ROYAL CANADIAN AIR FORCE JOURNAL

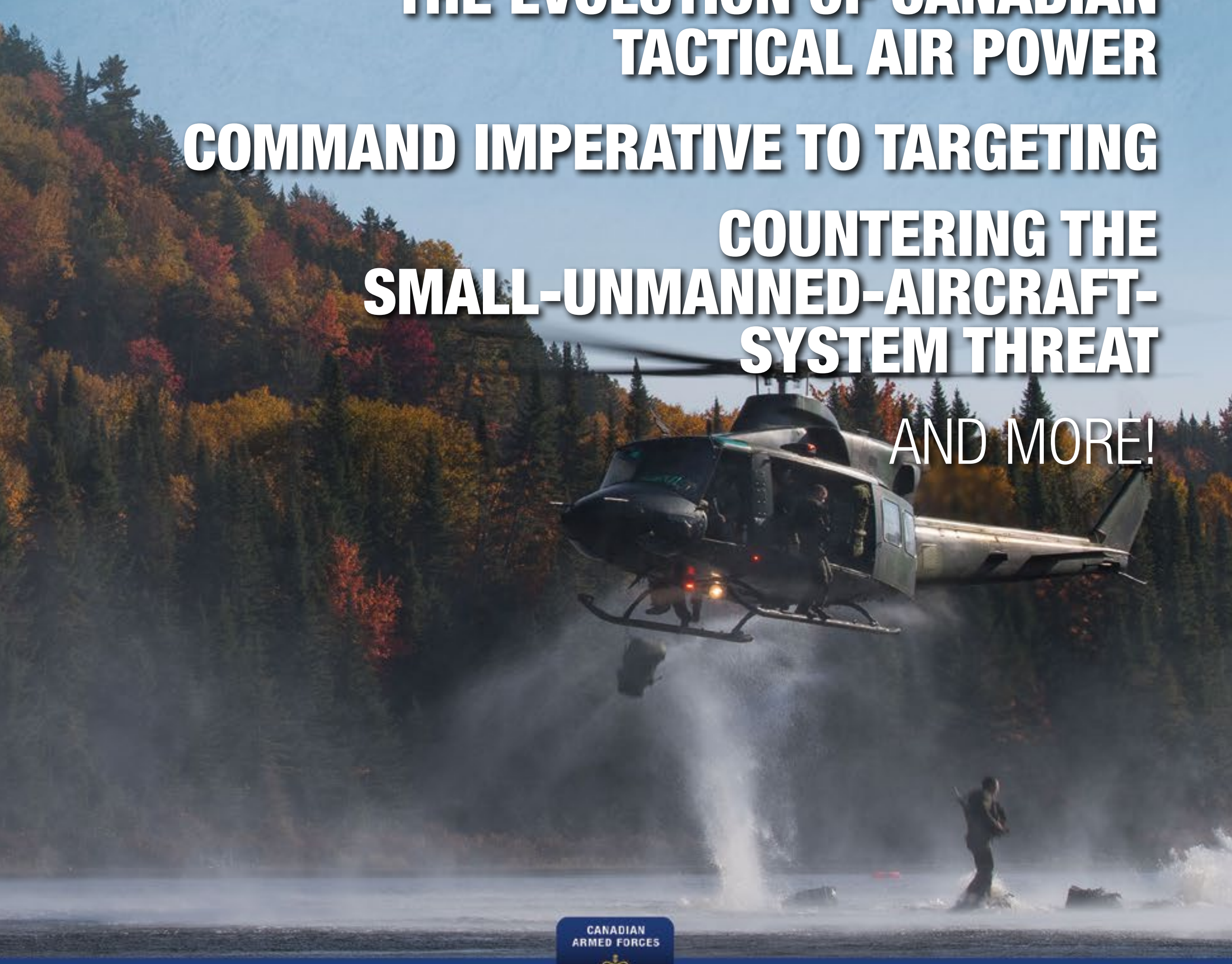
FALL 2016 • VOL.5, NO.4

THE EVOLUTION OF CANADIAN TACTICAL AIR POWER

COMMAND IMPERATIVE TO TARGETING

COUNTERING THE SMALL-UNMANNED-AIRCRAFT-SYSTEM THREAT

AND MORE!



