. This year's award recipient, Lieutenant-Colonel P. E. C. Martin, provides some brilliant insights into a variety of approaches open to the RCAF in dealing with the issues associated with cyber and, in particular, how the RCAF might best approach these issues.

Enjoy the read.

Sic Itur Ad Astra

Lieutenant-Colonel Doug Moulton, CD, MBA
Senior Editor

2 CANADIAN AIR DIVISION

BY COLONEL RICK WITHERDEN, OMM, MB, CD
WITH AN INTRODUCTION BY BRIGADIER-GENERAL DAVE COCHRANE, MSM, CD

INTRODUCTION

As Commander 2 Canadian Air Division (Comd 2 Cdn Air Div), I am pleased to provide an introduction to the following article, written by Colonel (Col) Rick Witherden, on the division's role and history. Col Witherden is uniquely qualified to write this article, as he was there when 2 Cdn Air Div was created and has served continuously within the division ever since (the majority of that time as our Chief of Staff, with a short stint as Director of Air Force Training). I am pleased and honoured to have been assigned my current responsibilities and am proud of the dedicated team of professionals working within my headquarters, wings and training establishments.

As much as 2 Cdn Air Div has reached a level of maturity through six years of evolution, the dynamic nature of Royal Canadian Air Force (RCAF) operations continues to keep us fully engaged in innovating and modernizing the education and training that we deliver in order to enable those operations. My priority is to contribute to the institutional excellence of the RCAF by accomplishing four main goals:

- Deliver core training and education, in accordance with our mandate.

- Develop and modernize training delivery across the full continuum of education and training.

- Institutionalize professional development of our officers and non-commissioned members (NCMs) within the RCAF.

- Support our personnel and their families.

These goals can only be achieved through the dedicated efforts of our personnel, working in concert with other organizations within the RCAF and beyond, and I firmly believe people work more effectively together when everyone's role is clearly understood.

Whether you are reading for personal or professional interest, this article provides a solid foundation for anyone hoping to garner a better understanding of the crucial role 2 Cdn Air Div plays in the development of air power for the Canadian Armed Forces (CAF).

MISSION:

2 CDN AIR DIV GENERATES AND DEVELOPS PERSONNEL AS TRAINING AUTHORITY FOR THE RCAF.

VISION:

2 CDN AIR DIV WILL DELIVER ADVANCED AEROSPACE KNOWLEDGE AND LEADING-EDGE TRAINING THROUGH A RESPONSIVE, INNOVATIVE AND EFFECT-BASED METHODOLOGY TO ACHIEVE MAXIMUM TRAINING EFFECTIVENESS FOR THE RCAF.

2 Cdn Air Div commenced stand-up work in January 2009 and declared full operational capability (FOC) in July 2010. Considerable structural evolution has taken place over the past six years, but the division maintains the core mandate of training and education for the RCAF. While it may be obvious to some, what does this mandate really mean? How did 2 Cdn Air Div get to its current structure in support of that mandate, and what changes may be in its future? This article introduces 2 Cdn Air Div, its structure, roles and history to date and answers the question of why this formation is of critical importance to the RCAF's future.

2 Cdn Air Div provides the basic occupation training for all RCAF occupations and trades and is responsible for delivering the professional development needed for officers and NCMs. It is important to note, however, that these responsibilities extend beyond 2 Cdn Air Div, with training managers across the RCAF being responsive to Comd 2 Cdn Air Div. In fact, all of the RCAF's 638 qualification standards (QSs),[1] regardless of the division or unit under which they are delivered, are approved by 2 Cdn Air Div. Furthermore, 2 Cdn Air Div dictates and monitors the systems approach to training, which is known as the Air Force Training and Education Management System (AFTEMS)[2] and is used at all training establishments, including operational training units (OTUs) and fleet schools. As such, 2 Cdn Air Div acts as the RCAF training and education nexus and is the foundation upon which RCAF personnel are developed.

2 Cdn Air Div is a Level 2 formation that reports directly to Comd RCAF (see Figure 1). Given its mandate, it should be no surprise that the formation is comprised of all RCAF ab initio[3] training establishments and the two education institutions: the Royal Canadian Air Force Academy and Canadian Forces School of Aerospace Studies (CFSAS)—the "schoolhouses" of the RCAF for NCMs and officers respectively.
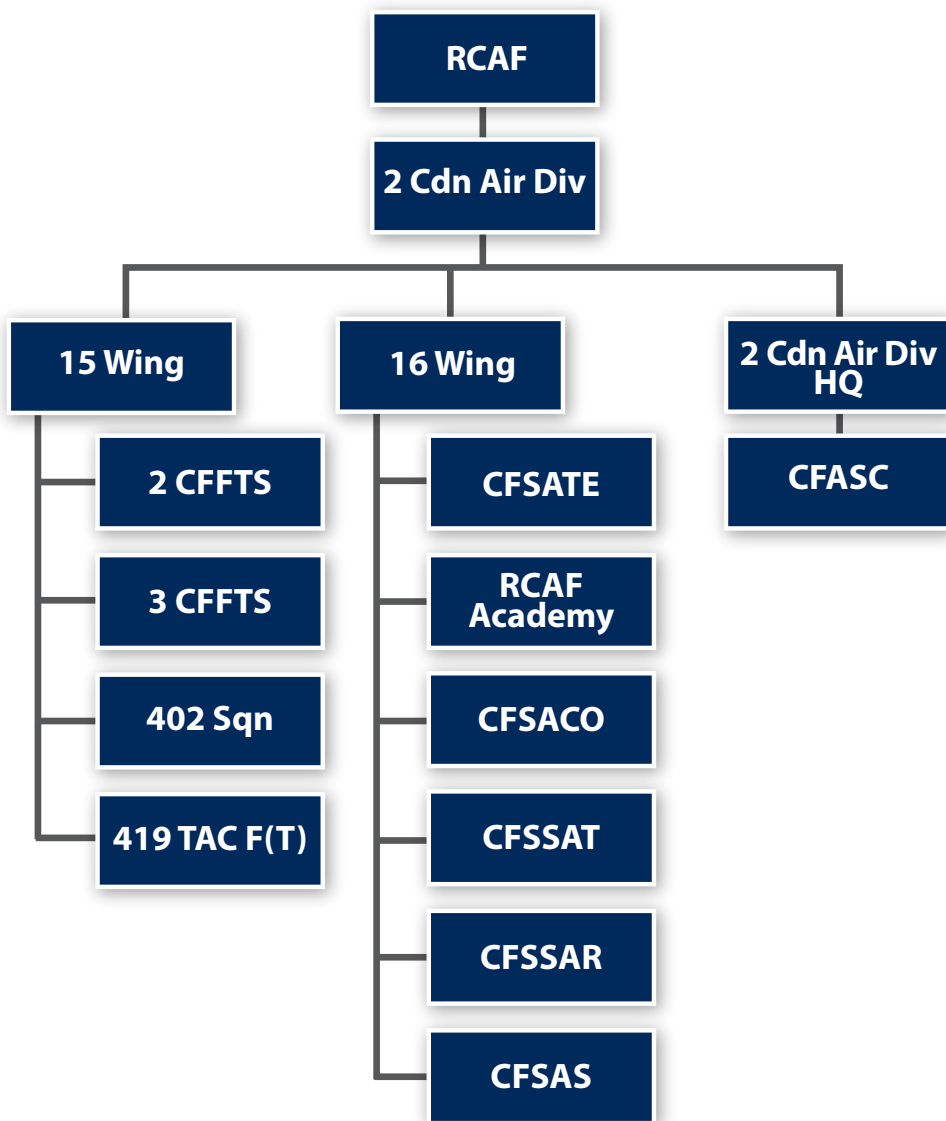
Figure 1. 2 Cdn Air Div organization

Given its broad training management responsibilities, 2 Cdn Air Div Headquarters (HQ) is relatively small at 90 personnel, which includes elements of the former Central Flying School (CFS). The former Air Force Training Directorate of 1 Cdn Air Div HQ became the core of 2 Cdn Air Div HQ, bringing their mandate and related resources intact. This mandate included the training management, movement and funding of all personnel in the RCAF training system, including most out-service and outside-Canada training contract arrangements. To support the Comd 2 Cdn Air Div and provide the overhead management of the division and HQ (financial, administrative, etc.), 12 additional positions were sourced from mainly vacant establishment positions at

1 Cdn Air Div HQ. However, this "lean" construct must be taken in context. Apart from the standard constraint of "person year (PY) neutrality"[4] in its creation, 2 Cdn Air Div knew that it could not follow the tendency toward HQ growth that afflicted other command organizations of the day. Operational units and training establishments were already operating below optimum personnel numbers, and a part of 2 Cdn Air Div's success depended on not becoming another "tooth to tail" problem. Additionally, the combined air operations centre capability was standing up within 1 Cdn Air Div HQ at the same time, and personnel resources were at a premium. As a result, 2 Cdn Air Div entered into a matrix support agreement, whereby services provided by 1 Cdn Air Div HQ give 2 Cdn Air Div HQ a virtual size that is not reflected on organizational charts. In return, 2 Cdn Air Div HQ provides routine and surge support to 1 Cdn Air Div HQ when and where it can. For this reason, the two HQs remain ideally located close to each other in Winnipeg, Manitoba, and achieve equally close synergies via an extensive service-level agreement.

Why create a distinct training and education formation in the first place? Since the end of World War II, Canada's Air Force has had Training Command, 14 Training Group, the Air Force Training Directorate of 1 Cdn Air Div HQ and now 2 Cdn Air Div—once again a separate formation. Clearly, there has been a recurring imperative to centralize expertise and management of training and education matters. Many current members of the RCAF would be surprised to learn that the concept of 2 Cdn Air Div predated its formation by many years. In fact, with the end of Air Command Headquarters in 1997, there might have been two divisions created from the outset. Command and control (C2) recommendations made as part of Project 2020 in 1995 could have seen a separate training formation continue, but the overall aerospace-combat-group concept did not receive sufficient support at the time. In 2004, revised C2 arrangements were considered again, this time with recommendations for an Air Force training and transformation division to be formed by separating the training functions out of 1 Cdn Air Div. Various permutations of the concept were studied over the following years, but no decision was made until Lieutenant-General Watt, then Chief of the Air Staff, directed the creation of 2 Cdn Air Div in late 2008.

A student in a Bell CH139 Jet Ranger helicopter makes final preparations before a flight during the rotary-wing phase III course at 3 CFFTS in Portage la Prairie, Manitoba.

A member of 2 CFFTS prepares for a flight in the Harvard II at 15 Wing Moose Jaw.

The current structure of 2 Cdn Air Div, while somewhat similar, is not the way it looked at FOC in 2010. 15 and 16 Wings, already considered training wings and with the preponderance of RCAF basic occupation schools, were aligned with 2 Cdn Air Div from the outset. This included 2 and 3 Canadian Forces Flying Training Schools (CFFTS) and 419 Tactical Fighter Training Squadron (419 TAC F[T] Sqn), located at Moose Jaw, Portage La Prairie and Cold Lake, respectively, in support of 15 Wing's pilot training role. 16 Wing was predominantly composed of the Canadian Forces School of Aerospace Technology and Engineering (CFSATE) and Canadian Forces School of Aerospace Control Operations (CFSACO), located in Borden and Cornwall, respectively. However, several training establishments, such as 1 CFFTS (formerly the Canadian Forces Air Navigator School), 402 Squadron, Canadian Forces School of Survival and Aeromedical Training (CFSSAT), Canadian Forces School of Search and Rescue (CFSSAR) and CFSAS, were not located on predominately training-oriented wings. With the majority of them located at 17 Wing Winnipeg, it appeared that those units might lead to a 17 Wing alignment with 2 Cdn Air Div (interestingly, such an alignment was first assumed as part of the 2004 C2 proposals). A final decision on alignment was deferred to a later date, and in the interim, a distinct Level 3 formation called the Air Force Training Centre (AFTC) was established, pooling these schools and the Canadian Forces Aircrew Selection Centre (CFASC, located in Trenton) under a double-hatted 17 Wing Commander. Finally, the Canadian Forces Aerospace Warfare Centre (CFAWC) was assigned to Comd 2 Cdn Air Div, providing doctrinal and knowledge linkages to the education mandate of the new division.

The story of 2 Cdn Air Div has been one of constant evolution. Legacy structures, not necessarily tuned to a strictly training and education focus, as well as interim arrangements put in place for practical reasons of the day have been replaced by increasingly functional and streamlined organizations. 1 CFFTS amalgamated with 402 Squadron—given their shared mandate for air combat systems operator (ACSO) and airborne electronic sensor operator (AESOP) training—and realigned under 15 Wing as part of a larger aircrew-training-wing concept. Similarly, the availability of a colonel position for 16 Wing (downgraded to lieutenant-colonel in the mid-90s) allowed that formation to absorb the remaining AFTC units, thus seeing the dissolution of that interim construct. CFASC became a direct report to Comd 2 Cdn Air Div and added integrated personnel selection officer support, in recognition of the need for greater alignment between aircrew selection and the training standards being applied. CFS, being disbanded over the period of 2 Cdn Air Div's creation,

saw its Aircrew Standards and Evaluation Team (SET) assets assigned to 2 Cdn Air Div HQ under the Air Operations Training Section. CFAWC returned to reporting directly to Comd RCAF, as a more detailed study of its mandate revealed greater utility for that alignment at the present time.

Returning to the question of why 2 Cdn Air Div exists or is even necessary, it is important to look at the wider RCAF and CAF contexts in which it operates. The concept of "operations primacy" is a given—it is the raison d'être of military forces. Yet, for a relatively small air force and in an era of constraint and shrinking operating budgets, it is possible to "mortgage the future to pay for today" if training resources and dedicated expertise are reduced below sustainable levels. The former Air Force Training Directorate of 1 Cdn Air Div HQ had shrunk to a size less than half of its 14 Training Group predecessor, despite an expanded mandate. Efficiencies had been introduced over the years, but some core training management and oversight functions had been reduced or ceased altogether. CFS, once the guardian of all aircrew training standards, had significantly reduced its oversight of OTUs in the years preceding its disbandment. The creation of 2 Cdn Air Div again recognized the historical need to centralize the expertise and management of training and education matters. Operating separate from the current operations milieu (but with its own high tempo), 2 Cdn Air Div can remain focused on generating and developing tomorrow's air personnel and combat leaders. Of course, 2 Cdn Air Div must still be mindful of ongoing operations, as it is those operations that shape the desired product for delivery to readiness and deployment authorities. As such, the close working relationship maintained with 1 Cdn Air Div, CFAWC and the Comd RCAF staff at National Defence Headquarters remains key.

2 Cdn Air Div is still evolving. Overall training modernization continues across all training establishments, with increased focus on simulation and virtual-learning schemes. The current NATO Flying Training in Canada pilot-training contract expires approximately 2021, and work on the next generation aircrew training requirements is well underway. Air Technician Training Renewal (ATTR) is still proceeding with numerous enhancements to training delivery and related aids. In terms of education and professional development, the RCAF Academy has significantly upgraded its course offerings in recent years. For officers, the Air Force Officer Development (AFOD) programme is now in full delivery, and research is underway to further improve the education for all officers, from junior to senior. With all RCAF qualifications returning to a state of 100 per cent currency, 2 Cdn Air Div HQ is now turning its attention to training validation, further ensuring that the operational communities are indeed receiving the high calibre personnel that they require. At the same time, the 2 Cdn Air Div HQ Training SET has begun to engage with OTUs to assist with training quality and performance—the role lost with the disbandment of CFS.

The RCAF is an organization constantly preparing for the next challenges. The training and education of our people is fundamental to that preparation. Working diligently and often in the background, 2 Cdn Air Div guarantees that core mandate is met.

Brigadier-General (BGen) D. B. Cochrane enrolled in the Canadian Forces in 1982. He received a baccalaureate degree in Mechanical Engineering from the Royal Military College in Kingston, Ontario, in 1986. Following receipt of his air navigator (air combat system operator) wings, BGen Cochrane spent his flying career with 426 Squadron and 436 Squadron, commanded 426 Squadron from 2006 to 2009 and subsequently deployed, for six months, as Commanding Officer Theatre Support Element at Camp Mirage in Dubai, United Arab Emirates. BGen Cochrane assumed command of 8 Wing / CFB Trenton in 2010. He is a graduate of the Canadian Forces Command and Staff College Course in Toronto and the Australian Defence College's Defence and Strategic Studies Course. Promoted to BGen in 2015, he assumed the position of Commander 2 Cdn Air Div in Winnipeg and oversees individual training and education for RCAF officers and NCMs.

Col Rick Witherden joined the Canadian Forces in January 1979. During his Regular Force career, he served tours on all three maritime helicopter squadrons and also enjoyed an instructional tour with 3 Canadian Forces Flying Training School in Portage La Prairie, Manitoba. Selected for Staff College, Col Witherden attended the Canadian Forces College in Toronto. He finished his Regular Force career as the Division Instrument Check Pilot at 1 Cdn Air Div. In July 2001, Col Witherden transferred from the Regular Force to the Reserves. He was subsequently appointed Commanding Officer of 402 "City of Winnipeg" Squadron in July 2006. In February 2009, he was promoted to his current rank and appointed Chief of Staff, 2 Cdn Air Div.

ABBREVIATIONS

419 TAC F(T) Sqn	419 Tactical Fighter Training Squadron
AFTC	Air Force Training Centre
AFTEMS	Air Force Training and Education Management System
AVS	avionic systems
BGen	brigadier-general
C2	command and control
CAF	Canadian Armed Forces
Cdn Air Div	Canadian Air Division
CFASC	Canadian Forces Aircrew Selection Centre
CFAWC	Canadian Forces Aerospace Warfare Centre
CFFTS	Canadian Forces Flying Training Schools
CFS	Central Flying School
CFSACO	Canadian Forces School of Aerospace Control Operations
CFSAS	Canadian Forces School of Aerospace Studies
CFSATE	Canadian Forces School of Aerospace Technology and Engineering
CFSSAR	Canadian Forces School of Search and Rescue
CFSSAT	Canadian Forces School of Survival and Aeromedical Training
Col	colonel
comd	commander
FOC	full operational capability
HQ	headquarters
NCM	non-commissioned member
OTU	operational training unit
PY	person-year
QS	qualification standard
RCAF	Royal Canadian Air Force
SET	standards and evaluation team

NOTES

1. QSs are established for each distinct qualification and describe in detail the performance level to be achieved on any given course. The RCAF maintains a uniquely high number of QSs due to its complex qualification structure in support of numerous aircraft fleets.

2. AFTEMS is based on the Canadian Forces Individual Training and Education System (CFITES).

3. Ab initio or "from the beginning" generally refers to the first stage of training and is traditionally applied to RCAF flight training.

4. PY neutrality refers to zero growth of the RCAF establishment, thus the creation of the new HQ depended on realigning existing resources.

BGen Cochrane, Comd 2 Cdn Air Div

INTRODUCTION

The use of unmanned air assets by militaries has been a concept which has existed almost as long as the idea that aircraft had military applications. From Hap Arnold's Kettering Bug, through the development of early steerable bombs such as the Fritz, glide bombs and target drones such as the Dennymite, there has always been an understanding of the value they held, and that more was possible.[1] The sophisticated reconnaissance and offensive semi-autonomous systems found in the form of today's Avengers, Eitans, Reapers and other similar UAS are finally beginning to scratch the surface of the potentially revolutionary capabilities they present; these new developments create substantial concern about what comes next and what it means for air power.[2] This paper investigates current developments in the technology and its employment by militaries around the world and evaluates its impact on air power, force structures, operations and culture, presenting how or if Canada should move forward with adopting a more comprehensive use of unmanned systems as a means of providing Canadian air power in the near future. It is the position of this paper that Canada should foster capability, operational knowledge and technical familiarity in order to stay competitive and be capable in the future; however, doing so should not radically alter the Royal Canadian Air Force's (RCAF's) force structure in the immediate future. The approach of the Royal Australian Air Force (RAAF) to UASs represents one which is most compatible with Canadian air power needs, and should the RCAF commit to adopting UASs beyond the tactical scale, emulation of this approach and the UASs considered would most appropriately conform with Canadian air power needs and financial/political realities. Outside of this approach, contemporary manned systems already slated for acquisition or currently in use will continue for some time to adequately fulfil Canada's air power needs without additional dramatic cost or disruptive effect upon RCAF culture, doctrine or capabilities.

CAN UNMANNED AIRCRAFT SYSTEMS MEET CANADIAN AIR POWER NEEDS?

BY CONRAD EDWARD ORR

CANADA'S PREVIOUS EXPERIENCE AND CURRENT SITUATION

A good place to start when evaluating Canada's future with UASs is its relevant past. Canada's national history with UASs is almost as long as the use of UASs by militaries, having had its start in the 1960s with projects such as the CL-89 surveillance drone (1963), CL-327 helicopter-like surveillance drone (1977) and ROBOT-X target drone (1985), with industry-leading Canadian companies such as Canadair developing these indigenously.[3] These early developments make Canada one of the nations with the longest and most intimate familiarity with the military use of UASs. This fact makes Canada's current lack of widespread use of UASs,[4] while other early adapters such as Israel continue to excel,[5] all the more compelling to investigate. At present, CAF makes use of UASs on a small scale across the various environments, employing only "tactical" sized systems[6] such as the ScanEagle[7] and Raven-B;[8] the former being deployed on all Navy frigates in the Gulf of Aden since 2012, and both being used by the Army.[9] These tactical systems are all directed at intelligence, surveillance and reconnaissance (ISR) work, lack any kind of strike capabilities and are intended for short-range, short-duration tasks. The RCAF has previously used UASs, having employed the French-made, truck-launched Sperwer[10] as well as several leased Israeli medium-altitude long-endurance (MALE) Herons[11] in support of Army and Navy operations abroad.[12] Both of these UASs were unarmed, intended for ISR and have since been retired from Canadian use.

Both the Canadian Government and CAF have explicitly expressed a contemporary interest in and intention to acquire more sophisticated UASs, through the *Canada First* Defence Strategy (*CFDS*) and the Joint Unmanned Surveillance and Target Acquisition System (JUSTAS) programme respectively.[13] The *CFDS*, published in 2008, was a strategy for force-structure reorganization and defence posturing to meet the Conservative government's "vision for defence."[14] The JUSTAS programme was established in 2000 by the Department of National Defence in order to "establish a joint direction for concept development and experimental activities,"[15] is led by the Air Force Experimental Centre and was originally intended to produce an operational unmanned air vehicle (UAV) capability for Canada by 2009.[16] Currently, the program has a delivery date of 2025 and a budget estimate of between $500 million and $1.5 billion.[17] Both initiatives present Arctic and maritime sovereignty as a key focus for CAF and, though in unspecific terms, both indicate UASs will have a role in that mission. In *CFDS*, six core objectives are identified, the first of which is "daily domestic and continental operations, including in the Arctic,"[18] an objective that would be supported through JUSTAS that has the stated goal "to acquire an unmanned aircraft system (UAS) weapon system to support Canadian Armed Forces … [that] will complement existing ISTAR [intelligence, surveillance, target acquisition and reconnaissance] capabilities, [and] increase maritime and Arctic domain awareness."[19]
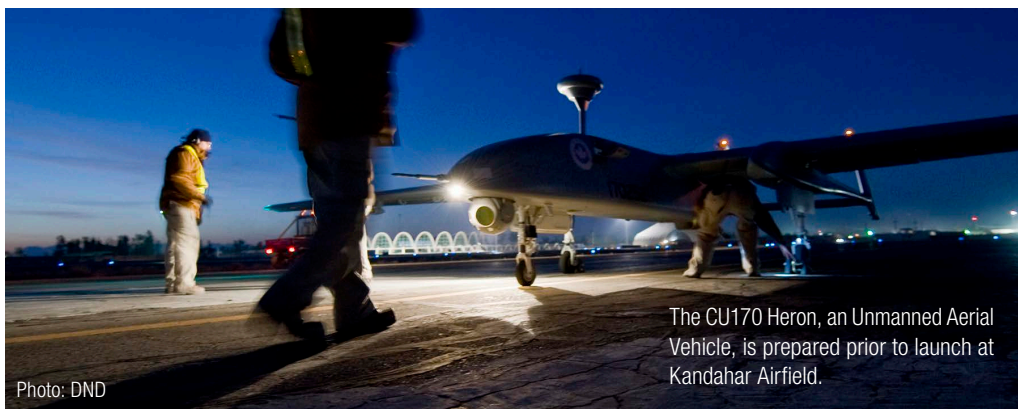

The CU170 Heron, an Unmanned Aerial Vehicle, is prepared prior to launch at Kandahar Airfield.

Photo: DND

However, since its commission, the JUSTAS programme has been stalled or significantly slowed due to lack of funding and shifting priorities, and though Arctic surveillance with space assets in the form of Project Polar Epsilon has moved forward, Canada remains without UAS beyond the tactical scale.[20] In 2008, a parliamentary study, now known as the Manley Report, was conducted into CAF's immediate needs regarding UASs.[21] The Manley Report stated that Canada needed to quickly adopt UAS capabilities, lest it miss its opportunity and suffer operationally as a result. This report and its sense of urgent need to adopt UASs led to the leasing of the Israeli Herons in 2009, the programme having been twice renewed, but following the end of combat operations in Afghanistan in 2011, the Herons were turned over to the RAAF and Canadian MALE UAS capability was lost.[22]

The question that emerges quite clearly is "why was UAS capability beyond small systems allowed to languish?" particularly in the face of apparent enthusiasm and articulated need to be a part of what is increasingly seen as a transformational change in air power. Dutch researcher Gary Shuab offers that it is because UASs represent for the RCAF a disruptive and expensive change at a time when budgets are otherwise occupied; while for the Army and Navy, smaller UASs presented a cost-efficient technology that could be adaptively integrated into current methods of operation and which extended/enhanced their methods of operation non-disruptively.[23]

Stephen Rosen, a theorist on military change, adds weight to this idea with his theory that the independent services of a nation's armed forces have unique cultures and interests, defined internally as well as through interservice struggle, and that this shapes their perceived/preferred "way of war."[24] According to military change theorists Theo Farrell and Terry Terriff, each service must approach military change at its own pace and in accordance with its own understandings/limitations, doing so through either indigenous innovation, adaptation of existing means/practices or emulation of other armed forces by importing foreign tools and methods of fighting.[25] The Army began its familiarity with UASs in the form of the Sperwer while in Afghanistan from October 2003 to April 2009[26] and saw immediately the benefits it offered in situations of regular use of indirect fire, mountainous terrain and difficulties obtaining up-to-date intelligence. The Army's choice of UAS surprised and frustrated the RCAF, as the Sperwer was a larger, fixed-wing design, and the RCAF was of the opinion it, therefore, was an aircraft and theirs to control.[27] The resultant tensions and issues in command and control (C2) of the Sperwer led to the Chief of the Defence Staff ordering that the environments "sort it out" and culminated in the 2006 publication of the *Canadian Forces UAV Campaign Plan*.[28] This document placed all but mini-UAVs,[29] such as the ScanEagle or Raven-B, under the control and responsibility of the RCAF. The *Canadian Forces UAV Campaign Plan* also established the Director of Joint Capability Development, essentially an RCAF organization, and tasked it with coordinating all UAS development and acquisition efforts across the Canadian military.

Published two years later, the Manley Report created the expressed immediacy in need for the RCAF to move forward with the leasing of the Israeli Herons for use in Afghanistan, following the 2009 retirement of the Sperwer. At the same time, the Navy moved ahead with its investigations into the use of embarked mini-UASs, resulting in the 2011 adoption by the Navy of the ScanEagle, used previously by the Army. The Navy's newfound sentiment expressed by Navy Commander Canadian Fleet Atlantic Commodore Scott Bishop was that "without embarked UAVs, the ability of surface ships to conduct ISR was severely limited."[30] The then Chief of the Maritime Staff, Vice Admiral Paul Maddison, further pointed out that the ScanEagle did not replace the capabilities offered by the Sea King helicopters but "enhance[ed] the warship's existing capability"[31] and was easily incorporated into operations without substantially altering operational procedures.

It would seem that for Canada, UASs have thus far come to find homes within the Army and Navy as force multiplying tactical systems which have been integrated into how these environments conduct their operations and, as a result, extended their capabilities. With regard to Canadian air power within the RCAF however, UASs have not made a significant impact, as the RCAF has not indigenously developed them nor attempted to adaptively integrate UASs into existing RCAF means of operating.

The third option for approaching change, emulation, is the approach attempted by the RCAF thus far, exemplified by the leasing of the Israeli systems and the more common endorsement in Canadian military writing of purchasing or modifying systems off the shelf, such as the Global Hawk or Predator used by the United States Air Force (USAF).[32] An exemplar of this approach elsewhere is the United Kingdom's (UK's) Royal Air Force (RAF) and its method for adopting UASs.[33] With this in mind, it is valuable to next evaluate the roles through which the RCAF provides Canada with air power and question—in light of how other nations' air services have changed and what current fleet upgrades Canada is undertaking—whether these roles could be fulfilled in the future more suitably through UASs.

CAN UASs SOLVE CANADIAN PROBLEMS? LOOKING INWARDS AND OUTWARDS

Looking at the roles that air power serves for Canada domestically as well as abroad, it becomes less surprising that the RCAF has been less than enthusiastic about dramatically incorporating UASs into Canadian air power. The three principle objectives of the RCAF outlined by the Canadian government are the defence of Canada, the defence of North America as well as a contribution to international peace and security abroad.[34] The actual roles provided for by air power in achieving these objectives are air-combat capability, ground-strike capability, search and rescue (SAR), maritime/Arctic surveillance, airlift capability, general ISR, disaster response and support of the other environments through integrated operations.[35] When seeking to understand how these roles are currently undertaken, what immediate needs exist and whether these could be addressed through UASs, a look to recent operations and fleet improvements, as former Canadian Chief of the Air Staff Lieutenant-General André Deschamps provided in 2010,[36] is illuminating. Canada contributed significantly to the disaster in Haiti through Operation (Op) HESTIA by providing a massive airlift effort using CC177 Globemasters and CC130 Hercules transporting people, equipment and aid.[37] In Op PODIUM, the RCAF conducted extensive airlift and provided "multinational, and interdepartmental air security"[38] for the Vancouver Olympic Games; this was done using CH146 Griffon, CH124 Sea King, CP140 Aurora and CC138 Twin Otter aircraft as part of the Joint Task Force Games' Air Component. Further, CF188 Hornets, CH146 Griffons, CC130 Hercules, CC150 Polaris tankers and deployable radar units were used to provide aerospace warning and control.[39] Looking at kinetic operations, Canada most recently participated in Op IMPACT against the so-called Islamic State.[40] In Op IMPACT, the RCAF has made use of CC150T Polaris aerial refuellers, CP140 Aurora long-range patrol aircraft for ISR and CF188 Hornets for air-strike operations.[41] An examination of how these capabilities are being maintained/improved for the future reveals that acquiring new CC177 Globemaster IIIs, CH147F Chinooks and CC130J Hercules will update airlift capability;[42] new CH148 Cyclone shipborne helicopters will replace the aging CH124 Sea Kings;[43] and the CF188 combat aircraft fleet is set to be replaced following an open competition,[44] as the new Liberal Government opposes the originally slated F-35 acquisition.[45] As well, though no airframes have been selected, there is an ongoing effort to replace the aging CC115 Buffalo and CC130 legacy Hercules aircraft used for fixed-wing SAR.[46] When identifying what kind of air power can be provided by MALE or HALE (high-altitude long-endurance) UASs, the roles achievable are maritime/Arctic ISR, overseas ISR, communications relay and, potentially,

air-ground or air-air strike capability. In filling these roles with UASs, the United States (US), the UK, France and Australia each stand out as distinct exemplars of different approaches worth evaluating comparatively, as was done by Colonel Ryoji Shirai of the Japanese Air Self Defense Force in 2014[47] and will be summarized/explored below.

> **WHILE AMERICAN DEFENCE AND SECURITY PRIORITIES REQUIRE HIGH AND CONTINUOUSLY GLOBAL OPERATIONAL TEMPO, CANADIAN PRIORITIES ARE LESS DEMANDING, AND THUS, THE INCREDIBLE COSTS OF INFRASTRUCTURE PROCUREMENT AND MAINTENANCE BECOME SUBSTANTIALLY MORE PRONOUNCED IN LIGHT OF ACTUAL OPERATIONAL NEEDS.**

The US has been operating UASs across all three services since the late 1970s and, similar to Canada and nearly all allied nations with UASs, has relegated smaller tactical-scale systems to control by the Army and Navy while what it refers to as class 4 and class 5 UAS (MALE and HALE UASs, respectively) are viewed "as airplanes" and are controlled by USAF. Dissimilar to Canada, the Army and Navy operate a vast and varying fleet of tactical systems for different needs, with the USAF fleet of MALE and HALE UASs being both robust and capable of ground strike. USAF organizes its UAS usage in the traditional form of squadrons, establishing its first in 1995. As of the 2008 reactivation of the 556th Test and Evaluation Squadron,[48] USAF has eight such squadrons and recognizes/trains its UAS operators as pilots. After experiencing significant friction between the new UAS pilots and the traditional manned-aircraft-pilot centric culture within USAF, a special set of "organizational wings" for UAS pilots was created, and the requirement that UAS operators undergo typical pilot training was instated.[49]

In terms of operational gains, USAF has flown UASs continuously, often in sorties upwards of 24 hours with "about three dozen USAF UAVs and a much larger number of smaller Army variants"[50] in the air over conflict zones such as Afghanistan, Iraq and Syria at any given time. While it is hard to quantify the benefits of UAS usage comparative to what USAF operations with traditional means would have looked like without substantial HALE or MALE UASs, it is informative that as of 2014 USAF UASs were "conducting over 500 strike missions per year."[51] These figures, combined with the increased intelligence gathering and reduced risk to human pilots through reduced need for humans to perform the "Dull, Dirty, or Dangerous"[52] missions these sorties carry out, would seem to preliminarily indicate a significant return on the US's investment. However, it is important to be mindful of the infrastructure, operational tempo and budgetary concerns that set the American situation apart from the Canadian.

While American defence and security priorities require high and continuously global operational tempo, Canadian priorities are less demanding, and thus, the incredible costs of infrastructure procurement and maintenance become substantially more pronounced in light of actual operational needs. Obtaining a HALE UAS such as the Global Hawk, favoured by those advocating Canadian UASs[53] for maritime/Arctic ISR, would require upwards of a billion dollars in initial investment,[54] and as such systems are reliant on satellite communication (SATCOM) for control,[55] it would likely require the launch of Canadian controlled secure military-communications satellites.[56] With Canada having already invested upwards of $445 million in the Polar Epsilon satellite-reconnaissance project for northern ISR[57] (with $100–$249 million planned for Polar Epsilon 2),[58] being aware of the disruptive cultural frictions and interservice tensions adopting UASs created for the US and in the costly midst of updating its core air power capabilities via conventional contemporary aircraft, the RCAF's lack of enthusiasm for emulating a structure similar to that of USAF becomes understandable.

Looking elsewhere, the UK's RAF emulated USAF with a nearly identical though significantly smaller force structure regarding MALE and HALE UASs.[59] As a result, the RAF has faced similar problems of cultural friction internally. RAF leadership has addressed this problem in part, as the Americans have, by requiring full pilot training as well as by granting UAS pilots their "wings."[60] However, slight coloration differences in the wings worn on the uniform continue to set UAS pilots apart from their traditional counterparts.[61] Regarding set-up costs, the RAF circumvented much of them through close cooperation with USAF via use of shared facilities, infrastructure and training; their first of two squadrons having been based at Creech Air Force Base in Nevada until 2013.[62] However, according to a 2014 UK House of Commons Defence Committee report, "the consequence of this strategic partnership is a significant continuing UK dependence on the USAF for support infrastructure and future upgrades to Reaper systems, and access to the USAF training programme for Reaper pilots and sensor operators."[63] What this shows is that while purchasing off-the-shelf models used by the US presents a lower cost of acquisition, it creates a relationship of dependency for expertise, training, parts and infrastructure. It also demonstrates the disruptive effect to service culture that introducing UASs to an air force can have as well as the importance of properly choosing whether to adapt/integrate another's technology or to indigenously develop it along the lines of the RCAF's own culture and needs.

The French Air Force (FAF), while only beginning its use of tactical-sized systems in 1995[64] with the Israeli-designed RQ-5 Hunter,[65] quickly graduated in 2007 to using a SATCOM-reliant MALE reconnaissance UAS known as the Harfang,[66] a modified Heron. In 2013, under the Projet de loi de programmation militaire 2014-2019,[67] the FAF began its transition to using the popular Reaper, currently possessing three, with a plan to have twelve operational by 2019;[68] it is worth noting, however, that as of 2015, though possible, these UASs have not been armed due to public sentiment.[69] Unlike the RAF, the FAF has opted to purchase a European C2 system, which it will have full ownership of; however, it did cooperate with USAF in training its initial Reaper crews at Holloman Air Force Base in New Mexico.[70]
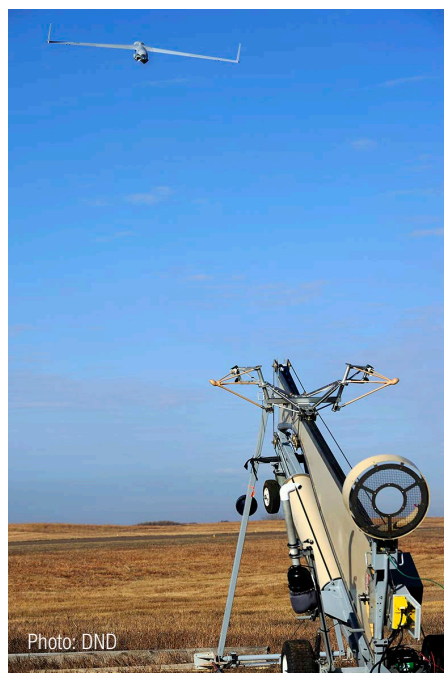
The RAAF stands out as a case study for Canadian UAS integration purposes. Similar to Canada, maritime and overland ISR have been identified as critically important areas of national security and defence for Australia; these ISR missions are also ones in which air power plays a substantial and growing role. Furthermore, the RAAF is both a part of the F-35 acquisition programme and is in the midst of updating its maritime/overland ISR capability under the multiphase Air 7000 programme.[71] This programme is a plan outlining the creation of a balanced force of manned-unmanned systems to serve ISR purposes and continue to foster HALE UAS familiarity within the RAAF. Also like Canada, Australia has been involved with UASs since the 1960s, was home to UAS research initiatives and had a fledgling UAS industry from early on.[72] Furthermore, the Australian Army and Navy

Photo: DND

A Boeing ScanEagle micro-unmanned air vehicle (MUAV) is catapulted into the air during Exercise MAPLE RESOLVE 1101 in Wainwright, Alberta, October 21, 2011.

Can Unmanned Aircraft Systems Meet Canadian Air Power Needs?

operate their own tactical systems;[73] the SHADOW 200[74] and ScanEagle (the same one used by the Canadian Navy) respectively, with the RAAF remaining focused on HALE- and MALE-scale systems. Also using the squadron model of organization, the RAAF currently has one squadron, created in 2010, which operates Herons, the same UASs that were originally leased by Canada until 2011, the initial training notably having been provided in Canada as well, though this has since shifted to Australia.[75] It is difficult to accurately gauge how disruptive to internal air force culture the introduction of UAS pilots has been for the RAAF; however, RAAF pilots are required to train to the same standards of normal manned-aircraft pilots and are then selected upon certification to serve in the specialized role.[76] Some friction can be discerned, however, from the language used in related writings; Australian Army Lieutenant Colonel Tim Rutherford wrote in 2014 about the rise of the "warrior geeks" in reference to UAS and cyber-warfare operators, and articles such as the one titled "Boys Toys a Part of Defence" still appear in civilian papers.[77] Particularly interesting from a Canadian perspective is the UAS that the Australian government committed to purchasing pursuant to the Air 7000 program in a 2016 defence White Paper,[78] the MQ-4C Triton.[79] The Triton is a HALE/MALE UAS designed specifically for broad area maritime surveillance (BAMS); it relies only on ground-based C2, has an enhanced anti/de-ice capable airframe[80] and has the capability to act as a mobile network-relay node.[81] The latter capability means that the UAS itself can be an alternative to in-theatre reliance on satellites, provide data transfer and cross-theatre networking capabilities as well as offer a redundant form of theatre-wide communication. Seemingly, this could be the ideal UAS for Canadian purposes, and close attention should be paid to the RAAF experience with it in the coming years.

ON AIR-AIR CAPABLE UASs AND THE F-35

While Canada has not expressed an explicit interest in the possibility of armed UASs down the road, it is worth considering what is possible and developing. Currently, the offensive capabilities of the most sophisticated UASs are limited to ground strikes, though with the advent of projects such as the X-47 and Dassault Neuron, unmanned air combat appears to be an impending reality.[82] Both of these projects are aimed at delivering an air-to-air combat UAS, the former being a US project and the latter a French, and both are in their early phases. Some, such as Captain Michael W. Byrnes of USAF,[83] have speculated that an air-air UAS reality is closer at hand than most would think and is only a matter of combining presently available or developing systems. The imagined result is a UAS capable of completing the observe, orient, decide and act (OODA) loop, conceptualized by John Boyd, with such efficiency and maneuverability without regard for human restrictions such that it would render manned fighters nearly obsolete,[84] if not relegated to "mothership" status.[85] This mothership concept is actually focused on the current development of the Neuron, a "swarm" functionality being planned for use with the new Raphael fighters.[86] The UAS in this conceptual-ization screens ahead for threats, provides sensor data to the Raphael pilots over a wide area, serves as a decoy against enemy systems and even engages enemy air assets.[87] This swarm concept and the advantages of having an ambient swarm of integrated air-air capable air cover is not lost on the naval thinkers of the world either, with Ian Shields and James Spencer putting forward a vision of naval air power in the form of "commando carriers," filled and protected by such UASs.[88] The benefits being more air assets per ship, persistent air cover and ISR by virtue of long loiter times as well as a reduction of the need for large carriers and their extensive crews.[89] Exciting and revolutionary as these capabilities are, many within the Canadian military purport that they are still far from reliably attainable within the time frame that the F-35's lifespan is expected to provide for. Preparing for the arrival of these technologies, such as with the example of planned integration with Raphael, is an excellent strategy and one which the incoming F-35s may become capable of further into their lifespan, as recent proof-of-concept tests with the F-16 have hinted at as a possibility.[90] At present,

though shunned by the current Liberal Government, the F-35 certainly has the confidence and support of many within the RCAF, even when considered in light of the developing X-47, as was done by former Chief of Force Development Lloyd Campbell.[91] Campbell, and others, find it "inconceivable that an operationally viable, multirole UCAV [unmanned combat aerial vehicle] will become available in time to realistically replace the CF188 fleet at the end of this decade."[92]

A VERDICT ON CANADIAN UASs

Having considered Canadian air power needs, current fleet improvement projects as well as how and which UASs have been integrated into several major air forces, the emulation of the RAAF stands out as Canada's best option. With the current budget proposal for the JUSTAS programme being between $500 million and $1.3 billion,[93] Canada could theoretically emulate an American scheme on a smaller scale in a way similar to what was done by the RAF; this would include the launch of a SATCOM constellation, possibly a merger of capabilities with the Polar Epsilon 2 satellite constellation project and would likely involve the purchase of a currently conceptual modified Global Hawk system capable of Arctic flight known as the Polar Hawk. This approach is not only among the most expensive, a not unsubstantial problem in itself with regard to the amounts already being spent on other procurements, but the ISR capabilities it would generate come with the introduction of complications and vulnerabilities associated with relying on SATCOM for C2 of the UAS. These issues include maintaining space assets, the vulnerabilities presented by potential loss of control in the event of SATCOM failures, risk of cyberattack, all in light of the fact that for all the cost/ complications, the role could be filled by a small manned aircraft.

Emulating the RAAF, with its slimmer dedication to UASs and planned combination of manned-unmanned systems to complement one another specifically for the roles of maritime and overland surveillance, has obvious benefits for Canada, particularly the adoption of a UAS not reliant on SATCOM. The Triton (the system recently committed to by the RAAF, with its network-relay capability, incredible range/loiter time, maritime-specific design and high vertical manoeuvrability) would seem to be the perfect fit for Canadian needs with regard to identifying and tracking ships and people, providing additional communications/networking capabilities in remote regions and enhancing day-to-day ISR overland, in both the maritime regions and the North. With the JUSTAS timeline currently set to only reach the first phase, definition approval, in 2017, and contract award / implementation approval by 2020,[94] there is plenty of time to observe the RAAF scheme and experience with the Triton specifically; the close relationship between the RCAF and RAAF allows for a potential fostering of domestic knowledge and familiarity with the system, force structure and application of UASs to maritime security. Thus, Canada should, for the immediate future, keep abreast of developments with a keen eye on the RAAF and should not rush to emulate our allies to the south simply to gain UAS capability where current fleet improvements and initiatives will provide for the RCAF's actual air power needs. The reality of such emulation would require a retooling of current procurements and their budgetary needs, likely creating only further unproductive costs and delays across the board. Canada's immediate air power future may not be a robotic one, but the door is certainly not closed to having robotic systems alongside manned capabilities down the road; it is merely a matter of finding the right fit, possibly with a later version of the Triton, and a force structure similar to the RAAF.

Conrad Orr is currently a civilian postgraduate student at the Royal Military College of Canada studying for a master's in War Studies. Conrad also holds a Bachelor of Arts in Law from Carleton University and is currently focusing his academic research on air power, small wars and intelligence methodologies.

ABBREVIATIONS

C2	command and control
CAF	Canadian Armed Forces
CFDS	*Canada First* Defence Strategy
DND	Department of National Defence
FAF	French Air Force
HALE	high-altitude long-endurance
ISR	intelligence, surveillance and reconnaissance
JUSTAS	Joint Unmanned Surveillance and Target Acquisition System
MALE	medium-altitude long-endurance
Op	operation
RAAF	Royal Australian Air Force
RAF	Royal Air Force
RCAF	Royal Canadian Air Force
SAR	search and rescue
SATCOM	satellite communication
UAS	unmanned aircraft system
UAV	unmanned air vehicle
UK	United Kingdom
US	United States
USAF	United States Air Force

NOTES

1. P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin Press, 2009), 47–49.

2. Home web pages for information on the Avenger, Eitan and Reaper are respectively: "Predator C Avenger RPA," General Atomics Aeronautical, accessed May 6, 2016, http://www.ga-asi.com/predator-c-avenger; "UAV's," Israeli Air Force, accessed May 6, 2016, http://www.iaf.org.il/903-34528-EN/IAF.aspx; and "Predator B Avenger RPA," General Atomics Aeronautical, accessed May 6, 2016, http://www.ga-asi.com/predator-b.

3. Andrew Carryer, *A History of Unmanned Aviation in Canada* (Richmond, BC: MacDonald, Dettwiler and Associates, 2008) 3–4.

4. Gary Schaub, "JUSTAS for All? Innovation and UAVs in the Canadian Forces," *Defence Studies* 15, no. 2 (2015): 124, accessed May 6, 2016, doi:10.1080/14702436.2015.1035941.

5. David Rodman, "Unmanned Aerial Vehicles in the Service of the Israel Air Force," *Meria Journal*, 14, no. 3 (September 2010), accessed May 6, 2016, http://www.rubincenter.org/2010/09/rodman-2010-09-07/.

6. Schaub, "JUSTAS for All?," 124.

7. "ScanEagle Unmanned Aerial Vehicle," Boeing, accessed May 6, 2016, http://www.boeing.com/history/products/scaneagle-unmanned-aerial-vehicle.page.

8. "UAS: RQ-11B Raven," AeroVironment, accessed May 6, 2016, http://www.avinc.com/uas/small_uas/raven/.

9. Schaub, "JUSTAS for All?," 134.

10. "Sperwer System," Safran Sagem, accessed May 6, 2016, http://www.sagem.com/land-defense/tactical-uav-systems/sperwer-system.

11. "Heron TP," Israeli Aerospace Industries, accessed May 6, 2016, http://www.iai.co.il/2013/18551-37204 EN/Groups_Military_Aircraft_MALAT_Products_Heron_Family.aspx.

12. Schaub, "JUSTAS for All?," 130 and 133.

13. Canada, Department of National Defence (DND), "*Canada First* Defence Strategy" (Ottawa: Department of National Defence, 2008), accessed May 6, 2016, http://www.forces.gc.ca/en/about/canada-first-defence-strategy.page#ql2; "Joint Unmanned Surveillance and Target Acquisition System," DND, accessed May 6, 2016, http://www.forces.gc.ca/en/business-defence-acquisition-guide-2015/aerospace-systems-59.page.

14. Canada, DND, "*Canada First* Defence Strategy," 3.

15. Schaub, "JUSTAS for All?," 129.

16. Ibid.

17. "Joint Unmanned Surveillance and Target Acquisition System."

18. Canada, DND, "*Canada First* Defence Strategy."

19. "Joint Unmanned Surveillance and Target Acquisition System."

20. Levon Bond, "JUSTAS and Project Epsilon: Integrated Intelligence, Surveillance, and Reconnaissance of the Canadian Arctic," *Canadian Military Journal* 13, no. 4 (Autumn 2011): 25–26.

21. John Manley et al., *Independent Panel on Canada's Future Role in Afghanistan* (Ottawa: Minister of Public Works and Government Services, 2008).

22. Murray Brewster, "Canadian Military Drone Plan Grounded Amid Debate," *Toronto Star*, August 17, 2014, accessed May 6, 2016, http://www.thestar.com/news/canada/2014/08/17/canadian_military_drone_plan_grounded_amid_debate.html.

23. Schaub, "JUSTAS for All?," 130.

24. Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, NY: Cornell University Press, 1991), 19–20.

25. Theo Farrell and Terry Terriff, *The Sources of Military Change: Culture, Politics, Technology* (Boulder, CO: Lynne Rienner Publishers, 2002), 4–10.

26. "UAV Display Brings Modern History to Greenwood Museum," Sara Keddy, Canada, DND, Government of Canada, accessed May 6, 2016, http://www.rcaf-arc.forces.gc.ca/en/article-template-standard.page?doc=uav-display-brings-modern-history-to-greenwood-museum/hwn8upn9.

27. Schaub, "JUSTAS for All?," 130.

28. Ibid., 130–31.

29. These being systems with a take-off weight of less than 84 kilograms.

30. Scott Bishop, "Libya and the Lessons of Naval Power," *Canadian Naval Review* 8, no. 4 (Winter 2013): 17.

31. "Canada Military Drones: ScanEagle, Unmanned Aircraft, To Be Deployed on Mediterranean Missions," *The Huffington Post*, November 22, 2011, accessed May 6, 2016, http://www.huffingtonpost.ca/2011/11/22/canada-drones-scaneagle_n_1108479.html.

32. D. F. Holman, "The Future of Drones in Canada: Perspectives from a Former RCAF Fighter Pilot," Strategic Studies Working Group Papers (n.p., Canadian Defence & Foreign Affairs Institute, August 2013), accessed May 6, 2016, http://www.cdfai.org.previewmysite.com/PDF/The Future of Drones in Canada.pdf: 7; and Bond, "JUSTAS and Project Epsilon," 28.

33. Colonel Ryoji Shirai, *Incorporating Unmanned Aerial Systems into the Japan Air Self-Defense Force* (Washington, DC: Brookings Institution, Center for 21st Century Security and Intelligence, September 2014), 23–24, accessed May 6, 2016, http://www.brookings.edu/research/papers/2014/09/25-unmanned-aerial-systems-japan-air-self-defense-force-shirai.

34. "Overview," Canada, DND, accessed May 6, 2016, http://www.rcaf-arc.forces.gc.ca/en/overview.page.

35. Ibid.

36. André Deschamps, "Into the 21st Century – An Overview of Canada's Air Force in 2010," *Canadian Military Journal* 10, no. 4 (2010).

37. Ibid., 59–60.

38. Ibid., 60.

39. Ibid.

40. "Operation IMPACT," Canada, DND, accessed May 6, 2016, http://www.forces.gc.ca/en/operations-abroad-current/op-impact.page.

41. Ibid.

42. Deschamps, "Into the 21st Century," 60–61.

43. Ibid., 61.

44. "F-35," Liberal Party of Canada, accessed May 6, 2016, https://www.liberal.ca/realchange/f-35/.

45. Deschamps, "Into the 21st Century," 62.

46. "Fixed-Wing Search and Rescue Aircraft Replacement Project," Canada, Public Works and Government Services Canada, accessed May 6, 2016, http://www.tpsgc-pwgsc.gc.ca/app-acq/amd-dp/air/arsvf-fwsar/index-eng.html.

47. Shirai, *Incorporating Unmanned Aerial Systems*, 18.

48. "Squadron Activated at Creech," *Las Vegas Review-Journal* (March 6, 2008), accessed May 6, 2016, http://www.reviewjournal.com/news/squadron-activated-creech.

49. Shirai, *Incorporating Unmanned Aerial Systems*, 18–20 and 28.

50. "UAV & UCAV: Force Multipliers," Defence and Security of India, April 2, 2014, accessed March 1, 2016, http://defencesecurityindia.com/uav-ucav-force-multipliers/ (site discontinued).

51. Shirai, *Incorporating Unmanned Aerial Systems*, 18.

52. Singer, *Wired for War*, 54.

53. Holman, "Future of Drones in Canada," 7; and Bond, "JUSTAS and Project Epsilon," 27.

54. Holman, "Future of Drones in Canada," 7.

55. "Data Overload: Satellite Communications on the Battlefield," Grant Turnbull, Airforce Technology, November 27, 2013, accessed May 6, 2016, http://www.airforce-technology.com/features/feature-data-overload-satellite-communications-battlefield/.

56. Ibid., 4.

57. "Archived - Polar Epsilon Project," Canada, DND, accessed May 6, 2016, http://www.forces.gc.ca/en/news/article.page?doc=polar-epsilon-project/hnps1uo5.

58. "Archived - Polar Epsilon 2," Canada, DND, accessed May 6, 2016, http://www.forces.gc.ca/en/business-defence-acquisition-guide-2015/joint-and-other-systems-19.page.

59. Shirai, *Incorporating Unmanned Aerial Systems*, 23–24.

60. Ibid., 25.

61. Jasper Copping, "The First Deskbound Drone Pilots Get their RAF Wings," *The Telegraph*, April 2, 2013, accessed May 6, 2016, http://www.telegraph.co.uk/news/uknews/defence/9967186/The-first-deskbound-drone-pilots-get-their-RAF-wings.html.

62. Shirai, *Incorporating Unmanned Aerial Systems*, 23–24.

63. UK, House of Commons Defence Committee, "Remote Control: Remotely Piloted Air Systems - Current and Future UK Use: Government Response to the Committee's Tenth Report of Session 2013–14," (London, UK: House of Commons, 29 July 2014), 34, accessed May 6, 2016, http://www.publications.parliament.uk/pa/cm201415/cmselect/cmdfence/611/611.pdf.

64. Shirai, *Incorporating Unmanned Aerial Systems*, 24.

65. "Hunter," Israeli Aerospace Industries, accessed May 6, 2016, http://www.iai.co.il/2013/18555-16401-EN/Groups_Military_Aircraft_MALAT_Products_Hunter.aspx.

66. "Harfang MALE Unmanned Aerial Vehicle (UAV), France," Airforce Technology, accessed May 6, 2016, http://www.airforce-technology.com/projects/harfang-drone/.

67. France, Ministry of Defense, *Projet de loi relatif à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale* (Paris: Présidence du Sénat, 2013), accessed May 6, 2016, http://www.senat.fr/leg/pjl12-822.html [viewed by author through Google translate].

68. Shirai, *Incorporating Unmanned Aerial Systems*, 25.

69. "French Air Force Reapers Exceed 2 000 Flight Hours," DefenceWeb, November 17, 2014, accessed May 6, 2016, http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=37015:french-air-force-reapers-exceed-2-000-flight-hours&catid=35:Aerospace&Itemid=107.

70. Shirai, *Incorporating Unmanned Aerial Systems*, 25.

71. Australia, Department of Defence, *Defence Capability Plan 2012, Public Version.* (Canberra: Australia, Department of Defence, Capability Development Group, 2012), 62–67, accessed May 6, 2016, http://www.defence.gov.au/publications/capabilityplan2012.pdf.

72. Shirai, *Incorporating Unmanned Aerial Systems*, 26.

73. "Unmanned Aerial Vehicles," Australia, Army, September 7, 2012, accessed May 6, 2016, http://www.army.gov.au/Our-work/Equipment-and-clothing/Surveillance/UAV; and "Insitu Pacific to Provide ScanEagle Services to Royal Australian Navy," Irawan Dheni, Defence News, accessed May 6, 2016, http://www.antaranewss.xyz/2012/07/insitu-pacific-to-provide-scaneagle.html.

74. "Shadow," Textron Systems, accessed May 6, 2016, http://www.textronsystems.com/products/unmanned/shadow.

75. Shirai, *Incorporating Unmanned Aerial Systems*, 26–27.

76. Ibid., 27.

77. Tim Rutherford, "Rise of the Warrior Geek: The Impact of Remote Systems on Future Personnel Needs," *Australian Defence Force Journal* no. 195 (2014), accessed May 6, 2016, http://www.adfjournal.adc.edu.au/UserFiles/issues/195 2014 Nov_Dec.pdf; and Larry Pickering, "Boys' Toys a Part of Defence's Testosterone 'Culture,'" *Pickering Post*, April 23, 2014, accessed May 6, 2016, http://pickeringpost.com/story/boys-toys-a-part-of-defence-s-testosterone-culture-/3142.

78. Australia, Department of Defence, *2016 Defence White Paper* (Canberra: Australia, Department of Defence, 2016), 87 and 94, accessed May 6, 2016, http://www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf.

79. "MQ-4C Triton: Persistent Maritime Intelligence, Surveillance and Reconnaissance," Northrop Grumman, August 15, 2012, accessed May 6, 2016, http://www.northropgrumman.com/MediaResources/MediaKits/GEOINT/Documents/MQ-4C_Triton_datasht.pdf.

80. Ibid.

81. "Triton Drone Prepares for First Flight," Kris Osborne, DefenseTech, accessed May 6, 2016, http://www.defensetech.org/2013/04/04/triton-drone-prepares-for-first-flight/.

82. "X-47B UCAS Makes Aviation History … Again!," Northrop Grumman, accessed May 6, 2016, http://www.northropgrumman.com/Capabilities/x47bucas/Pages/default.aspx; and "nEUROn Capabilities," Dassault Aviation, accessed May 6, 2016, http://www.dassault-aviation.com/en/defense/neuron/introduction/.

83. Michael W. Byrnes, "Machine Autonomy in Air-to-Air Combat," *Air & Space Power Journal* 28, no. 3 (2014): 48–75; and Michael W. Byrnes, "Dark Horizon: Airpower Revolution on a Razor's Edge," *Air & Space Power Journal* 29, no. 5 (2015): 31–56.

84. Byrnes, "Machine Autonomy in Air-to-Air Combat."

85. "Unmanned Aerial Vehicles: Current Developments and Future Utility," *The Military Balance* 108, no. 1 (2008): 458.

86. Ibid.

87. Ibid.

88. Ian Shields and James Spencer, "An Unmanned Future for Naval Aviation," *The RUSI Journal* 156, no. 6 (December 22, 2011).

89. Ibid.

90. "Imagine F-16s Deploying Swarms of Tiny Drones," War Is Boring, March 10, 2016, accessed May 6, 2016, http://warisboring.com/articles/imagine-f-16s-deploying-swarms-of-tiny-drones/.

91. Lloyd Campbell, "Replacing the Canadian Manned Fighter Capability," *Canadian Military Journal* 11, no. 3 (2011): 59, accessed May 6, 2016, http://www.journal.forces.gc.ca/vo11/no3/09-campbell-eng.asp.

92. Ibid.

93. "Joint Unmanned Surveillance and Target Acquisition System."

94. Ibid.

AIR POWER THEORY AND FORCE CLASSIFICATION

BY MATHEW PRESTON, BA, MSS

INTRODUCTION

Theories of air power often assume that the force studied is large and capable of strategic mass. The literature is essentially blind to smaller air forces; the Royal Canadian Air Force (RCAF), the Royal Australian Air Force (RAAF) and the Royal Netherlands Air Force mean, essentially, nothing throughout the literature. They are not allowed the funding or manpower to muster numbers large enough to be considered capable of providing a strategic effect, nor do they have capabilities that are purely and inherently strategic (from a traditional standpoint), such as intercontinental ballistic missiles (ICBMs) or intercontinental bombers like the B-1 or Tu-160. Often, air forces are considered to be either "large," like the United States Air Force (USAF), or "small." This definitional habit groups the RCAF and RAAF with air forces far less capable than themselves from a qualitative perspective. This, in turn, limits the strategic consideration given to incredibly modern but quantitatively limited air forces.

Traditional air power theory often focuses on the strategic uses of air power. Strategic bombing has largely characterized this theoretical framework, becoming practical in World War II (WWII) and achieving theoretical perfection with the advent of thermonuclear weapons. Following WWII, a distinction was created between strategic air power and tactical air power. The traditional separation of definitions has created a situation in which smaller air forces are unable to operate across the entire air power spectrum. The focus on large air forces within air power literature creates a theoretical problem, especially when considering air power as employed by the combined services of the United States. If these definitions of air power do not adequately describe the contributions and capabilities of smaller air forces such as the RCAF, then a new understanding within air power theory is required.

A number of theoretical and technological changes have taken place and facilitate the creation of a new classification system that can be used to discuss the application and operation of strategic air power in the modern context.

THE VIETNAM SHIFT

"For centuries most of the things shot by military men at their enemies have missed their target."[1] During the Vietnam War, in the air, at least, that reality had changed and was apparent in the minds of military men. Between 14 and 15 May 1972, air power saw a technological feat that would increase its effectiveness more than was ever before thought possible. Fourteen sorties of fighter-bombers managed to destroy two bridges in North Vietnam that had previously seen 871 sorties fail at the cost of 11 aircraft.[2] The F-4 Phantoms were able to succeed where conventional bombers had failed due to the use of laser-guided precision-guided munitions (PGMs), and at $8,000 apiece, the Paveway bombs used were as effective as twenty-five unguided bombs of higher yield and that were more expensive.[3] While there had been variations of weapons with guidance systems since 1943, the 1972 attacks marked the beginning of the modern era of precision weapons.[4] What was especially significant for the current discussion is that while there had been laser-guided systems used in combat before the 1972 bridge raids, this was the first instance of a single fighter-bomber carrying both the bomb and the target marker.[5] A RAND study in 1975 summed up the shift in capability thusly: "tanks may be efficiently hit by RPVs [remotely piloted vehicles] launched from big bombers, 'tactical' submarines could send cruise missiles against enemy ICBM silos."[6] The lines were blurred by PGMs. Therefore, these weapons are an important component to a definition of air power, as they have the "potential to destroy enemy ground forces either on the move or in defensive positions at a high rate while concurrently destroying vital elements of the enemy's war

fighting infrastructure."[7] They can be wielded to even greater proportional effect by small air forces; logistical chains are smaller and are required to move less, making it easier to get into the field faster.[8]

> Air power advocates have long dreamed of a day when the weapon, platform, and willingness to use them properly would come together to make air power a decisive force. Today, those dreams are reality. One need only look back to our raids on Schweinfurt, Germany, in World War II to see how dramatically precision weapons have enhanced our capabilities over the last 50 years. Two raids of 300 B-17 bombers could not achieve with 3,000 bombs what two F-117s can do with only four. Precision weapons have truly given new meaning to the term *mass*.[9] [emphasis in original]

Even before the Gulf War—the campaign that generated the previous comment—PGMs were understood to be game changing. The aforementioned RAND study noted that "accuracy is no longer a strong function of range … if a target can be acquired … it can usually be hit. For many targets, hitting is equivalent to destroying."[10] The Gulf War showed that by far the most effective weapons were PGMs, most of those being dropped from fighters or small attack aircraft.[11] The large bombers which made up Strategic Air Command's forces were relegated to being bomb-trucks for cruise missiles. What this showed is that for the most part, barring payload size limitations, the fighter-bomber, or multirole fighter, is the most effective combat aircraft available to a modern air force. Most applicable to RCAF-sized air forces is that the multirole fighter is the best platform for the modern application of air power. In the era of PGMs, "the best combination is, not surprisingly, the trained operator on a smart platform with smart sensors dispensing a smart weapon."[12]

A FUNCTIONALIST AIR FORCE

Before adding a new structure within the theoretical assumptions of air power, it must be stressed that there is no real distinction between strategic air power and tactical air power—only the reason behind its deployment. As strategist Edward Luttwak attests, "During the last fifty years or so, the habit has developed of applying the adjective 'strategic' to long-range forces and weapons, as opposed to 'tactical' bombers and missiles."[13] Adding that, "we obtained this unfortunate terminology from the rhetoric of the early airpower advocates."[14] To Luttwak, there are levels of weapons usage: tactical, operational and strategic.[15] Weapons are not strategic, only the nature of their employment can be considered strategic. Colin Gray echoes this sentiment, which is simply shown in the title of his book *Air Power for Strategic Effect*. Air power is strategic when it is used strategically, not because it has certain characteristics in its material make-up. Some observers would note that it is impossible to act strategically without bringing sufficient mass to bear to defeat an enemy. This is a false notion of strategic. If the Trans-Pacific Partnership can be a strategic act (through establishing Western economic norms to Asia before China can implement its own framework),[16] then having a small air force act in a particular way within a coalition can be just as strategic. This is especially true for middle powers, who are largely unable to achieve strategic goals with hard power alone. Instead, military force is deployed in concert with allies to achieve a political end. The goal of the war itself is not the political end, but merely being there to prosecute the war achieves the national policy. Arguably, this is the most relevant to Canadian strategy as well as most nations fielding air forces that would be equivalent in size to the RCAF. Functionalism wins the day.

Small air forces cannot create mass. This, however, does not prevent them from acting strategically. The strategic imperative of tier 2 air forces[17] is, broadly speaking, to a) maintain their alliances

(whether that be among a broad alliance or in the Canadian example to maintain the favour of the United States) and/or b) maintain peace, security and humanitarianism in exchange for either international or domestic political capital. In this way, making a *meaningful* contribution is a strategic imperative. Providing some CC130s to help move munitions does not endear oneself to USAF. Taking full control of a theatre of the airborne battlespace (say, for example, Canada is totally responsible for a specific area of the Libyan airspace) does. And this, in turn, can only be achieved if the tier 2 air force is *qualitatively* equal to a tier 1 air force. Basically, in order to act strategically, it is not enough to make a contribution; one must make a meaningful contribution.

Bearing this in mind, it can be seen that material defeat of an enemy is not the only—or even central—strategic objective of a small or medium-sized air force. Instead, the strategic goal is the political capital gained by playing an important role in the campaign (which can be actual war fighting, deterrence or simply reassurance). This requires a new way of thinking about air force composition and the employment of air power.

In many ways, this seems self-evident for any middle power, whether employing air, sea or land power. Air power, however, consists of unique characteristics that necessitate definitional refinement when considering its employment by middle powers. Technological developments come about exceptionally fast, and there are few, if any, great power conflicts that allow for real-world testing of tactics and technology. While land power undergoes technological change (and is even less likely than air forces to come into contact with a peer or near-peer competitor), the fundamental tactical employment changes little whether opposing a first-rate squad or an insurgency. With this in mind, the following definition is proposed:

> Air power is the ability of an air force to employ its power, both kinetic and non-kinetic—such as search and rescue (SAR); airlift; or command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR)—in a specific area and over a specific amount of time in order to defeat an enemy or achieve a goal. This includes either material or political defeat of an enemy, or an increase in a nation's standing within an overall power structure.

With this definition, air power can be employed by a broader range of actors and in multiple ways. An attack against the enemy's army can be strategic or tactical, depending on the method of deployment of the armed forces. If the main use of air power is to destroy the enemy's tanks, for example, air power is in support of an invading army; thus it is tactical. If, on the other hand, the destruction of the enemy's tanks brings about the collapse of the enemy's war effort, such as in Iraq in 1991, then the action is indeed strategic. In this way, aircraft can do the exact same job in both the strategic and tactical realms, showing that air power, while it can be used for strategic ends, is not inherently strategic in any way.

DEFINING SMALL AIR FORCES

"For air forces, the size of the country's population is not as vital as its characteristics."[18] Technology and training are key. This is especially true for air forces that are unable to match the quantity of larger and more affluent states. While technology and training act as force multipliers in all aspects of warfare this is especially true for air power. Technology and training are the first aspects that provide a division between the different types of air forces.

> TO SIMPLY RELY UPON *SMALL* AND *LARGE* AS DISTINGUISHING TERMS IS PROBLEMATIC BECAUSE USE OF THESE TERMS IS DEPENDENT UPON TOO MANY INDEFINABLE FACTORS.

To simply rely upon *small* and *large* as distinguishing terms is problematic because use of these terms is dependent upon too many indefinable factors. Reference to small air forces and large air forces is common in the literature, but rarely are these terms clearly defined. If air forces are distinguished by size alone, then the importance of technology, training and favourable geography is lost.[19] Additionally, the split into two broad terms, large or small, leaves air forces like Canada's in the same category as less technologically and numerically capable air forces from small Caribbean and Baltic nations. Technology and training can be used to distinguish between the types of air forces. As S. A. Mackenzie describes, in one of the few works dedicated to small air forces: "Let it be that a small air force is one that, for some fundamental reason, such as economic, geographic, political or social, will have chosen not to conduct some element or part of the complete air power spectrum."[20] This definition limits an air force not by size, but by capability, which is a helpful distinction.

A high level of training and technical proficiency are also keys to any able air force. This is illustrated by Colonel John Boyd's OODA loop. OODA stands for observe, orient, decide and act and is a mental process that is extremely important for pilots. The faster a pilot can complete the thought process, the better they will be, and the pilot who goes through the loop fastest, generally, wins.[21] The better the training, the faster the OODA loop, and the better the air force is, as a sum of its pilots.[22] "Done well, it [the OODA loop] becomes the key to winning … done exceedingly well, it becomes the mark of genius."[23] Only an air force that dedicates itself to an intensive training regime is able to produce pilots who are among the best in the world. If, using Mackenzie's logic, air force capability is based on capabilities and not quantity, then one can also include the metric of power-projection capability.

Having been defined, the theoretical understanding of air power can be discussed without the misnomers of large and small. Instead of saying an air force is small or large, it would perhaps be more useful for a discussion on air power to separate air forces into tiers. A tier 1 air force would have to include those of the United States, Russia as well as, while not perfect examples, Britain and France. These air forces do not compromise any capabilities; all have full air-combat capabilities including dedicated air-superiority fighters, fighter-bombers, ground-attack platforms as well as full cruise missile and ICBM capabilities. These states have full capabilities in the non-kinetic means of air power as well, especially airlift, SAR, electronic warfare (EW) and airborne warning and control systems (AWACSs). Additionally, they have access to the highest level of technology and are able to project their power anywhere in the world due to either friendly air bases or naval air power. Technical advancement in

the guise of simulators also allows pilots to undergo extensive training. So, the characteristics of a tier 1 air force are: no compromise on the type of capabilities, highest possible level of technology and the ability to project power anywhere in the world. This comes from the idea that the United States—due to its numerous carrier groups, foreign bases and agreements for basing with allied countries—is the most powerful air force numerically, technologically and through its ability to project force worldwide. Since the United States is the most powerful air power in the world, its key characteristics are the best to compare all others to, and its abilities are to be considered top tier.

If, as Mackenzie argues, a small air force naturally compromises some aspect of the air power spectrum for reasons of geography, technology, economics or national character, then the logic can be extended that they also make compromises to the ability to project power. Countries such as Australia, Canada, the Netherlands and Norway exemplify a tier 2 air force. They do not compromise on kinetic capabilities in their manned platforms, and all operate multirole fighters as their primary combat vehicle. Major compromises occur in the size of their airlift capabilities; lack of dedicated air-to-ground platforms, dedicated interceptor or air-superiority aircraft; and a limited, if not absent, cruise missile or ICBM capability. While some, such as Australia and the Netherlands, are moving towards having naval air capabilities,[24] most are unable to project power in this way, and none can operate in a high-intensity environment, far from home, without substantial help from an ally or allies. The capabilities that these air forces choose to deploy, however, are qualitatively on par with a tier 1 air force. The biggest difference between a tier 1 and tier 2 air force is quantitative, not qualitative. This is partially the result of the effectiveness and relative low cost of PGMs, although other technological and personnel factors are also important. Training is incredibly key in this respect. Only the rich—or incredibly dedicated—countries can afford to run their planes and pilots in real-world training to such an extent as to give them a competitive edge. With the growth of fifth-generation fighter capabilities, technological advancement will also become necessary in the very near future. Additionally, the high level of technology that is afforded to quantitatively small air forces, as the Australian example will show, illustrates the idea that it is no longer technology that separates large air forces from small. To sum up, a tier 2 air force has the following characteristics: qualitative technological parity with tier 1 powers, combat aspects heavily reliant on the multirole fighter, little compromise on capability (largely only in quantitative aspects) and, finally, the limited ability to project air power anywhere, anytime, without the aid of a major ally or coalition of allies.

Finally, a tier 3 air force compromises most air-spectrum capabilities, focusing largely on kinetic capabilities and geared towards operations only within its own region. A tier 3 air force is unable to afford advanced technology, especially in the EW and AWACS spectrum, and is, therefore, severely inhibited in any conflict involving a tier 1 or tier 2 air force. The ability to project power also determines the level at which an air force operates. As mentioned, a tier 3 air force's level of power projection is relatively poor. While a tier 2 air force can project power anywhere in the world with some help of others (or in some cases with only the need for basing rights and not actual logistics), a tier 3 air force is only able to deploy worldwide if it is completely piggybacking on a larger and more capable air force. Largely, a tier 3 air force is able to operate only within its immediate area. Technologically, they rely heavily on previous-generation fighters and other aircraft, and training is limited due to finances. Due to their technological capabilities, many non-Western or non-industrialized countries have tier 3 air forces.

Since a tier 2 air force would most readily apply in the Canadian context, it is these air forces that will receive the most attention. First, this group's focus—PGMs, multirole fighters, airlift, and now EW and AWACS capability—has made these air forces more of a tactically orientated

group in the traditional sense. The RCAF, in particular, has historically deployed this way. During the early stages of the Cold War, the RCAF Air Division in Europe was first equipped with the F-86 Sabre, an air-superiority fighter,[25] and later with tactically important aircraft, primarily the CF-104 Starfighter.[26] This, along with the CF-5, was acquired primarily for the tactical-strike role in Europe.[27] The big air forces, the United States primarily, would deal with the strategic aspects of air power, specifically bombing Russian facilities behind the lines. Canada, along with the other allied states, focused on this tactical type of air power employment. This has led to tactically orientated doctrines being accepted in these air forces. This can be seen in the procurement of aircraft, especially the primary fighter. When the CF188 was procured, it was largely chosen due to its multirole, tactical capabilities.[28]

In the current era, tier 2 air forces are focusing on high-technology and multimission-capable aircraft. Australia is a perfect example of this. The purchase of EW capable EA-18 Growlers, F-35 fighters and Boeing Wedgetail (a highly capable EW, AWACS and C4ISR aircraft that is considered by many to be better than anything the United States currently deploys) reveals a focus on high technology, multirole and multimission capability, but in small numbers.[29] Additionally, these are all traditionally tactical tools. None are meant to strike at an enemy's homeland, behind the lines; they are for operational, front-line use.

There is no objective reality concerning strategic air power or tactical air power; air power is only used for tactical or strategic means. PGMs are the main tool of modern air forces and are employed primarily from multirole fighters, meaning the ability of tier 2 air forces to apply air power can be fully evaluated. If, as discerned previously, air power is the ability to act both strategically and tactically, as defined by the commander of the operation or political leaders in a specific area, for a specific amount of time, how do these tier 2 air forces fit within air power theory?

The ability to act both strategically and tactically is largely dependent on the nature of what is meant by strategic. Traditionally, in the air power context, strategic is equated with targeting the enemy's homeland in order to bring about the collapse of their war efforts. This can be seen in the writings of Douhet, Trenchard and even Warden.[30] As discussed, tier 2 air forces are largely geared towards tactical operations or, at least, what are perceived as tactical operations. With the newfound ability of PGMs to strike smaller targets, there is no need for city bombing. Therefore, there is no need for a dedicated weapons platform for strategic bombing in a high-intensity conflict. Since the multirole fighter is highly capable, especially in the deployment of PGMs, and tier 2 air forces rely heavily on the multirole fighter, then in the arena of bombing, the tier 2 air forces are well positioned for this capability. The multirole fighter's importance to modern air power, even to a tier 1 air force, can be demonstrated by these air forces shrinking the number of different aircraft that their fleet is made up of as the abilities of the multirole fighter become more apparent. The American replacement for the Harrier, A-10, F-16, F-18 and F-15E by the F-35 shows this as well as the Chinese movement to a two-ship air force (the J-20 for air superiority and J-31 for more strike-orientated missions). Increasingly, one or two highly capable variants of the fighter-bomber or air-superiority fighter are being seen as able to do the majority of the heavy lifting. As this is how most tier 2 air forces are outfitted, it sets them up to be just as capable to deploy air power as a tier 1 force, at least in the immediate area of operations, if not theatre wide.

The notion that it is the commander who decides what is a strategic and what is a tactical deployment in terms of air power is one that is actually harder for a tier 2 air force to work with at a political level, at least as individual actors. As mentioned, tier 2 air forces are rarely, if ever, able to operate in an expeditionary fashion without the aid of allies, largely due to the limits a tier 2

A CF188 Hornet takes off in Constanta, Romania during Exercise RESILIENT RESOLVE.   Photo : MDN

force has in numbers. When deployed overseas, they operate largely as part of a coalition. This means that they are not able to set the strategy of their own campaign. Often they are under the command of another (e.g., a North Atlantic Treaty Organization [NATO] mission commander) where they are unable to determine what application of air power is strategic and what is tactical. For example, the RCAF played a role in the Kosovo air strikes in 1999, but they were only given strike packages, the nature of which were determined by NATO headquarters. Tier 2 air forces are simply being a good soldier and bombing the target. This, however, does help to illustrate the fact that a tier 2 air force is able to act both strategically and tactically.

Finally, the last aspect of air power—the ability to operate in a specific area for a specific period of time—is fully within the realm of the tier 2 air force. Since tier 2 air forces, as described, are largely qualitatively equal to a tier 1, then all that is preventing a tier 2 air force from achieving air supremacy is numbers. The technological ability to suppress enemy air defences, both air and ground based, is one that is becoming increasingly important with tier 2 forces. The Australian example of the F-35, Growler and Wedgetail procurement, all with either a strong stealth and/or EW capability, shows that the ability to suppress highly capable air defences is falling within the reach of tier 2 air forces.[31] This ability allows them to operate in a given area, free from enemy harassment, for a given period of time. This includes the ability to operate for a specific amount of time in a specific area both kinetic air power, such as ground attack or close air support, and non-kinetic air power, such as airlift and SAR. Imagine a bubble of safety around a nation's air assets in theatre. This is what modern air power represents geographically.

THE IMPLICATIONS OF A DIFFERENT UNDERSTANDING OF AIR POWER AND AIR FORCE SIZE

Why create a new definition of air power? And why does this matter, and how can it affect small, yet well-trained and capable, air forces? Air power is by far the most theoretical of the dimensions of war.[32] Because technology changes much faster than the rate at which high-intensity engagements with which to test theories against occurs, it is important to develop theory and doctrine in order to stay up to date in training and ways of thinking. If times they are a-changin', then so should the way the times are a-thought about.

This is not to say that previous definitions were wrong, or insufficient, or, for that matter, that some things do not stay the same. It is always important to find the enemy's centre of gravity, for the air campaign as much as for the total war effort. Additionally, while the weapons change, the principles never will. Step one, and always step one, achieve air supremacy, or in a highly equal engagement, air superiority, and then attack the enemy as needed. The end goal of air power will always be to achieve air superiority in a theatre, allowing the free use of air power.[33] The attack on the enemy may be strategic, such as Warden's concentric circles of prime targets, or tactical, like the attack on Muammar Gaddafi's armour to protect civilians and aid rebel fighters. Sometimes, the two merge, such as in DESERT STORM and the attack on Republican Guard tanks.[34] Regardless, there will always be targets inherently tactical, inherently strategic and ones that blur the lines. No change in technology will change these realities.

The most important thing that a comprehensive definition of air power does is that it expands the definition's applicability by making it more specific. It does little for air power theorists to define air power simply as something done from the air. This creates a definition so broad that it makes thinking about the issue too abstract.

Another reason to expand the definition of air power is that most theorists have geared their work towards large, or tier 1, air forces. Giulio Douhet called for Italy to field a force of 20,000 bombers, while John Warden was writing in the American context.[35] By expanding the definition to include a specific place for a specific amount of time, the idea of all places at all times is eliminated, which is a realization that air power is really only achievable by the United States.

Creating a definition and theoretical framework that is as applicable to smaller air forces as it is to large ones provides the ability to both assess the performance of all air forces and recommend suitable procurement, deployment and doctrine moving forward. For example, the idea that a tier 2 air force can be qualitatively as good as a tier 1 is expressed in the new definition, but a tier 2 air force can only properly employ air power if it maintains an array of capabilities. It may compromise some capabilities, but very few if it wants to compete and employ air power successfully. Unlike the trend in smaller armies, to become niche forces in order to better serve coalitions,[36] smaller air forces must maintain a strong all-around capability.

Recently, in the Libyan operation of 2011, Canada showed the importance of a multicapable air force. Due to upgraded systems, the CF188 was one of the most capable multirole fighters in the operation. The newly acquired CC177 Globemasters made it possible for the RCAF to operate independently, albeit from Italian airfields, an act that would have been impossible with only the CC130s that were previously Canada's only heavy-lift aircraft. The CP140 Auroras that were brought into theatre provided highly capable sensors, and despite their limited number, highly trained Canadian CF188 pilots utilizing the newest technology flew a surprisingly high proportion of the sorties, despite providing only seven fighters. Only a qualitatively equal air force, with many different capabilities, would have been able to perform as well.

Despite the awesome power afforded by air platforms, it is still a relatively young field, which is why there are so many theorists with so many views. It has yet to reach maturity and is constantly changing due to technological advancements, which are much more influential in air power than any other dimension of warfare. Despite this, there is rich scholarship on the issue, both by academics and practitioners of air power. Due to the nature of air power, the plethora of writers and the lack of a real foundational base (like a Clausewitz),[37] it is hard to reach a real consensus on how to define air power, let alone employ it. That should not, however, stop us from trying.

Mathew Preston is a strategic consultant (and owner) at Heartland Strategic based in Calgary. He received his Master of Strategic Studies from the University of Calgary's Centre for Military and Strategic Studies. He is also a part-time farmer, musician and volunteer firefighter. He tweets @prestonm2 and occasionally blogs for the Canadian Global Affairs Institute's 3DS Blog.

ABBREVIATIONS

AWACS	airborne warning and control systems
C4ISR	command, control, communications, computers, intelligence, surveillance and reconnaissance
EW	electronic warfare
ICBM	intercontinental ballistic missiles
NATO	North Atlantic Treaty Organization
OODA	observe, orient, decide and act
PGM	precision-guided munition
RAAF	Royal Australian Air Force
RCAF	Royal Canadian Air Force
SAR	search and rescue
USAF	United States Air Force
WWII	World War II

NOTES

1. James Digby, "The Technology of Precision Guidance: Changing Weapon Priorities, New Risks, New Opportunities" (Santa Monica, CA: RAND Corporation, 1975), 1.

2. Stephen Budiansky, *Air Power: The Men, Machines, and Ideas that Revolutionized War, From Kitty Hawk to Gulf War II* (Toronto: Penguin Books, 2004), 408.

3. Ibid.; and Doctor Richard Hallian, "Precision Guided Munitions and the New Era of Warfare," APSC Paper Number 53 (Canberra: Air Power Studies Centre, 1997), 8, accessed May 4, 2016, http://airpower.airforce.gov.au/Publications/Details/110/Precision-Guided-Munitions-and-the-New-Era-of-Warfare.aspx.

4. Hallian, "Precision Guided Munitions," 8.

5. Digby, "Technology of Precision Guidance," 2.

6. Ibid., 7.

7. Alan J. Vick et al., *Enhancing Air Power's Contribution Against Light Infantry Targets* (Santa Monica, CA: RAND Corporation, 1996), 54–57.

8. Ibid., 30–31.

9. General Buster C. Glosson, quoted in David R. Mets, *The Long Search for a Surgical Strike: Precision Munitions and the Revolution in Military Affairs* (Maxwell Air Force Base, AL: Air University Press, 2001), 36.

10. Digby, "Technology of Precision Guidance," 7.

11. Roughly 9 per cent of the munitions dropped in Iraq were PGMs, yet they destroyed roughly 90 per cent of the targets during the campaign. Hallian, "Precision Guided Munitions," 3.

12. Ibid.

13. Edward N. Luttwak, *Strategy: The Logic of War and Peace* (Cambridge, Mass: Harvard University Press, 1987), 90.

14. Ibid.

15. Ibid.

16. Michael B. Froman, "The Strategic Logic of Trade: New Rules of the Road for the Global Market," *Foreign Affairs* (November/December 2014), accessed May 4, 2016, https://www.foreignaffairs.com/articles/americas/strategic-logic-trade.

17. Tier 1, 2 and 3 air forces will be discussed in detail later in this article.

18. Robin Higham, "Introduction," in *Why Air Forces Fail: The Anatomy of Defeat*, ed. Robin Higham and Stephen J. Harris (Lexington, KY: The University Press of Kentucky, 2006), 2.

19. Squadron Leader S. A. Mackenzie, "Strategic Air Power Doctrine for Small Air Forces" (Canberra: Air Power Studies Centre, 1994), 1.

20. Ibid.

21. David S. Fadoka, "John Boyd and John Warden: Airpower's Quest for Strategic Paralysis," in *The Paths of Heaven: The Evolution of Air Power Theory*, ed. Phillip S. Meilinger (Maxwell Air Force Base, AL: Air University Press, 2002), 366.

22. Ibid., 366–67.

23. Ibid., 367.

24. "Amphibious Assault Ship (LHD)," Royal Australian Navy, accessed May 4, 2016, www.navy.gov.au/fleet/ships-boats-craft/lhd; and "Ships," Royal Netherlands Navy, accessed May 4, 2016, www.defensie.nl/english/organisation/navy/contents/navy-units/ships.

25. Raymond Stouffer, "Nuclear Virgin or Nuclear Strike? John Diefenbaker and the Selection of the CF104 Starfighter," in *Sic Itur Ad Astra Canadian Aerospace Power Studies, Volume 3, Combat if Necessary, but not Necessarily Combat*, ed. W. A. March (Ottawa: Department of National Defence, 2011), 29.

26. Ibid., 29 and 33.

27. Ron Pickler and Larry Milberry, *Canadair: The First 50 Years* (Toronto: CANAV Books, 1995), 186.

28. Kim Richard Nossal, "Late Learners: Canada, the F-35, and Lessons from the New Fighter Aircraft Program," *International Journal* (Winter 2012–13): 168.

29. "Australia's 2nd Fighter Fleet: Super Hornets & Growlers," Defense Industry Daily, accessed May 4, 2016, http://www.defenseindustrydaily.com/australia-to-buy-24-super-hornets-as-interim-gapfiller-to-jsf-02898/; "The Wedgetail Enters into Service: The Aussies Build Out their 21st Century Airpower Capabilities," Second Line of Defense, accessed May 4, 2016, http://www.sldinfo.com/the-wedgetail-enters-into-service-the-aussies-build-out-their-21st-century-airpower-capabilities/; and "The Coming of the F-35 to Australia: Shipping a 21st Century Approach to Airpower," Robbin Laird, Second Line of Defense, site discontinued, http://www.sldinfo.com/the-coming-of-the-f-35-to-australia-shaping-a-21st-century-approach-to-airpower/.

30. Phillip S. Melinger, "Giulio Douhet and the Origins of Airpower Theory," in *Paths of Heaven*, 1; Phillip S. Melinger, "Trenchard, Slessor, and Royal Air Force Doctrine before World War II," in *Paths of Heaven*, 41; and Colonel John Warden, *The Air Campaign: Planning for Combat* (n.p., Macmillan Publishing, 1998), 7.

31. "Growler Advocates Outline Stealth Vulnerabilities," Amy Butler, Aviation Week, accessed May 4, 2016, http://aviationweek.com/awin/growler-advocates-outline-stealth-vulnerabilities.

32. Frederick W. Kagan, *Finding the Target: The Transformation of American Military Policy* (New York: Encounter Books, 2006), 126.

33. Walter J. Boyne, *The Influence of Air Power upon History* (Gretna, LA: Pelican Publishing, 2003), 18.

34. Budiansky, *Air Power*, 418.

35. Melinger, "Giulio Douhet," 6.

36. See Ugurhand G. Berkok, "Specialization in Defence Forces," *Defence and Peace Economics* 16, no. 3 (2005): 191–204.

37. Colin S. Gray, *Airpower for Strategic Effect* (Maxwell Air Force Base, AL: Air University Press, 2012), 13.

Commander RCAF, Lieutenant-General M. Hood, presents Lieutenant-Colonel Paul Martin with the inaugural Carr Award. Part 1 of his winning paper, "Cyber Warfare Schools of Thought: Bridging the Epistemological/Ontological Divide," follows. Part 2 will be published in the fall issue.

The Carr Award

In order to promote vital airpower research within the Royal Canadian Air Force (RCAF), the RCAF Commander has instituted a series of awards that will recognize individuals who contribute first-class papers that address airpower-related issues.

Five research awards have been established, and the first to be awarded in the series is the Carr Award, which is presented to a Joint Command and Staff Programme student at Canadian Forces Staff College for a pre-eminent paper on an innovative airpower topic.

The Carr Award is so-named in recognition of Lieutenant-General Bill Carr, a highly decorated World War II veteran who is considered the father of the modern Canadian air force. He retired in 1978 after 36 years of dedicated service, and his final leadership role was as the creator and first Commander of Air Command.

Beginning with his first Spitfire flight over enemy territory while commanding the United Nations air transport operation in the Congo, Lieutenant-General Carr, a pilot with over 18,000 flying hours, understood the importance of air power and experienced first-hand the effects of technological advancements.
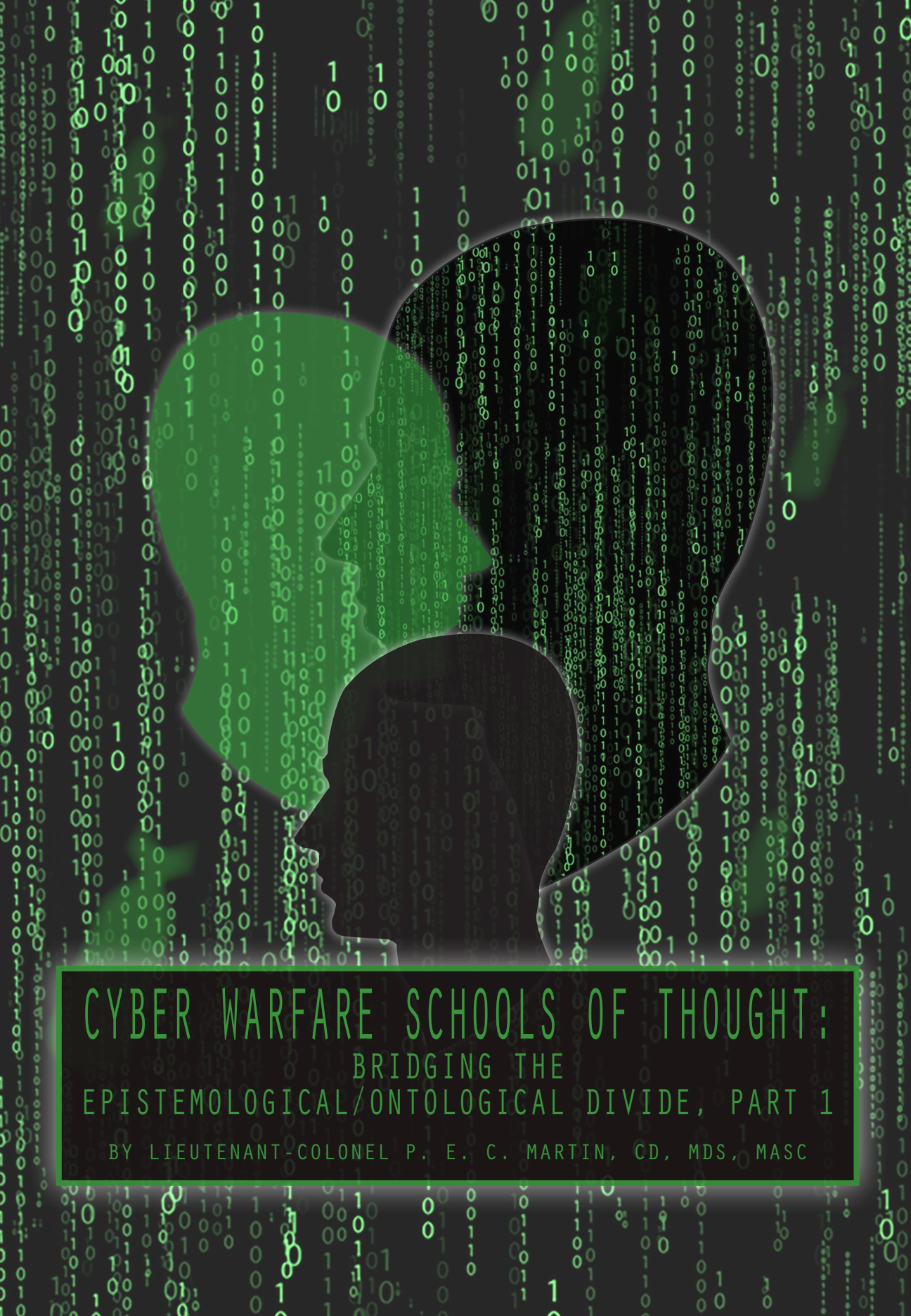
CYBER WARFARE SCHOOLS OF THOUGHT:

BRIDGING THE EPISTEMOLOGICAL/ONTOLOGICAL DIVIDE, PART 1

BY LIEUTENANT-COLONEL P. E. C. MARTIN, CD, MDS, MASC

ABSTRACT

There are tangible ontological influences of modern-day communications and computerization on our daily lives. An important consequence of the increasing dependence on networked communications is that it presents opportunities for agents wishing to exploit system vulnerabilities. These agents range from nation states to non-state actors. The most basic question a modern military confronts from the challenge of cyber threats is: "what is to be done?" Purely technological responses are available, but the implications of their use often raise more questions than they answer. Governments and militaries are presented with a basic epistemological problem which hinders their ability to answer the question already posed. Analysing the existing body of relevant literature offers a process by which the uncertainties posed by these questions can be sorted out. However, the rapid pace of developments bedevils those who seek to keep up with this evolving issue. This paper seeks to rectify this situation by proposing a schema for classifying the different epistemological conceptions in terms of discrete, cyber warfare schools of thought. By so doing, a better understanding of the differing conceptions is both possible and achievable. Ultimately, the purpose of such a typology is to help bridge the epistemological/ontological divide that exists in different understandings and conceptions of cyber.

CHAPTER 1 — INTRODUCTION

The nations, of course, that are most at risk of a destructive digital attack are the ones with the greatest connectivity.[1]

– Kim Zetter

The activities and capabilities of the cyber realm are often influenced by exposure to popular culture and visionary writers of science fiction. An example of this is the 1983 movie *War Games*, in which a high school student hacks into a military system to play online games but almost initiates global thermonuclear war by accident. In the 2015 movie *Blackhat*, nuclear plant safety and trade exchange security are imperiled by evil individuals with cyber exploitation skills. These sorts of fears and concerns related to the possible implications of the wired world on human existence are shaping opinions on what cyber connectivity represents. Does the interconnected environment hosting the cyber activity represent a new arena, territory or battlefield? Popular culture would seem to suggest that cyberspace is in fact a new construct for individuals to conduct daily tasks as well as to interact and exchange information with other individuals in a highly interconnected fashion. With origins relating back to the ancient Greek term *kubernétés*,[2] cyberspace as a term was derived from Norbert Wiener's 1948 seminal work[3] on cybernetics and automation. Wiener's philosophy and pursuit of automation to improve people's lives have led to the current perceptions of cyberspace as a medium in which masses of people are interconnected and influenced by the activities within this realm.[4]

DEFENCE AND SECURITY IMPLICATIONS

Cyber security within the Canadian federal government is increasingly becoming a point of concern not only from the perspective of information confidentiality, integrity and availability but also in terms of public safety. There are unambiguous ontological[5] influences of modern-day communications and computerization on our daily lives. Alun Munslow, in his book *The Routledge Companion to Historical Studies*, defines the meaning of ontology as:

> that branch of metaphysics that addresses the general state of being, the nature of existence, and how the human mind apprehends, comprehends, judges, categorizes,

makes assumptions about and constructs reality. For the historian ontological questions arise when we address how to create historical facts within the larger ontology of our own existence, that is, the condition(s) of being under which we create or construct the-past-as-(the discipline of)-history.[6]

Human existence—the ontological—is progressively being supported by computerized information. The reality of increasing dependence on networked communications presents opportunities for those wishing to exploit system vulnerabilities ranging from nation states to non-state actors. In Canada today, the Department of National Defence and the Canadian Armed Forces (CAF) are responsible for providing defence intelligence as well as monitoring cyber threats and providing military response options to them.[7]

The most basic question a modern military confronts from the challenge of cyber threats is: "what is to be done?" Information technology (IT) offers a host of new capabilities for military forces. They offer new opportunities for acquiring information and executing action within a battlespace as well as the potential for generating new threats. But events do not wait for us to have a systematic understanding of them before they occur, as the Stuxnet[8] and Buckshot Yankee[9] incidents illustrate. The daily news announces that more computer systems have been hacked and compromised by malware; more companies and governments have lost information to spies, criminals and activists;[10] and more individuals have had their privacy invaded.[11] Nearly every United States (US) arms programme tested in 2014 showed "significant vulnerabilities to cyber-attacks,"[12] including some of the most sophisticated weapon systems in use or development. The United States Air Force (USAF) saw the Predator and Reaper drone fleets infected with the "credential stealing" virus and the F-35 fighter was revealed to have a cyber vulnerability in the Autonomic Logistics Information System that could allow adversaries to defeat the plane without ever firing a round.[13]

Despite being a priority for action, the absence of doctrine for cyber warfare frustrates our ability to think about what should be done in terms of a military response to potential incidents or threats. Purely technological responses are available, but the implications of their use can raise more questions than they answer. Governments and militaries are presented with a basic epistemological problem which hinders their ability to answer the question of what a proper course of action might be. Munslow defines the meaning of epistemology as:

> the branch of philosophy that addresses the nature, theory and foundations of knowledge, its conditions, limits and possibilities. Historians, as the creatures of the modernist (Cartesian Enlightenment) revolution, have tended to stick with a particular vision of what history is, derived from a certain kind of analytical philosophy (this is often un-thought out as most historians are not actively engaged by philosophy of any sort).[14]

Has cyber interconnectivity changed our being and the conduct of military activities? The Canadian military involvement in cyber tests the very epistemological foundations of traditional military culture and the nature of warfare. Is cyber discrete and distinct enough that it has a cultural imperative strong enough to transcend land, sea and air domains? Sea, land and air forces have an internal logic to them by nature of the environment in which they operate. The sea generates a different culture than the land or the air.[15] The nature of military-based cyber operations may be so different from those on the land, at sea and in the air that cyber operations should be encultured in a separate and distinct domain designation.[16] The absence of a clear typology for cyber conceptions generates uncertainty in determining a clear path for action.

CYBER WARFARE SCHOOLS OF THOUGHT

Consulting the literature is typically a process by which the uncertainties posed by these questions can be sorted out. However, the rapid pace of developments in computer issues bedevils those who seek to keep up with this evolving field. Even experts can express feelings of being overwhelmed by the rapid pace of events and the explosion of writing on the subject. Dorothy Denning, a well-known cryptologist, wrote of the challenge of completing her landmark book on information warfare in 1998:

> A major challenge has been keeping up with developments in the field, including new technologies, methods of attack, laws, and studies and developments related to incidents covered in the book. On a typical day, I find another story or two in *The Washington Post* of some book or magazine. By the time this book goes to print, I no doubt will have accumulated a huge pile of material that I wish could have been included.[17]

This explosion of literature has to be organized in some way if any sense is to be made of the data. With no clear guideposts to the rapidly accumulating mass of material, it remains to the individual reader to make sense of the wealth of material, and it is easy to become quickly overwhelmed. The epistemological understanding of what cyberspace is and how it relates to the ontological being of humanity varies greatly depending upon individual biases and perspectives. This paper seeks to rectify this situation by proposing a schema for classifying the different opinions in terms of discrete cyber warfare schools of thought.

If the literature for cyber warfare is examined, one can see clear delineations between three groups or schools of thought, each of which revolves around specific assumptions about the nature of how IT is affecting the practice of warfare. The schools can be placed on a spectrum of opinions along which one can measure a dialectical relationship between technological and human agency (see Figure 1). The three schools can be grouped in the following manner: Revolutionary materialist, Liberal Materialist and Conservative.
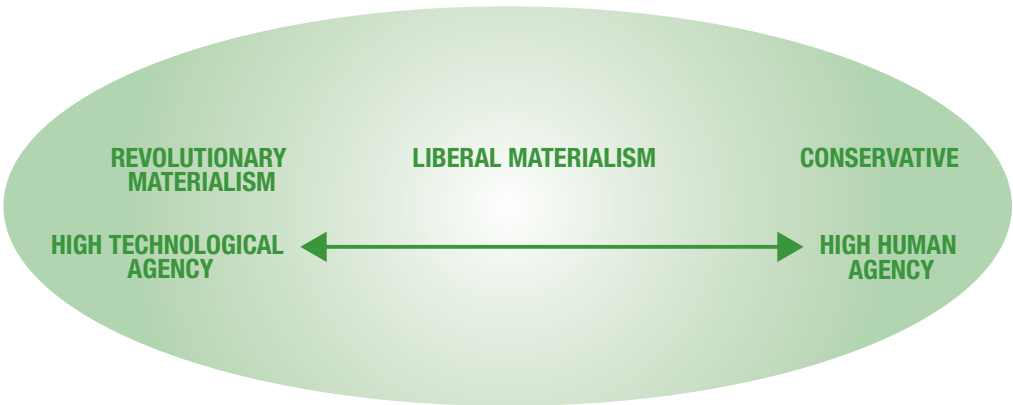

Figure 1. Cyber warfare schools of thought

The Revolutionary Materialist school of thought makes the basic assumption that IT will change the praxis[18] of warfare, if not the nature of war itself. The Revolutionary school of thought bears a close resemblance to air power theory in both its basic credo and its objectives. Revolutionaries, like

the air power theorists before them, emphasize the possibilities for manoeuvre that IT offers military forces. Cyber warfare can be used to go around or avoid confrontation between major military forces altogether. By attacking a state's critical infrastructure through a major event (frequently referred to as an electronic Pearl Harbor [EPH]), the state's ability to control both its regular military forces as well as society itself will be compromised. Financial markets are disrupted, transportation grids are rendered dysfunctional, electrical power is removed from broad swathes of the country, and information networks are collapsed. Social chaos results from these actions, and the state loses its ability to act. A war effectively ends through basic governmental paralysis and/or regime change.

The Liberal Materialist school of thought is closely related to the Revolutionary school in its focus on materialism, but it places a greater emphasis on the ability of human agency to control the effects of cyber warfare through the power of social institutions. Liberals emphasize the trans-formative power of technology on the nature of society itself. Unlike the Revolutionaries, however, Liberals emphasize a more evolutionary process in which technology produces new phenomena which both individuals and institutions can take advantage of as they see fit for their own ends. Globalization is part of this process. Liberals, like Revolutionaries, see challenges to the ability of the state to control the issues confronting them. The emergence of non-state actors, a feature that is facilitated by the lowered entry costs that IT affords, allows various and sundry individuals and groups to diffuse power away from the state. For them, the future is far more uncertain in terms of what will ultimately emerge because of the unplanned emergent nature of this free choice in terms of both technology and praxis. While they observe that things are changing because of this expansion of agency, the normative vector of that change is unpredictable—it could be good or bad for society. This highlights the centrality of human agency in the technical aspects of the evolutionary process. Liberalism speaks more to the enabling of agency than of any assumed progressive outcome associated with technological development. Cyber warfare is just one aspect of this process of societal evolution. It represents a risk for the future, but not one that is impossible to resist and might even be brought under the firm control of the state (either in terms of its ultimate rejection or its practical employment as just another tool).

Finally, the Conservative school of thought is inherently reactive to the claims both the Revolutionaries and Liberals make. It makes the basic assumption that IT has always been important to the conduct of warfare; therefore, its effects will not be revolutionary but will be more in line with the nature of additions to the existing models of warfare. Secondly, Conservatives emphasize the role of the state in its ability to impose local order on an otherwise anarchical system. In other words, this school accepts the increasing importance of IT to the prosecution of war but denies that it fundamentally changes everything. In this conception, change is incremental or evolutionary at best. It represents simply the steady increase of military capability that militaries have dealt with since at least the dawn of the industrial age and the advance of science in terms of weapons development. The school tends to be heavily influenced by the writings of Carl von Clausewitz,[19] which it uses as a benchmark from which to observe the effects that IT is having on the acts of war. However, some Conservatives also examine the fundamental nature of IT and emphasize the operational limitations affecting the Revolutionary claims of the previous school of thought. In particular, Conservatives tend to emphasize the human context of warfare, rather than its technological domain. Their challenges tend to be epistemologically based, raising basic questions about the implications stemming from future predictions of technological capability. Their observations tend to revolve around the praxis of warfare, rather than any theoretical or hypothetical predictions. History remains very much a guide to understanding the continuation of the essentials of human conflict. Finally, Conservatives seem to emphasize the social construction of military technology. Weapons serve specific political

and organizational needs rather than driving military affairs in and of themselves. In this, the Conservatives make a definite break between their Revolutionary and Liberal Materialist challengers. Rather than stressing the scientific potential or the technical application of technological affordances, Conservatives focus on the practical questions which revolve around its use.

This paper will address the potential impacts of cyber warfare on CAF by observing changes to the praxis of warfare through the different lenses and perspectives associated with the cyber warfare schools of thought schema. Leveraging this schema to acknowledge the potential biases towards cyber warfare, one can better bridge the divide between what one knows about this new technology through evidence-based epistemological induction and the changes/influences cyber capabilities continue to have on our very existence from an ontological perspective. In order to traverse the epistemological/ontological divide, this paper will conduct a comprehensive review of cyber warfare literature and arrange the key ideas by chapter according to the relevant cyber warfare school of thought schema. Chapters 2, 3 and 4 will articulate the Conservative, Revolutionary Materialist and Liberal Materialist cyber warfare schools of thought respectively. Finally, Chapter 5 will conclude this paper with the key points derived from applying the cyber warfare schools of thought schema to the wealth of cyber-based literature as well as consider how an institution may approach bridging the epistemological/ontological divide. In addition, the conclusion portion of Chapter 5 will provide some thoughts and recommendations for CAF leadership facing the challenges of exposure to and use of cyberspace in future defence activities and the need for epistemological normalization to effectively bridge the divide.

CHAPTER 2 – THE CONSERVATIVE SCHOOL OF THOUGHT

Conservatism discards Prescription, shrinks from Principle, disavows Progress; having rejected all respect for Antiquity, it offers no redress for the Present, and makes no preparation for the Future.[20]

– Benjamin Disraeli

It is questionable if all the mechanical inventions yet made have lightened the day's toil of any human being.[21]

– John Stuart Mill

Those who subscribe to the Conservative cyber warfare school of thought are cautious in their perception and acceptance of technological changes to society and the conduct of war. Typically, Conservative perspectives are reluctant to change or to contemplate new concepts that challenge the nature and dogma of warfare. As a group, the Conservative school favours the preservation of established principles and praxis of warfare and in doing so opposes the contemplation of changing their perspectives based on any ontological changes that may be due to technology. This school tends to employ the writings of Clausewitz, Jomini and Sun Tzu as the foundation of their epistemological assessment of military affairs through historical evidence-based induction and reject things that do not conform to this framework of understanding.[22]

Being averse to change, this school is resistant to the notion of technology-led Revolutions in Military Affairs (RMAs),[23] siding with the more traditional concept of evolution in military technological innovation. Through incremental/evolutionary approaches to technological changes, the Conservative school is able to defend traditional concepts of warfare and incorporate any modified praxis based on the advantages of the increase in technology.

TECHNICAL EVOLUTION VICE REVOLUTION

In his book *Strategy for Chaos*, the British strategic thinker Professor Colin S. Gray discusses the concept of RMAs and their occurrences throughout history. Gray articulates how RMAs manifest themselves through "strategy" or the employment of "force and the threat of force"[24] in the achievement of political goals. Furthermore, Gray views war as "organized violence carried on by political units against each other for political motives."[25] From this train of thought, Gray views an RMA as "a radical change in the character or conduct of war" that is not necessarily instigated by new technology.[26] Gray's theories of RMAs conform to the Conservative school of thinking by closely aligning with the Clausewitzian approach to strategy where warfare is both instrumental and political.[27] As Clausewitz stated in *On War*, "war is not merely a political act but a real political instrument, a continuation of political intercourse, a carrying out of the same by other means."[28]

Gray offers a nine-step framework to further explain how an RMA process alters the character or conduct of warfare.[29] First – Preparation: RMAs require time to manifest themselves as a non-linear change/reform and are generally considered a radical alteration to the praxis of warfare. Second – Recognition of Challenge: The identification of an opportunity or challenge posed by an adversary that generates a reason requiring an RMA solution. Gray highlights that for there to be a true RMA, there must be a belief in a real adversary offering a strategic challenge. Third – Parentage: An RMA requires revolutionary leadership in positions of authority to facilitate the change. Fourth – Enabling Spark: A person or event that acts as a catalyst for the RMA to occur and deviate the praxis of warfare off its linear evolutionary path. Fifth – Strategic Moment: The opportunity to convey the RMA possibilities to those open minded to receive the revolutionary messaging. Sixth – Institutional Agency: The requirement for a military institution to adopt, train on and implement with competence the innovative operational concepts fuelled by new technologies. Seventh – Instrument: The military instrument of the new RMA is established and institutionalized through formalization within doctrine and training. The new military instrument/capability must also be grown and replicated in size to have significant impact on the praxis of the institution as well as its potential adversaries. Eighth – Execution and Evolving Maturity: The application and employment of the RMA in battle will have an initially significant and destabilizing effect on its adversaries. The destabilizing effect will be reduced with subsequent uses and demonstrations of the RMA as adversaries learn from this new mode of warfare. Ninth – Feedback and Adjustment: If an enemy is not overwhelmed by the first application of the RMA capability, it will study and counter it with like capabilities or appropriate tactics to nullify the strategic effectiveness of the new and innovative way to conduct war. To be continually effective as a warfare instrument, the capability must be continually adjusted to counter adversarial adaptations. In effect, feedback and adjustment creates a new linear evolutionary path in the same direction forged by the non-linear radical change itself.

> TYPICALLY, CONSERVATIVE PERSPECTIVES ARE RELUCTANT TO CHANGE OR TO CONTEMPLATE NEW CONCEPTS THAT CHALLENGE THE NATURE AND DOGMA OF WARFARE...
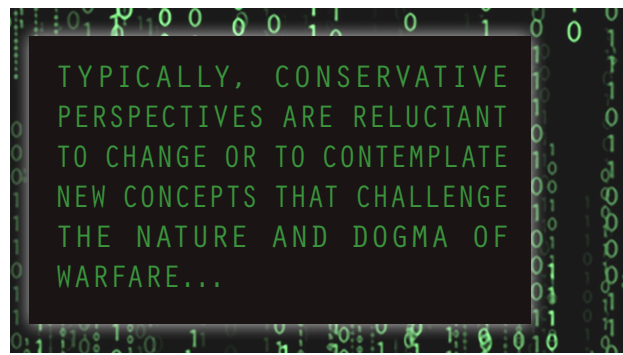
Comparing historical examples of RMAs (such as the French revolutionary wars, the First World War and the nuclear age) with the potential information-led (cyber) RMA of the 1990s, Gray concludes that cyber as an event in strategic history lacks the necessary political and human actions to be considered an RMA.[30] The Conservative school position is that cyber represents increased technology but has done little to change the character or nature of war.[31]

The Conservative view of warfare is less technologic and very much human-agency centric in thinking. Aligned with the writings of Clausewitz with respect to the intangible elements of human nature and morale in warfare, the Conservative school is more concerned about the human element and not the weapons technology that impacts strategy. Clausewitz states:

> Military activity is never directed against material force alone; it is always aimed simultaneously at the moral forces which give it life, and the two cannot be separated … the moral elements are among the most important in war … . Unfortunately they will not yield to academic wisdom. They cannot be classified or counted. They have to be seen or felt.[32]

Those in the Revolutionary school that prefer technical over political solutions are often seen as self-serving technocrats who focus on the means vice the ends of strategy.[33] Gray argues: "When people and organisations are not required to think about difficult topics (in this case, policy assumptions and strategy), they will choose to focus on more congenial topics (e.g., a technically defined RMA)."[34]

Others in the Conservative school view cyber as an incremental/evolutionary increase in technology more akin to existing capabilities performing electronic warfare. With the advent of wireless networking and telephones that are also network appliances, the characteristics that distinguish electromagnetic-spectrum issues from data-network-infrastructure issues are becoming common to both disciplines.[35] Others in the Conservative school consider that a "Cyber Electronic Warfare (CEW) concept, which merges cyberspace capabilities with traditional electronic warfare methods, is a new and enhanced form of electronic attack."[36] The convergence between wireless communications and cyber leads the Conservative school to believe "that the cyber environment is nothing new. Rather, it is simply a unique manifestation of the electromagnetic (EM) operating environment—a familiar component of military operations with integral operating concepts and principles that lend themselves well to cyber."[37] The US Chief of Naval Operations, Admiral Jonathan W. Greenert, argued in 2012 that wireless activity in the EM spectrum had become integral to cyberspace. Admiral Greenert stated: "The EM-cyber environment is now so fundamental to military operations and so critical to our national interests that we must start treating it as a warfighting domain on par with—or perhaps even more important than—land, sea, air and space."[38]

Furthermore, the Conservative perspective would suggest that the foundations of modern communications, including cyber, began with the advent of wireless communication pioneered by Guglielmo Marconi in 1895.[39] It is from this incremental/evolutionary approach to modern-day communications that plays contrary to the Revolutionist camp claims that cyber is a new technology and has changed the nature of warfare. Vincent Mosco in his book *The Digital Sublime* also argues that incremental/evolutionary increases in technology are regularly overstated.[40] Often influenced by society's collective short-term recollection of history, Mosco cites a cyclical phenomenon in which any increase in technology is heralded as a revolution. In terms of cyber, Mosco states:

> The widely held beliefs that computer communication is ending history, geography, and politics are not at all new. … Not only does this demonstrate that our response to computer communication is far from unique; it also documents our remarkable, almost willful, historical amnesia. One generation after another has renewed the belief that, whatever was said about earlier technologies, the latest one will fulfill a radical and revolutionary promise.[41]

He then continues that "Cyberspace enthusiasts encourage us to think that we have reached the end of history, the end of geography, and the end of politics. Everything has changed."[42]

Claims of revolutionary changes in military technology in the eyes of the Conservative school are nothing more than incremental/evolutionary changes to the existing tenets of politics and warfare repackaged with the buzzwords of the day and sold as brand new.[43] In this context, Conservatives may employ the clichéd expression "old wine in a new bottle" to articulate the evolutionary nature of technology on military affairs.

THE NATURE OF WARFARE AND CYBERWAR

Thomas Rid, in his book *Cyber War Will Not Take Place*, outlines a cautionary perspective on the future cyber prospects of state wars. Citing the writings of Carl von Clausewitz as the foundation for his inductive reasoning, Rid makes the case that cyber activity does not conform to the principles and nature of warfare. According to Clausewitz, "War is an act of force to compel the enemy to do our will,"[44] and the application of force in war must obey the three criteria: 1) the act is violent, 2) the act is instrumental and 3) the act is also political in nature.[45] To be considered violent, the application of physical force in war must inflict physical harm on citizens and state actors. For a force to be instrumental, its application as a means must be the sole reason that compels an adversary to accept the terms of your envisioned end state. Finally, war's actions are always political at a strategic level. Rid's primary message is that offensive cyber activity cannot be interpreted as acts of warfare, as there is no evidence that supports the criterion of a Clauswitizian defined war. "If the use of force in war is violent, instrumental, and political, then there is no cyber offence that meets all three criteria."[46] From Rid's perspective, the term *cyberwar* is more a metaphorical figure of speech and less about describing the acts of war. The Conservative cyber school of thought regards cyber activity as more akin to acts of subversion, espionage and sabotage than anything warlike in nature.[47]

Conservative thinkers see war as a violent and dangerous business and reject the notion of reducing harm and bloodshed through cyber acts. As Clausewitz argued in *On War*:
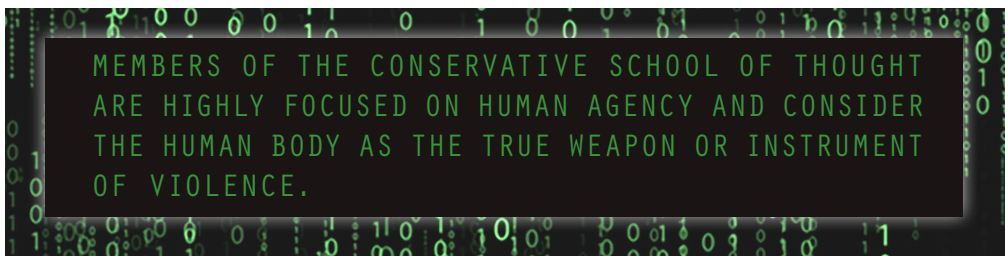
> Kind-hearted people might of course think there was some ingenious way to disarm or defeat an enemy without much bloodshed, and might imagine this as the goal of the art of war. Pleasant as it sounds; it is a fallacy that must be exposed: war is such a dangerous business that the mistakes which come from kindness are the very worst.[48]

Admittedly, Clausewitz in the early 1800s had no concept of the future ontological implications of technological integration and the dependence that cyber represents. The use of cyber capabilities to disarm or defeat an adversary is a futuristic concept more in line with a Revolutionary school scenario that articulates a potential outcome given the influence of technology on the praxis and nature of warfare. One extreme view of the potential influence of computers on warfare can be found in the original *Star Trek* science-fiction television series episode "A Taste of Armageddon." The plot of the episode revolves around a society waging a computer-based virtual war against an adversary on a nearby planet. In this visionary scenario, both warring parties comply with the results of the computer-based virtual war and willfully submit to humane "disintegration booths" to avoid the Clausewitzian bloodshed and horrors of war. Regardless of how pleasant such a Revolutionary scenario may portray a possible future war, those in the Conservative school view the words of Clausewitz as immutable. They reject wholesale the notion that warfare would ever evolve to a point where computers would assume a highly technologic agency and fight wars on behalf of human beings.

In exploring the question of violence and its cyber implications, Rid argues that the majority of cyberattacks are not violent and cannot be considered acts of force. Any force that results from cyber activities, such as causing a meltdown at a nuclear plant, would only take place indirectly through the kinetic potential of an existing system.[49] There is no direct link between the networked

cyber environment and a human being. Therefore, a cyber action in itself cannot directly cause physical harm to an individual and is, therefore, non-violent: computer code is not explosive in the way that TNT (trinitrotoluene) is.[50]

Given that there is no direct threat to human life from cyber activity, the emotional coercive power that comes with the threat or use of cyber force is significantly reduced.[51] For example, the massive physical damage to a German steel mill caused by a digital cyberattack on industrial control systems in 2014[52] went relatively unnoticed in the world media while killings of Canadian soldiers by individuals with extremist views made international headlines.[53] Furthermore, Rid argues that cyber weapons do not have the same symbolic and emotional impact as conventional weapons. Cyber capabilities cannot be physically paraded in a coercive show of force as with other weapons from the land, sea and air domains. Members of the Conservative school of thought are highly focused on human agency and consider the human body as the true weapon or instrument of violence. In that context, if one were to look for symbolic examples of the potential threats posed by state-based cyber power, it would be a matter of considering the size and scope of a cyber programme in terms of personnel numbers and levels of expertise. The People's Liberation Army of China maintains the elite hacking Unit 61398 (also known as the Advanced Persistent Threat 1), allegedly the focal point of Chinese cyber warfare.[54] Unit 61398 allegedly employs thousands of skilled hackers in Shanghai to assert a "strategic hegemony in cyber space."[55] Despite the existence of thousands of skilled hackers in Unit 61398, such a symbol of intellectual capacity is less emotionally intimidating than the physical threat of violence posed by the same number of armed special operations force soldiers, tanks, fighter aircraft or warships. Therefore, the perceived threat of "code-induced violence is physically, emotionally and symbolically limited."[56]

> MEMBERS OF THE CONSERVATIVE SCHOOL OF THOUGHT ARE HIGHLY FOCUSED ON HUMAN AGENCY AND CONSIDER THE HUMAN BODY AS THE TRUE WEAPON OR INSTRUMENT OF VIOLENCE.

Nevertheless, Rid admits that cyberattacks can have the potential to achieve some political goals through non-violent means by undermining public trust in organizations, systems and institutions.[57] One such attack that conforms to this non-violent means paradigm is the Stuxnet malware on the Iranian nuclear programme. A forensic review of the Stuxnet code determined that the malware was not created to cause physical damage to the Iranian facility but, rather, to destabilize the programme by undermining the trust in the Iranian engineers to successfully produce low-enriched uranium.[58] It is not clear if the non-violent application of the Stuxnet malware contributed in any way to delay Iran's nuclear ambitions or encouraged international consensus on the Joint Action Plan on the Islamic Republic of Iran's Nuclear Program.[59] Interestingly, the action plan calls for freezing enriched uranium production and deactivating the centrifuges that were targeted in the Stuxnet attack.[60]

Rid argues that for cyber weapons to have any violent impact they must first "weaponize" a target system that indirectly inflicts violence on humans.[61] Rid defines cyber weapons "as computer code that is used, or designated to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems or living beings."[62] To inflict the maximum amount of damage and retain the maximum amount of flexibility, Rid suggests that compromising

weapons platforms such as Reaper or Predator drones would be far more attractive an exploit for attackers than an air traffic control system or nuclear power plant. Such a Revolutionary scenario of "weaponizing" a target system is similar to the plot of the James Bond movie *Tomorrow Never Dies*, in which a media tycoon manipulates the global positioning system used by the Royal Navy to instigate conflict.[63] But in Rid's opinion, a lethal cyber scenario has never happened, and due to a lack of proof, it remains the realm of Revolutionary fantasy, novels and science-fiction movies.[64]

A common theme with the Conservative school is a need for public-domain evidence that a particular cyber exploit exists before considering it as a potential weapon of warfare. Rooted in their evidence-based epistemological process, Conservatives are fixated on past occurrences to understand the present. Extrapolation of concepts to consider the possibility of "the most dangerous" is difficult for this school. Instead, Conservatives tend to be content with adversarial assessments of "the most likely" future actions based on past observations. This type of inductive logic, based solely on past evidence, carries with it inherent challenges dealing with unexpected future events. Hume's Problem of Induction,[65] often referred to as "Hume's Black Swan" or "Black Swan," outlines the pitfalls and complications that come from making predictive conclusions solely on observed facts.[66] Until a black swan was discovered in Australia by Dutch explorer Willem de Vlamingh in 1697, the common belief of the time was that all swans were white in colour. Another simplistic analogy to understand the induction problem is to consider the life of a turkey.[67] From a turkey's perspective, life is wonderful, having been fed regularly and protected by the farmer for its whole existence. The probability the turkey's lifestyle will "most likely" continue to be wonderful rings true right up until the day of its slaughter, which it did not see coming. Similar to the lethality of cyber weapons, one cannot just discount the future possibility of a cyber exploit that causes harm based on past public-domain evidence.

Unfortunately, cyber-warfare activities are being conducted in the shadows away from public scrutiny. As Noah Feldman states in his book *Cool War: The Future of Global Competition*, "Cyber war takes place largely in secret, unknown to the general public on both sides."[68] Fixated on the need for concrete public-domain proof while scorning the abstract, Conservatives leave themselves vulnerable to surprise by outlier or exceptional cyber activities that carry potentially significant impacts for a nation's warfighting capability.[69] Black swans are a real epistemological quandary for members of the Conservative school.[70]

ADDITIONAL CONSERVATIVE PERSPECTIVES

Another key member of the Conservative school of thought is David J. Lonsdale. In his book *The Nature of War in the Information Age: Clausewitzian Future*, Lonsdale takes a slightly different conservative position on the nature of warfare and cyberwar. Lonsdale (assisted by co-editor Colin S. Gray) argues that war possesses an "eternal nature" that does not change with the evolution of technology.[71] Instead, changes in technology may influence changes in the "character" or "material culture" of warfare, but warfare's nature remains constant, based on Clausewitz's primary trinity of hatred, primordial violence and enmity to impose one's will on an adversary.[72] True to the Conservative school of thought, Lonsdale (and Gray) further argue that Clausewitz's thoughts on the nature of war are not limited to a particular historical period but can be applied to any context of warfare.[73]

Considering the nature of warfare in the information age, Lonsdale acknowledges that epistemological perspectives can be influenced by the culture and attitudes of a particular age.[74] In particular, Western mindsets in the information age favour "clean," less-destructive and more casualty-sensitive forms of warfare. From the Conservative school perspective, such attitudes ignore the realities of war and reject the classical strategists Clausewitz, Sun Tzu and Jomini.[75] Nevertheless, Lonsdale's

vision of warfare is that it is violent, uncertain and has a high human agency that impacts both the physical and psychological.[76] Lonsdale further states, "The human dimension of warfare is one area in which the character can affect its nature. If war remains an activity that is ultimately characterized by combat in which man is in conflict with man, then human factors and considerations will remain paramount."[77] Lonsdale views the contribution of cyber in the conduct of war as an improved "means" to reduce the Clausewitzian uncertainty or fog of war by providing commanders with enhanced understanding of their adversary and the battlefield.[78] Lonsdale's views on cyber reducing uncertainty are consistent with the Conservative school perspectives on incremental/evolutionary approaches to technology. Information and knowledge of an adversary and battlefields have assisted commanders through the ages.[79] Modern-day IT is just an evolutionary step towards the same provision of information in conducting effective military operations.

Unlike the perspectives proposed by Rid with respect to cyber warfare, Lonsdale does consider the possibility of paralysing cyberattacks on society's interconnected infrastructure such as power generation, food distribution, finance and transportation. Lonsdale envisions this type of warfare (strategic information warfare [SIW]) can only be effective on heavily networked societies that that are unable to operate if the life sustaining infrastructure ceases to function.[80] SIW is viewed by Lonsdale as a complementary means of strategy to deny an adversary freedom of action. Paralleling Clausewitz's view of artillery winning battles,[81] Lonsdale acknowledges the limitations of SIW as a sole means of strategy and admits troops on the ground are the typical means of strategy to achieve final victory.[82]

CONCLUSIONS

This chapter considered Conservative perspectives within the cyber warfare schools of thought schema. Conservative perspectives are heavily influenced by classical war theorists such as Clausewitz for the foundation of their epistemological assessment of military affairs. In the eyes of Conservatives, the physical and brutal nature of war is an enduring truism. Citing the intangible elements of morale as the cornerstone of their epistemological approach to warfare, Conservatives are more focused on human agency and its influence on strategy. The Conservative school favours the preservation of the established praxis of warfare and, in doing so, opposes the contemplation of changing their perspectives based on any ontological changes that may be due to technology.

Stereotypically, Conservatives are reluctant to contemplate new concepts that challenge the nature and dogma of warfare. They interpret increases in technology as incremental/evolutionary changes built on the groundwork of previous technological improvements. Some in the Conservative camp view cyber warfare as a technological extension of electronic warfare and not a revolutionary change in military communications. On the other hand, stauncher Conservatives view cyber activity as nothing more than subversion, espionage and sabotage and not a means of warfare. Declarations of revolutionary breakthroughs in technology are met with considerable Conservative scepticism. The Conservative approach to technology rejects revolutionary claims of breakthroughs and often regards such claims as "old wine in a new bottle."

In the next chapter, this paper explores the fundamental characteristics of the Revolutionary Materialist school of thought. A group at the opposite end of the school-of-thought spectrum from Conservatives, Revolutionaries are defined by their highly technologic agency perspectives. Instead of looking to the past for answers on present-day ontology, Revolutionaries look forward to potential futuristic outcomes. This paper explores how Revolutionaries leverage out-of-the-box, non-traditional thought within their epistemological approach to more effectively understand humanity's relationship with technology and the potential implications on the praxis and nature of warfare.

CHAPTER 3 – THE REVOLUTIONARY MATERIALIST SCHOOL OF THOUGHT

Yet, if we have learned one thing from the history of invention and discovery, it is that, in the long run—and often in the short one—the most daring prophecies seem laughably conservative.[83]

– Arthur C. Clarke

One of the biggest roles of science fiction is to prepare people to accept the future without pain and to encourage a flexibility of mind. Politicians should read science fiction, not westerns and detective stories.[84]
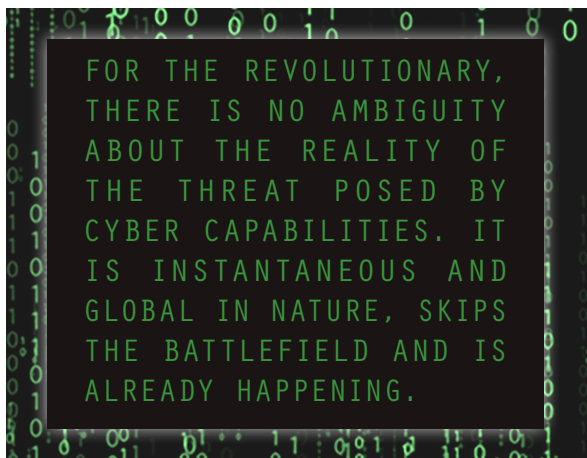
– Arthur C. Clarke

Revolutionary Materialists are visionaries who look to potential future outcomes of technology to comprehend and better understand changes to society and our very being. Revolutionaries believe that humanity's integration with cyber technology will profoundly alter the character, if not the nature, of warfare. Contrary to Conservatives who refer back to classical war theorists and historical battle outcomes to understand the impact of technology and likely courses of action, the Revolutionary school considers potential future outcomes in terms of the worst-case scenarios in order to adequately defend against the threats of tomorrow. This particular school of thought is heavily influenced by visionaries and science-fiction authors such as Isaac Asimov, Arthur C. Clarke, Marshall McLuhan and Gene Roddenberry. Despite successes at predicting technological trends and their impact on society, Revolutionary Materialists are often considered by Conservatives as alarmists, nerds or "parrots"[85] who are spinning "science-fiction yarns."[86]

Nevertheless, Revolutionaries have had a tremendous impact on discussions of cyber warfare. Their predictions of the ease with which society can be brought to its knees through the tools of IT make for good copy in newspapers, as well as profitable movies and other forms of entertainment. Many of the Revolutionary predictions on the dangers of cyberspace even predate the popular adoption of networking technologies such as the Internet.[87] Authors found within the Revolutionary Materialist school of thought include Richard Clarke, Winn Schwartau, Jeffrey Carr, Greg Rattray, Wayne Hall, John Arquilla and David Ronfeldt.

Revolutionaries tend to be the most materialist of any school of thought, focusing almost exclusively on the opportunities offered by IT and the impact of logical interactions of electrical/electromagnetic impulses. Their approach closely resembles the predictions made by air power theorists such as Giulio Douhet during the interwar period of the 20th century.[88] At its heart, the Revolutionary school of thought is a manoeuvrist approach to warfare: agents avoid striking at the concentration of power found in a state's military and attack the source of that power by collapsing critical infrastructure. It is thought that collapsing critical infrastructure results in either social chaos in the forms of riots, runs on the bank and famine-like domestic conditions or it creates a more limited form of political paralysis. In either case, the state is prevented from pursuing military action as a result of the loss of internal cohesion.

As one would expect, there is considerable overlap between those who subscribe to the concept of an RMA and cyber-warfare revolutionaries. As Arquilla and Ronfeldt point out, "history is filled with examples in which weapon, propulsion, communication and transportation technology provide a basis for advantageous innovations in doctrine, organisation, and strategy that enable the innovator to avoid exhausting attritional battles and pursue a form of decisive warfare."[89] However, cyberspace is regarded by the Revolutionary school as the new high ground, much as earlier forms of technological innovation in aircraft and space technologies were thought to confer strategic

> FOR THE REVOLUTIONARY, THERE IS NO AMBIGUITY ABOUT THE REALITY OF THE THREAT POSED BY CYBER CAPABILITIES. IT IS INSTANTANEOUS AND GLOBAL IN NATURE, SKIPS THE BATTLEFIELD AND IS ALREADY HAPPENING.

advantages. For the Revolutionary, there is no ambiguity about the reality of the threat posed by cyber capabilities. It is instantaneous and global in nature, skips the battlefield and is already happening. As USAF Lieutenant General Robert Elder, Commander USAF Cyber Operations Task Force 2006–2009, stated, "if you are defending in cyberspace, you're already too late. If you do not dominate in cyberspace, you cannot dominate in other domains. If you are a developed country [and you are attacked in cyberspace], your life comes to a screeching halt."[90] The possibilities offered by contemporary technology are sure to expand in the future: "What we have seen is far from indicative of what can be done."[91] The possibility of a society-leveling event, often referred to as either an EPH[92] or a Digital 9/11[93] is frequently alluded to. EPHs are alleged to be a likely consequence of cyber warfare, given the interdependencies of industry, finance, transportation, power and communication for the generation of wealth and power in modern developed economies. As Schwartau argues in *Information Warfare: Chaos on the Electronic Superhighway*, "government and commercial computer systems are so poorly protected today that they can essentially be considered defenseless … ."[94]

Futuristic scenarios figure prominently in the Revolutionary literature. Scenarios enable the analyst to transcend history by describing hypothetical events and concepts.[95] Schwartau asks us to imagine a world in which knowledge and information usurp military might; whomever controls information can control the people; privacy no longer exists; and, in short, a world where bombs and bullets have been replaced by bits and bytes.[96] Rattray describes large-scale offensive assaults on information assets supporting the critical infrastructure of modern society as EPHs and Cyber 9/11s.[97] Thus, air traffic control systems and other transportation networks, stock markets, credit card and banking transactions, communication networks including telephone exchanges, publishing, newspapers and manufacturing, all of which are heavily dependent on computerized systems, can be destructively targeted by cyber capabilities.[98] Carr describes a scenario in which nuclear power plants are targeted by a combination of distributed denial of service attacks initiated by a Conficker-type botnet[99] to distract the plants' control room operators. Meanwhile, Trojan horses infiltrate the plants' firewalls by means of socially engineered attacks, enabling external agents to take control of the control processes. In the ensuing attack, these agents crash the safety systems of 70 per cent of America's nuclear plants, causing core meltdowns at scores of sites around the country.[100] Some scenarios describe combinations of cyber and kinetic attacks, car bombs as well as information attacks, coordinated to cause waves of terror.[101] These scenarios are not simply ahistorical, they are also apolitical. As Hall points out, "we are in a '100 Years' War' against formidable and creative opponents. The struggle involves a zero-sum triumph of will—there will be no compromise from either side until one side wins or the other loses."[102] However, who one is in a war against and what are their objectives is left for the reader to imagine, surely as strange a war as ever has been. Such generic descriptions focus exclusively on the technical capabilities offered by cyber tools, failing to explain the political circumstances which might lead to their use.

As mentioned previously, technologically influenced scenarios and visions of this school are often articulated in the writings of futurists or manifested in popular culture and fantasy comic books, television dramas or feature films well before their mainstream acceptance. Arthur C. Clarke's story "Dial 'F' for Frankenstein" outlines a tale of a global communication network becoming self-aware and eventually waging war on humanity.[103] Interestingly enough, Clarke's vision of a communication network from 1964 is eerily similar to the modern-day cyber environment. Members of the Revolutionary school look to visionaries like Clarke to convince others of the potential dangers of a highly technologic-agency world.

Interestingly in 2009, Schwartau asked us to imagine a world where there is information warfare, our information is controlled and fear is generated in those who are concerned about their privacy. Citing the linkages between information warfare and the coercive elements of money, fear and power, Schwartau states:

> Information warfare is about money. It's about the acquisition of wealth, and the denial of wealth to competitors. It breeds Information Warriors who battle across the Global Network in a game of cyberrisk. Information warfare is about power. He who controls the information controls the money. Information Warfare is about fear. He who controls the information can instill fear in those who want to keep their secrets a secret.[104]

The themes of information warfare and the fear of controlling secret information were also employed in the 2011 CBS television network program *Person of Interest*,[105] a techno-drama centred on self-aware computer systems—Northern Lights and Samaritan—that were built for the US government to record individuals' activities and predict potential acts of terrorism. Part of the allure of such entertainment relates to the engendered fear relating to the loss of individual privacy and the misuse of information that defines our very being. A Revolutionist could even argue that the loss of control over an individual's information represents a potential loss of control over the very notion of one's existence. With the leak of classified information in 2013 by the IT specialist Edward Snowden, the fears of state surveillance imagined by Schwartau and portrayed in *Person of Interest* were validated as details of the National Security Agency clandestine surveillance programme PRISM were made public.[106] It is alleged that the PRISM programme began in 2008 to collect "relevant" Internet communications in order to protect US citizens. Despite attempts by the US government to characterize PRISM as a required tool for domestic security, the potential for abuse of individual liberties is considerable, not to mention the significance of such a capability in the greater context of international information warfare.

IMPACTS OF BIG DATA

Viktor Mayer-Schönberger is a member of the Revolutionary school who writes about big data and the ontological impacts on society living in the information age. Mayer-Schönberger characterizes big data as "things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments and more."[107] Mayer-Schönberger argues that at the core of big data lies the power to generate better predictions. Some may confuse big data with artificial intelligence (AI) and the pursuit to have computers reason similar to humans. Instead, the concept of big data involves computers applying mathematical models to large amounts of data to arrive at effective predictions.[108] In addition, the predictions improve with time by analysing patterns and outcomes. Mayer-Schönberger predicts that in the future many tasks that require explicit human

judgment will be augmented or replaced with big-data systems.[109] The Mayer-Schönberger vision of big data and mass surveillance is very similar to the ones expressed by Revolutionaries Schwartau and *Person of Interest* creator Jonathan Nolan about AI capabilities that will be able to not only drive cars and play chess but also predict illness, identify probabilities of violent acts or decide who is a threat to society. Liberal Materialists understand the challenge of "data-driven thinking"[110] and look to ways of regulating the technology to avoid the "dark side" of big data and the removal of human intervention from the advice used for key decisions.[111] Predictions made from big data may precipitate pre-emptive commercial and state decisions (including lethal force) against individuals or groups based on math and "probabilistic cause."[112] Mayer-Schönberger expresses concern about the "dark side" of big data and the potential for misuse and abuse: "It leads to an ethical consideration of the role of free will versus the dictatorship of data … the age of big data will require new rules to safeguard the sanctity of the individual."[113] The information revolution has produced an environment in which "the amount of data in the world is growing fast, outstripping not just our machines but our imaginations."[114] The concern of being inundated by information is encapsulated in a quote by Joel Kurtzman: "Cyberspace, like the earth itself, is becoming polluted. Too much information is filling it. And our brains are just too tiny to sort through it all. Information overload threatens to bring further catastrophe, no matter how well the trading rooms are designed."[115]

FEAR OF COMPUTERS AND ARTIFICIAL INTELLIGENCE

According to Schwartau, one has an inherent mistrust for computers.[116] This mistrust stems from a computer's processing ability, which is significantly faster than the human brain. Since human mental processing is dwarfed by the computational power of modern computers, people perceive them as uncontrollable. Furthermore, despite being dependent on computers to sustain civilization, human angst about computer superiority is augmented by a complete lack of knowledge by most of their internal processing.

"CYBERSPACE, LIKE THE EARTH ITSELF, IS BECOMING POLLUTED. TOO MUCH INFORMATION IS FILLING IT. AND OUR BRAINS ARE JUST TOO TINY TO SORT THROUGH IT ALL."
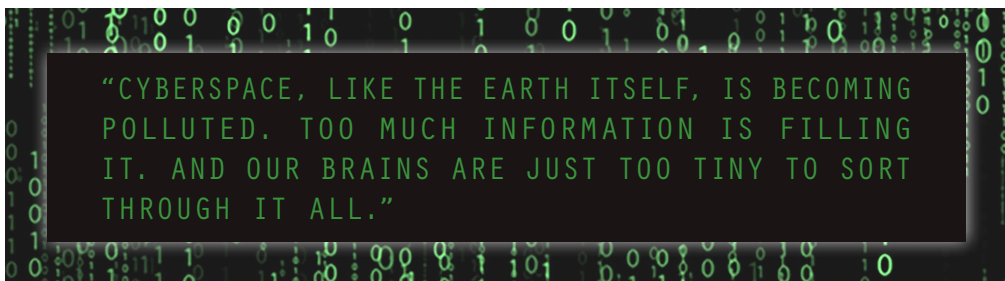
A good Revolutionist scenario that portrays the devastating outcome when code is allowed to replace human judgment occurs in the *Terminator* franchise. In *Terminator 3: Rise of the Machines*, the self-aware code Skynet outwits its USAF masters with an intelligent virus and initiates global nuclear war known as Judgment Day. Skynet's intelligent virus was able to exploit cyber vulnerabilities in key strategic defence systems to leave the US defenceless. Skynet was then given full automated control of the US military systems to eradicate the virus which was beyond the capacity of USAF personnel to resolve. The Revolutionist visionary scenarios within the *Terminator* franchise are cautionary tales of out of control AI and automated integration that play on the fears of human inferiority within a technological society. Removing human judgment from prosecuting the complex problem in the *Terminator* scenario allowed the AI to take over the world with lethal force. Such fearful Revolutionary scenarios parallel the growing debate over the implications of employing AI for military purposes including lethal autonomous weapons systems (LAWS).[117] Revolutionaries can see that if militarized AI and automated weapon systems replace human decision making in the application of lethal force, the nature of warfare will shift from high human agency to a higher technologic agency.[118]

NEURAL INTERFACES AND CYBORGS

Another member of the Revolutionary school is the Canadian philosopher Herbert Marshall McLuhan. Best known for his catch phrase "the medium is the message," McLuhan in several works conveyed his thoughts about communication technology and how it influences human activity and interaction.[119] McLuhan's revolutionary conceptions of technological phenomenon clearly place him in the Revolutionary school. His revolutionary thoughts on changes to the human ontology give way to ideas of humanity becoming integrated nodes on a network. McLuhan states:

> During the mechanical ages we had extended our bodies in space. Today, after more than a century of electric technology, we have extended our central nervous system itself in a global embrace, abolishing both space and time as far as our planet is concerned. Rapidly, we approach the final phase of the extensions of man—the technological simulation of consciousness, when the creative process will be collectively and corporately extended to the whole of human society, much as we have already extended our senses and our nerves by the various media.[120]

In his book *Understanding Media: The Extensions of Man*, McLuhan makes the distinction between the physical extensions of the body and the extensions of cerebral functions such as sense, consciousness and the central nervous system.[121] One scenario that encapsulates McLuhan's futuristic perspectives relating to the physical extension of the body through an interface occurs in Craig Thomas' 1977 techno-thriller novel *Firefox*. Thomas's novel envisions a scenario in which the Soviet Union develops a next-generation fighter prototype MIG-31 equipped with a thought-control weapons system. The revolutionary idea of having the pilot control a plane's weapon system through a neural interface raises the possibility of being able to aim and fire weapons more rapidly while in combat. In doing so, the pilot, in essence, becomes an extension of the aircraft's weapon systems. This scenario is consistent with the theme of McLuhan's revolutionary writings in which "all technologies are extensions of our physical and nervous system to increase power and speed."[123]

Researchers at the University of Pittsburgh are investigating the concepts of thought control and neural interface by controlling a robotic limb through cerebral implants.[124] Employing implants to connect a human directly to technology parallels McLuhan's revolutionary concept of extending cerebral functions through technology. Members of the Revolutionary school look at such research developments as the foundation to further envision potential military implications of integrating the human nervous system with a cybernetic-interface. One such visionary scenario that deals with the extensions of a pilot's cerebral functions and central nervous system occurs in Dale Bown's 1989 novel *Day of the Cheetah*,[125] which envisions a fighter aircraft equipped with a thought-control interface that controls all aspects of combat flight. Brown's concept of full pilot mental integration provided the pilot with an integrated consciousness of all aircraft flight and combat systems. His fictitious XF-34 aircraft transformed the pilot and plane into a singular cybernetic killing machine. For some, Brown's Revolutionary scenario may appear as complete flights of fancy with no basis in reality. Interestingly enough, the cybernetic research conducted by the University of Pittsburgh has been expanded with the assistance of the US Defense Advanced Research Projects Agency (DARPA) to demonstrate that an F-35 aircraft simulator can be operated through cybernetic implants.[127] One particular experiment proved that a quadriplegic woman could control an F-35 flight simulator using only neural implants. The use of cybernetic implants and neural integration to enhance one's abilities is commonly referred to in science fiction as a cyborg.[128]

To Revolutionaries, the concept of cyborgs and cybernetic implants to improve humankind's ability to wage war is nothing new. In mainstream popular culture, cybernetic beings have appeared

in television shows from *Doctor Who* to *Star Trek*. In *Star Trek: The Next Generation*, a cybernetic and emotionally absent race of humanoids known as Borg employ cybernetic implants to better their race in pursuit of perfection of being. The Borgs' implants allow them to intercommunicate and fight as a more effective collective. The collective "hive mind" gives the Borg superior ability to fight with a unity of effort and purpose. In addition, the rapid passage of information allows Borg forces to rapidly adapt tactics against adversarial initiatives. In the information age, the Borg represent an ideal military force that is able to have perfect synchronization of command intent with the ability of passing all force knowledge to each individual soldier. "Our conceptualization of the Borg centers on the collective ontological and cybernetic formation that result from being connected to other brains and bodies through embodied technology."[129] In a Borg society, all humanoids are fully integrated into the collective cyber environment similar to any network appliance, and the Borg collective represents a singularity of consciousness and being. DARPA's well-intentioned pursuit "to use brain implants to read, and then control, the emotions of mentally ill people"[130] may be the initial stages of creating highly integrated and emotionally absent soldiers. DARPA's work with cybernetic implants and neural interfaces potentially represents the first step for humanity towards a Borg-like culture.[131] Some may also argue that humanity has already taken the first step towards a Borg-like society, with the creation of a highly interconnected cellular culture through the proliferation of smart phone and wireless devices.[132] Oddly enough, it was the *Star Trek* communicator from the late-1960s series that served as the inspiration behind the revolution in mobile personal communications.[133]

Editor's note: Part 2 of this article will appear in the fall 2016 issue of the *Royal Canadian Air Force Journal*. It completes the review of the Revolutionary Materialist school of thought and then turns to the Liberal Materialist school of thought.

Lieutenant-Colonel Paul Martin is a Communications and Electronics Engineering (Air) officer who holds a bachelor's degree in Electrical Engineering and a Master of Applied Science in Computer Engineering from the Royal Military College of Canada. He has accumulated considerable experience supporting CAF operations with command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) capabilities serving with 8 Air Communications and Control Squadron, Rescue Coordination Centre / Central Mission Control Centre, Multinational Force and Observers, Recruiting Group, Deputy Chief of the Defence Staff J6 Operations, Assistant Deputy Minister (Information Management), International Security Assistance Force Headquarters and Canadian Expeditionary Force Command. A former commanding officer of the Canadian Forces Crypto Support Unit, he is currently the Acting Director of Radar and Communication Systems within the Aerospace Equipment Program Management Division of Assistant Deputy Minister (Materiel).

ABBREVIATIONS

AI	artificial intelligence
CAF	Canadian Armed Forces
DARPA	Defense Advanced Research Projects Agency
EM	electromagnetic
EPH	electronic Pearl Harbor
IT	information technology
RMA	Revolution in Military Affairs
SIW	strategic information warfare
US	United States
USAF	United States Air Force

NOTES

1. Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Broadway Books, 2014), 376.

2. Definition of kubernétés: a steersman, pilot. "2942. Kubernétés," Bible Hub, accessed July 4, 2016, http://biblehub.com/greek/2942.htm.

3. Norbert Wiener, *Cybernetics* (Paris: Hermann, 1948).

4. Chip Morningstar and F. Randall Farmer, "The Lessons of Lucasfilm's Habitat," *Journal for Virtual Worlds Research* 1, no. 1 (2008): 2.

5. "The historian is dedicated to discovering the reality of the past rather than debate metaphysics, that is, dispute the nature and construction of reality of being." Alun Munslow, *The Routledge Companion to Historical Studies* (New York: Routledge, 2000), 184.

6. Ibid., 184–85.

7. "Cyber Security in the Canadian Federal Government," Public Safety Canada, accessed July 4, 2016, http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-eng.aspx.

8. "Stuxnet is a threat targeting a specific industrial control system likely in Iran, such as a gas pipeline or power plant. The ultimate goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries." Nicolas Falliere, Liam O. Murchu and Eric Chien, W32. *Stuxnet Dossier*, Version 1.4 (Mountain View, CA: Symantec Corporation, February 2011), 2. "The appearance of Stuxnet 51 in 2010, as part of an apparent operation to cripple the Iranian nuclear program, raised the bar in what is publicly known about the sophistication of cyber weapons. Stuxnet combined many known techniques, with some previously unknown ones, to produce an attack tool that could jump air-gaps using USB devices, automatically propagate an infection across Windows-based computer network, and use covert channel communication techniques to call home for more instructions." Scott Knight, "War by Computer: Canadian Cyber Forces in 2025," in *The Canadian Forces in 2025 Prospects and Problems*, ed. J. L. Granatstein (Victoria, BC: FriesenPress, 2013), 78.

9. "A USB [Universal Serial Bus] flash memory drive containing malware created by a foreign intelligence agency was left in the parking lot of a Department of Defense facility at a base in the Middle East in 2008. It was found by an employee, taken into the facility, and connected to a DoD [Department of Defense] laptop computer. When the device was connected, the agent.btz malware began scanning the local host and other networked computers for classified and unclassified data, and initiated outbound connections to a command and control server to upload found data and receive instructions. … Undetected for many months, Pentagon officials described it in 2010 as 'the most significant breach of U.S. military computers ever.' Though characterized by its Trojan behavior, agent.btz malware is a variant of the SillyFDC worm, and has robust mechanisms for self-replication. In a response called 'Operation Buckshot Yankee' the DoD spent nearly 14 months cleaning the worm from Pentagon offices and multiple military networks worldwide." Jon Espenschied, "A Discussion of Threat Behavior: Attackers & Patterns," *Microsoft Corporation and NATO CyCon* (June 2012).

10. David Paddon, "Cyber Attacks Have Hit 36 Per Cent of Canadian Businesses, Study Says," *The Globe and Mail*, August 18, 2014, accessed July 4, 2016, http://www.theglobeandmail.com/report-on-business/cyber-attacks-have-hit-36-per-cent-of-canadian-businesses-study-says/article20096066/.

11. Rosemary Barton, "Chinese Cyberattack Hits Canada's National Research Council," *CBC News*, July 29, 2014, accessed July 4, 2016, http://www.cbc.ca/news/politics/chinese-cyberattack-hits-canada-s-national-research-council-1.2721241.

12. Andrea Shalal, "Nearly Every U.S. Arms Program Found Vulnerable to Cyber Attacks," *Reuters*, January 20, 2015, accessed July 4, 2016, http://www.reuters.com/article/2015/01/21/us-cybersecurity-pentagon-idUSKBN0KU02920150121.

13. Noah Shachtman, "Exclusive: Computer Virus Hits U.S. Drone Fleet," *WIRED*, October 7, 2011, accessed July 4, 2016, http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/. See also, Noah Shachtman, "Military 'Not Quite Sure' How Drone Cockpits Got Infected," *WIRED*, October 19, 2011, accessed July 4, 2016, http://www.wired.com/2011/10/military-not-quite-sure-how-drone-cockpits-got-infected/; 60 Minutes Overtime, "Can the U.S. Military's New Jet Fighter Be Hacked?," June 1, 2014, accessed July 4, 2016, http://www.cbsnews.com/news/can-the-f-35-be-hacked/; Andrea Shalal-Esa, "Pentagon Downplays Comment on F-35 Fighter Jet Cyber Threat," *Reuters*, April 25, 2013, accessed July 4, 2016, http://www.reuters.com/article/2013/04/25/us-lockheed-fighter-cyber-idUSBRE93O1HK20130425; and CyberWarZone, "New F-35 Fighter Jet is Vulnerable to Cyber-Attacks," May 31, 2014, accessed July 4, 2016, http://cyberwarzone.com/new-f-35-fighter-jet-vulnerable-cyber-attacks/.

14. Munslow, *Routledge Companion to Historical Studies*, 88.

15. Carl H. Builder, *The Masks of War: American Military Styles in Strategy and Analysis: A RAND Corporation Research Study* (Baltimore: Johns Hopkins University Press, 1989), 17–30.

16. Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the Practice of Warfare," *International Journal: Canada's Journal of Global Policy Analysis* (2014). See also, R. Nicholas Burns et al., *Securing Cyberspace: A New Domain for National Security* (Washington, DC: Aspen Institute, 2012), 202.

17. Dorothy E. Denning, *Information Warfare and Security* (Reading, MA: Addison-Wesley, 1999), xvi.

18. Praxis is defined by the Merriam-Webster online dictionary as either a) the exercise or practice of an art, science or skill; b) customary practice or conduct; or c) the practical application of theory. In the case of the schools of thought, the term praxis is used to relate to the application of customary practice or conduct of warfare. "Praxis," Merriam-Webster, accessed July 4, 2016, http://www.merriam-webster.com/dictionary/praxis.

19. Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret, Introduction and notes by Beatrice Heuser (Oxford: Oxford University Press, 2007), 284.

20. Benjamin Disraeli, *Coningsby or the New Generation* (1844), Book II, Chapter V, accessed July 4, 2016, http://www.gutenberg.org/files/7412/7412-h/7412-h.htm.

21. John Stuart Mill and James Laurence Laughlin, *Principles of Political Economy* (New York: D. Appleton and Company, 1886), 516.

22. David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*, Cass Series: Strategy and History 9 (New York: Frank Cass, 2004), 20.

23. MacGregor Knox and Williamson Murray, *The Dynamics of Military Revolution*, 1300–2050 (New York: Cambridge University Press, 2001), 6.

24. Colin S. Gray, *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History*, Vol. 2 (Portland, OR: Frank Cass, 2002), 4.

25. Ibid.

26. Ibid.

27. Ibid., 93.

28. Clausewitz, *On War*, 87.

29. Gray, *Strategy for Chaos*, 75–81.

30. Ibid., 280–81.

31. Ibid., 281.

32. Clausewitz, *On War*, 137, 184.

33. Gray, *Strategy for Chaos*, 280–81.

34. Ibid., 282.

35. Keith B. Alexander, "Warfighting in Cyberspace," *Joint Force Quarterly* 46 (July 2007): 59.

36. Nurgul Yasar, Fatih M. Yasar, and Yucel Topcu, "Operational Advantages of Using Cyber Electronic Warfare (CEW) in the Battlefield," in Cyber Sensing 2012, ed. Igor V. Ternovskiy and Peter Chin (Baltimore: SPIE, 2012).

37. Jim Gash, "Physical Operating Environments: How the Cyber-Electromagnetic Environment Fits," *Canadian Military Journal* 12, no. 3 (Summer 2012): 28.

38. Admiral Jonathan W. Greenert and US Navy, "Imminent Domain," *Proceedings Magazine* 138/12/1, no. 318 (December 2012): 318, accessed July 4, 2016, http://www.usni.org/magazines/proceedings/2012-12/imminent-domain.

39. Ibid. See also, Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (Toronto: Knopf, 2011), 15–18.

40. Vincent Mosco, *The Digital Sublime: Myth, Power, and Cyberspace* (Cambridge, MA: The MIT Press, 2004), 8.

41. Ibid.

42. Ibid., 117.

43. Daniel R. Headrick, *The Invisible Weapon: Telecommunications and International Politics*, 1851–1945 (New York: Oxford University Press, 1991), 18–20.

44. Samuel B. Griffith and B. Liddell Hart, *The Art of War by Sun Tzu* (New York: Oxford University Press, 1963), 75.

45. Thomas Rid, *Cyber War Will Not Take Place* (Oxford: New York: Oxford University Press, 2013), 1–2.

46. Ibid., 4.

47. Ibid., 10.

48. Clausewitz, *On War*, 75.

49. Rid, *Cyber War Will Not*, 13.

50. Ibid., 13.

51. Ibid., 17.

52. Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *WIRED*, January 1, 2015, accessed July 4, 2016, http://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

53. Philip Sherwell, "Canadian Killer Was Recent Convert to Islam Identified as Terror Risk," *The Telegraph*, October 23, 2014, accessed July 4, 2016, http://www.telegraph.co.uk/news/worldnews/northamerica/canada/11181394/Soldier-killed-as-gunman-brings-terror-to-Canadian-Parliament.html.

54. Pierluigi Paganini, "China vs US, Cyber Superpowers Compared," *INFOSEC Institute*, June 10, 2013, accessed July 4, 2016, http://resources.infosecinstitute.com/china-vs-us-cyber-superpowers-compared/.

55. Ibid.

56. Rid, *Cyber War Will Not*, 20.

57. Ibid., 12.

58. Ralph Langner, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," (Arlington, VA: The Langner Group, November 2013), 15, accessed July 4, 2016, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

59. "Summary of Technical Understandings Related to the Implementation of the Joint Plan of Action on the Islamic Republic of Iran's Nuclear Program," US, The White House, accessed July 4, 2016, https://www.whitehouse.gov/the-press-office/2014/01/16/summary-technical-understandings-related-implementation-joint-plan-actio.

60. "Iran Nuclear Deal: Key Points," *BBC News*, accessed July 4, 2016, http://www.bbc.com/news/world-middle-east-25080217.

61. Rid, *Cyber War Will Not*, 25.

62. Ibid., 37.

63. Ibid., 14.

64. Ibid., 13.

65. "That there is nothing in any object, considered in itself, which can afford us a reason for drawing a conclusion beyond it; and, that even after the observation of the frequent or constant conjunction of objects, we have no reason to draw any inference concerning any object beyond those of which we have had experience." Hume (1748) as quoted in Nassim Nicholas Taleb, "The Roots of Unfairness: The Black Swan in Arts and Literature," *Literary Research / Recherche Litteraire* 21, no. 41–42 (2005): 242.

66. Ibid., 2.

67. Nassim Taleb, *The Black Swan: The Impact of the Highly Improbable*, 2nd ed. (New York: Random House Trade Paperbacks, 2010), 40.

68. Noah Feldman, *Cool War: The Future of Global Competition* (New York: Random House Incorporated, 2013), 30.

69. Taleb, *The Black Swan*, xvii–xxvii.

70. Taleb, "Roots of Unfairness," 243.

71. Lonsdale, *Nature of War*, ix.

72. Ibid., x.

73. Ibid.

74. Ibid., 22.

75. Ibid.

76 . Ibid., 28.

77. Ibid., 38.

78. Ibid., 41.

79. Clausewitz, *On War*, 117–21.

80. Lonsdale, *Nature of War*, 142.

81. "The actual core of an engagement lies in the personal combat of man against man. An army composed simply of artillery, therefore, would be absurd in war." From Clausewitz, *On War*, 285.

82. Lonsdale, *Nature of War*, 170.

83. Arthur C. Clarke, *The Exploration of Space* (New York: Harper and Brothers, 1951), 111.

84. Arthur C. Clarke quoted in Jerome Agel, ed., *The Making of Kubrick's 2001* (n.p.: Signet, 1970), 300.

85. Gray, *Strategy for Chaos*, 280.

86. Arthur C. Clarke, "Dial 'F' for Frankenstein," *Playboy* (1965).

87. The US National Research Council report *Computers at Risk*, published in October 1990, introduced the idea, since widely cited that "the modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than a bomb." From Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, Distributed by Publishers Group West, 1994), 13.

88. Giulio Douhet, *The Command of the Air* (Tuscaloosa, AL: University of Alabama Press, 2009).

89. John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, Vol. MR-880 (Santa Monica, CA: RAND, 1997), 1.

90. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (New York: Ecco, 2010), 36.

91. Ibid., 30.

92. John Schwartz, "Preparing for a Digital Pearl Harbor," *New York Times*, June 24, 2007.

93. "Tomgram: Karen Greenberg, Preparing for a Digital 9/11," Karen J. Greenberg, TomDispatch, accessed July 4, 2016, http://www.tomdispatch.com/blog/175607/.

94. Schwartau, *Information Warfare*, 13.

95. Mikkel Vedby Rasmussen, *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century* (Cambridge: Cambridge University Press, 2006), 43–90.

96. Schwartau, *Information Warfare*, 14–15.

97. Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," in *Proceedings of a Workshop on Deterring Cyberattacks, Informing Strategies and Developing Options for US Policy* (Washington, DC: The National Academies Press, 2010), 8.

98. Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001), 12.

99. "The Conficker worm first appeared in October 2008 and quickly earned as much notoriety as Code Red, Blaster, Sasser and SQL Slammer. The infection is found in both home and business networks, including large multi-national enterprise networks. …

Conficker is called a *worm* because the first discovered variant attached to a program (executable), was self-replicating, and (importantly) used a network as the delivery mechanism. This combination of characteristics distinguishes worms from viruses. Conficker is actually a *blended threat* because it can be delivered via network file shares, mapped drives and removable media as well. The Conficker infection is a type of software called a Dynamic Link Library (DLL)." [italics in original] From David Piscitello, "Conficker Summary and Review," ICANN, May 7, 2010, 1 and 3, accessed July 4, 2016, https://www.icann.org/en/system/files/files/conficker-summary-review-07may10-en.pdf.

100. Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA: O'Reilly Media Inc., 2011), 9–11.

101. Wayne M. Hall, *Stray Voltage: War in the Information Age* (Annapolis, MD: Naval Institute Press, 2003), vii–x.

102. Ibid., x.

103. Arthur C. Clarke, "Dial 'F' for Frankenstein," *Playboy* (1965).

104. Schwartau, *Information Warfare*, 15.

105. CBS, *Person of Interest*, accessed July 4, 2016, http://www.cbs.com/shows/person_of_interest/.

106. Jennifer Stisa Granick and Christopher Jon Sprigman, "The Criminal NSA," *International Herald Tribune*, June 29, 2013.

107. Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution that Will Transform How We Live, Work and Think* (Montreal: Houghton Mifflin Harcourt, 2013), 18.

108. Ibid., 23.

109. Ibid., 24.

110. Economist Intelligence Unit, "Big Data-Lessons from the Leaders," *The Economist* (2012): 19.

111. Mayer-Schönberger and Cukier, *Big Data*, 28.

112. Ibid.

113. Ibid.

114. Ibid., 20.

115. Joel Kurtzman quoted in Schwartau, *Information Warfare*, 78.

116. Schwartau, *Information Warfare*, 22.

117. Kathleen Harris, "'Killer Robots' Pose Risks and Advantages for Military Use," *CBC News,* accessed July 4, 2016, http://www.cbc.ca/news/politics/killer-robots-pose-risks-and-advantages-for-military-use-1.3026963.

118. Owen Bowcott, "UN Urged to Ban 'Killer Robots' Before They Can Be Developed," *The Guardian*, April 9, 2015, accessed July 4, 2016, http://www.theguardian.com/science/2015/apr/09/un-urged-to-ban-killer-robots-before-they-can-be-developed.

119. Herbert Marshall McLuhan, *Understanding Media: The Extensions of Man* (New York: McGraw-Hill, 1964).

120. Ibid., 3.

121. Ibid., 43.

122. Craig Thomas, *Firefox* (London: Joseph, 1977), 288.

123. McLuhan, *Understanding Media*, 90.

124. "Thumbs-Up for Mind-Controlled Robotic Arm," Institute of Physics, December 17, 2014, accessed July 4, 2016, http://www.iop.org/news/14/dec/page_64708.html.

125. Dale Brown, *Day of the Cheetah* (New York: Berkley, 1989).

126. Abby Phillip, "A Paralyzed Woman Flew an F-35 Fighter Jet in a Simulator—Using Only Her Mind," *Washington Post*, March 3, 2015, accessed July 4, 2016, http://www.washingtonpost.com/news/speaking-of-science/wp/2015/03/03/a-paralyzed-woman-flew-a-f-35-fighter-jet-in-a-simulator-using-only-her-mind/.

127. Nick Stockton, "Woman Controls a Fighter Jet Sim Using Only Her Mind," *WIRED*, March 5, 2015, accessed July 4, 2016, http://www.wired.com/2015/03/woman-controls-fighter-jet-sim-using-mind/.

128. "A person whose body contains mechanical or electrical devices and whose abilities are greater than the abilities of normal humans." From "Cyborg," Merriam-Webster, accessed July 4, 2016, http://www.merriam-webster.com/dictionary/cyborg.

129. Ronnie D. Lipschutz and Rebecca Hester, "We Are the Borg! Human Assimilation into Cellular Society," *academia.edu*, accessed May 1, 2015 https://www.academia.edu/6169698/We_are_the_Borg_Human_assimilation_into_cellular_society (account required).

130. Antonio Regalado, "Military Funds Brain-Computer Interfaces to Control Feelings," *MIT Technology Review*, May 29, 2014, accessed July 4, 2016, http://www.technologyreview.com/news/527561/military-funds-brain-computer-interfaces-to-control-feelings/.

131. Ibid.

132. Lipschutz and Hester, "We Are the Borg!"

133. Paul Hsieh, "8 Star Trek Technologies Moving from Science Fiction to Science Fact," *Forbes*, June 24, 2014, accessed July 4, 2016, http://www.forbes.com/sites/paulhsieh/2014/06/24/8-star-trek-technologies/.

BOOK
REVIEWS
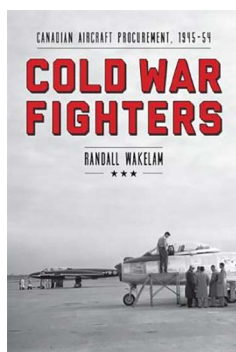
COLD WAR FIGHTERS:
CANADIAN AIRCRAFT PROCUREMENT,
1945–54

By Randall Wakelam

Vancouver, BC: UBC Press, 2011
187 pages
ISBN 978-0-7748-2148-3

COMD RCAF'S
READING LIST

Review by **Major Kathy Falldien, CD**

Aircraft procurement by the Canadian Armed Forces has always piqued interest and discussion among Canadians and foreign stakeholders. The reasons behind decisions to acquire one aircraft design over another spark debate, even after the aircraft is long out of service. Randall Wakelam, in *Cold War Fighters: Canadian Aircraft Procurement, 1945–54*, provides insight into Royal Canadian Air Force (RCAF) aircraft procurement and the Canadian aircraft manufacturing industry during the Cold War, investigating specifically the Avro-built CF100 and Canadair-built F-86. Wakelam, a Canadian Air Force officer with aircraft procurement experience, was able to access government and Avro documents to gather extensive data on how the RCAF went from building a peacetime air force after the Second World War (WW II) to acquiring a strong air force to defend the country against the Cold War threat.

The book explores Canada's need during the early years of the Cold War to have jet aircraft, with the hope of ensuring Canada's equality among its allies as well as the ability to maintain the RCAF's credibility. Wakelam provides insight into why the RCAF and the Canadian government wanted Canadian-built aircraft and engines, a great feat after having just exited WW II. Canadian-built aircraft and engines would require a financial commitment from a government just getting over a major war, a leap in technological advancement, and a sound understanding of a new threat.[1] The Canadian government and the RCAF wanted to become more self-sufficient, which they believed would solve parts-availability issues that in turn caused aircraft production delays. Self-sufficiency would also ensure the availability of required aircraft for the RCAF.[2]

The process of procurement has always included a lot of moving parts, as Wakelam explores, including RCAF needs, politics, standardization with allied air forces, and understanding the predicted threat of the time. Putting all these pieces together has not always been an easy task, resulting in aircraft production delays or aircraft acquiring additional roles that were not originally intended.

The Canadian government, during the early Cold War years, recognized the Air Force as the service that would be Canada's main line of defence against the Soviet threat.[3] Entering the picture was A. V. Roe Canada (Avro)—which would build the CF100—and Canadair, with its version of the F-86. Foreign policy and the RCAF's constant operational-requirement changes would cause delay issues for the production of the CF100. The development of the Orenda engine made both of these aircraft more attractive, but with delays, the aircraft would originally be rolled out with American-built engines.[4] With the onset of the Korean War and the North Atlantic Treaty Organization (NATO) requirements in Europe, the F-86 was purchased as a stopgap and would fulfil Canada's NATO commitment. Both aircraft would eventually fulfil Canada's domestic and NATO roles, but in 1953, they would be considered obsolete.[5] This meant that discussions about a replacement for both aircraft would begin the procurement cycle once again. Thus began talks of the Avro Arrow, a subject for another book.

This book was an interesting read about technology and also about personalities such as C. D. Howe, Crawford Gordon, Lester B. Pearson, John Diefenbaker as well as their military counterparts. Wakelam explores defence and foreign policies, the desire at the time to provide the RCAF with a Canadian-designed-and-produced aircraft as well as the changing threat, which ultimately led to the early stages of developing a jet interceptor that no one else could provide. *Cold War Fighters* gives a clear understanding of the relationship played in the procurement cycle between politics, military requirements, defence policy, and the changing threat. This well-researched book, while purposely stopping short of the Avro Arrow project, nevertheless leaves the reader speculating about the Arrow's rise and fall.

Major Kathy Falldien, an aerospace controller, is currently the Education Coordinator at the Canadian Forces Aerospace Warfare Centre.

Abbreviations

Avro	A.V. Roe Canada
NATO	North Atlantic Treaty Organization
RCAF	Royal Canadian Air Force
WW II	Second World War

Notes

1. Randall Wakelam, *Cold War Fighters: Canadian Aircraft Procurement, 1945–54* (Vancouver: UBC Press, 2011), 22.

2. Ibid.

3. Ibid., 37–38.

4. Ibid., 128.

5. Ibid., 134.
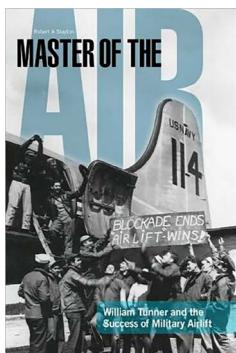
MASTER OF THE AIR: WILLIAM TUNNER AND THE SUCCESS OF MILITARY AIRLIFT

By Robert A. Slayton

Tuscaloosa: The University of Alabama Press, 2010

303 pages

ISBN 978-8173-1692-1

Review by **Dr. Richard Goette**

aster of the Air is a biographical study of the American air force champion for air mobility / strategic airlift, Lieutenant-General William Tunner. Robert Slayton, a professor in the Department of History at the Wilkinson College of Humanities and Social Sciences, Chapman University, California, calls Tunner "the father of military airlift."[1] This is an appropriate label, given that this remarkable American air force general played a key and often leading role in some of the most important airlift endeavours of the mid-20th century, including "the Hump" in Burma, the Berlin Airlift, Korea as well as the development and growth of the United States Air Force's (USAF's) air mobility community.

Within the pages of this book, Slayton outlines Tunner's long career in strategic airlift and, in particular, his constant endeavour to make military air mobility an equal partner to some of the other, more kinetic, air force communities such as fighters and bombers. In so doing, the author colours Tunner in an almost Billy Mitchell-esque manner. Tunner is compared not only to the famous American air power theorist's more inclusive interpretation of air power but also to his staunch and even crusading advocacy of what he believed in—which in Tunner's case was airlift. Indeed, Slayton calls Tunner a "transformation agent,"[2] emphasizing individuals as agents of change for institutions "who challenge the very core of the institutions' beliefs and practices and force them to change for the better."[3] However, Slayton does not focus on Tunner at the expense of others; indeed, the author effectively demonstrates a crucial aspect of leadership—having capable subordinates (what Slayton in Chapter 4 calls "Tunner's Men") on one's staff in order to enable a leader and their mission. Tunner was not one who suffered fools, but neither was he an overly authoritarian leader, as he also recognized the importance of healthy competition between aircrews to increase efficiency and that humour was essential in maintaining morale.

Although Slayton is clearly an admirer of Tunner, he does not back away from directing criticism at the USAF general where it is due. In particular, Slayton highlights how Tunner's incredible work ethic also meant that he expected the same from those under his command, resulting in his tendency to overwork his personnel and the subsequent development of morale problems. Furthermore, Tunner's grand vision to justify airlift as an equal partner sometimes blinded him to other pressing issues, such as being too focused on "getting immense supplies of goods in, and not stopping to take them out."[4] One is also reminded of the Royal Canadian Air Force's (RCAF's) own Air Marshal Gus Edwards when reading that Tunner worked so hard it literally made him sick.[5]

The highlight of the book is Slayton's examination of Tunner's role in Operation VITTLES during the Berlin Airlift, which it could be argued is one of the greatest demonstrations of the utility of air power (especially air mobility). Slayton makes the interesting point that the Soviets, based on the Luftwaffe's experience at Stalingrad in 1942–43, downplayed the ability of airlift to sustain a surrounded force or population.[6] He also desires to set the record straight in that, although General Lucius Clay got most of the credit for the Berlin Airlift, the true genius behind it was Tunner: "He became the architect of the airlift, the true victor of Berlin in those dark skies of 1948 and 1949."[7] Tunner devised the intricate system of cargo flights into and out of the beleaguered city and, in so doing, developed a variety of procedures and best practices for military and civilian aviation for years to come (i.e., uniform parallel runway orientation).

Much like the concept of the indivisibility of air power, which dictates that the military use of aviation should be handled by those with expertise (airmen and airwomen), Slayton also highlights Tunner's beliefs that airlift cannot be handled by an ordinary air force officer and that the individual has to be specifically trained in airlift—by those who **totally** know what they are doing.[8] This also includes command and control of air mobility resources: Tunner's "experience in Korea had confirmed the notion that all military transport should be centralized under one command and that only people experienced in this field should be in charge."[9] Another interesting aspect of Slayton's book is his emphasis on the business/professional aspect of Tunner; Slayton explains that the USAF general saw the running of an airlift command organization and mission as being like running a business.

At times the author tends to go off topic by focusing too much on the context without tying back to how it relates to Tunner himself (i.e., several pages of context without mention of Tunner). In these cases, however, Slayton paints an interesting picture of the events that surrounded Tunner's career, in particular the Burma Hump airlift and the Berlin Airlift. Though the author describes in detail Tunner's advocacy for airlift, describing it as one of the air force's "core missions,"[10] Slayton does not go so far as to **explicitly** identify air transport as a mainstream form of air power.

Nevertheless, such shortcomings are minimal. *Master of the Air* is a meticulously researched book that is very readable. Slayton has made a vital contribution to the history of military air transport and the study of air power. In particular, this book is a welcome addition to the literature that otherwise largely focuses on more "kinetic" forms of air power. This book is, therefore, highly recommended for students of air power, aviation enthusiasts and, in particular, professionals in the air mobility community.

Dr. Richard Goette lectures on air power and teaches in the Defence Studies Department at the Canadian Forces College. He is also an Associate Editor-in-Chief of *Airforce* magazine, the official publication of the RCAF Association.

Abbreviations

RCAF	Royal Canadian Air Force
USAF	United States Air Force

Notes

1. Robert A. Slayton, *Master of the Air: William Tunner and the Success of Military Airlift* (Tuscaloosa: The University of Alabama Press, 2010), 2.

2. Ibid., 1.

3. Ibid., 3.

4. Ibid., 155.

5. Ibid., 212.

6. Ibid., 87.

7. Ibid., 2.

8. Ibid., 168.

9. Ibid., 231.

10. Ibid., 3.

WHY AIR FORCES FAIL:
THE ANATOMY OF DEFEAT

Edited by Robin Higham and Stephen J. Harris
Lexington: University Press of Kentucky, 2006
382 pages
978-08-1312-374-5

Review by **Major Jennifer Foote, CD, MPA**

Learning lessons is key to the future success of the Royal Canadian Air Force (RCAF) and is an integral part of all operations, exercises and daily activities. The ability to analyse a situation, identify its shortcomings and recommend remedial action provides the building blocks for improvement and the potential to add value to our collective air force knowledge. This edited anthology, *Why Air Forces Fail: The Anatomy of Defeat*, is a valuable addition to an air power library, as it identifies numerous cause-and-effect dynamics that influenced the outcome of significant air battles. This well-researched historical study of the complexities which underpin the failure of air forces throughout the 20th century is a fairly broad overview of a few select air battles from which many lessons can be learned. The editors have grouped the failures into three categories: air forces that never had a chance to win, such as Poland and France; air forces that were victorious at the outset but were ultimately defeated, namely Germany and Japan; and the last group contains those air forces that struggled in the beginning, but ultimately triumphed, such as the American and British air forces. In all cases, the authors examined all possible contributing factors such as geography, politics, technology, training and timing.

Eleven cases are examined including Poland's Military Aviation in 1939, the gradual defeat of the French Air Force between 1933 and 1940 as well as the limited success of the Arab air forces which, interestingly, are grouped together in this essay even though the air forces discussed were from different nations and were not all allies. Other cases include the failure of the German Air Force during both World Wars as well as the defeat of the Italian and Argentinian air forces. Japan's surprising victory is explored, followed by more disasters by the Russian, American and British air forces. While not a complete examination of every failing air force, this collection captures what are certainly the most prominent battles and draws worthwhile conclusions.

This study of factors influencing the outcome of the application of air power cuts a wide swath, exploring not only the more obvious numerical or technological superiority of air power but also the doctrine upon which tactics were based and the geopolitical climate at the time. The effectiveness of command and leadership are challenged, while gaps in intelligence demonstrated the fatality of incorrect assumptions. The chapters examining each situation are dense, fact filled and generally assume that the reader has a certain level of familiarity with the history of military air power. *Why Air Forces Fail* is not the whole story, but it is an eye-opening introduction to a collection of complex military and political histories, culminating in each authors' assessment of the reasons behind the outcome of the battle being studied. Each historical vignette is followed with suggestions for further research and a recommended reading list, encouraging the reader to examine the air battles more closely and delve more deeply into the lessons that were learned. I feel that I am left with more questions than answers about the true nature of an air force's failure, but this collection provides a starting point and a roadmap to further discovery—a welcome redirect as I study air power and how it affects the Royal Canadian Air Force today and into the future.

Major Jennifer Foote, a Communications and Electronics Engineering (Air) officer, is employed as the technical lead for the Air Synthetic Environment at the Canadian Forces Aerospace Warfare Centre. Previous posts include Deputy Commanding Officer Canadian Forces Recruiting Centre Winnipeg, Air Staff Information Management Officer and RCAF planner for both the 2010 Olympics and the G8 Summit. She is a graduate of the Aerospace Systems Course at the Canadian Forces School of Aerospace Studies, holds a Master of Public Administration from the University of Manitoba and is currently enrolled in the Joint Command and Staff Programme at the Canadian Forces College.