CANADIAN ARMED FORCES
FORCES ARMÉES CANADIENNES

National Defence Défense nationale

Canada

The *ROYAL CANADIAN AIR FORCE JOURNAL* is an official publication of the Commander Royal Canadian Air Force (RCAF) and is published quarterly. It is a forum for discussing concepts, issues and ideas that are both crucial and central to air and space power. The *Journal* is dedicated to disseminating the ideas and opinions of not only RCAF personnel, but also those civilians who have an interest in issues of air and space power. Articles may 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. This journal is therefore dedicated to the expression of mature professional thought on the art and science of air warfare and is central to the intellectual health of the RCAF. It serves as a vehicle for the continuing education and professional development of all ranks and personnel in the RCAF as well as members from other environments, employees of government agencies and academia concerned with air-force affairs.

EDITORIAL TEAM

EDITORIAL STAFF

Editor-in-Chief: Colonel Kelvin Truss
Senior Editor: Lieutenant-Colonel Doug Moulton, CD, MBA

Published by Canadian Forces Aerospace Warfare Centre
ISSN 1927-7601

ASSISTANT EDITORS Adri Boodoosingh, Lisa Moulton and Vickie Thobo-Carlsen

GRAPHIC DESIGN Cara Hunter, Denis Langlois and Luc Leroy

ONLINE EDITION Christine Rodych

PRODUCTION MANAGER Denis Langlois

For copies of this publication or to be placed on a distribution list contact CFAWCProd@forces.gc.ca

http://www.rcaf-arc.forces.gc.ca/en/cf-aerospace-warfare-centre/index.page

http://w08-ttn-vmweb01/CFAWC/en/elibrary/journal/current-issue.asp

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 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 CFAWCRCAFJournal@forces.gc.ca

CALL FOR SUBMISSIONS

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

For the Fall 2017 issue: **30 July 2017**

For the Winter 2018 issue: **30 October 2017**

For the Spring 2018 issue: **30 January 2018**

DISCLAIMER

Opinions expressed in the *RCAFJ* remain those of the author and do not represent Departmental or Canadian Armed Forces policy. Doctrine, training and other material published in the *RCAFJ* does not represent authority for action on that particular topic. All published material remains copyright of the Department of National Defence and may not be used without written permission.

Photo: DND

CONTENTS

FALL 2016

VOLUME 5 • NUMBER 4

EDITOR'S MESSAGE 4

ARTICLES

MCNAUGHTON AND THE EVOLUTION OF CANADIAN TACTICAL AIR POWER: A CAUTIONARY TALE OF THE LIMITS TO JUNIOR-ALLIANCE-PARTNER INNOVATION 6
BY LIEUTENANT-COLONEL PAUL JOHNSTON, CD

COUNTERING THE SMALL-UNMANNED-AIRCRAFT-SYSTEM THREAT TO THE CANADIAN ARMED FORCES 27
BY MAJOR DAN WALTERS, CD, MDS

COMMAND IMPERATIVE TO TARGETING: CANADIAN ARMED FORCES EFFECTIVENESS IN TARGETING WITH AIR POWER DURING OPERATIONS MOBILE AND IMPACT 40
BY LIEUTENANT-COLONEL JARED PENNEY, CD

CYBER WARFARE SCHOOLS OF THOUGHT: BRIDGING THE EPISTEMOLOGICAL/ONTOLOGICAL DIVIDE, PART 2 64
BY LIEUTENANT-COLONEL P. E. C. MARTIN, CD, MDS, MASC

BOOK REVIEWS

AIR POWER HISTORY: TURNING POINTS FROM KITTY HAWK TO KOSOVO 90
REVIEW BY LIEUTENANT-COLONEL PUX BARNES, CD, MA

THE BRIDGE TO AIRPOWER: LOGISTICS SUPPORT FOR ROYAL FLYING CORPS OPERATIONS ON THE WESTERN FRONT 1914–1918 93
REVIEW BY MAJOR WILLIAM MARCH, CD, MA

THIEVES OF STATE: WHY CORRUPTION THREATENS GLOBAL SECURITY 95
REVIEW BY MAJOR CHRIS BUCKHAM, CD, MA

POINTS OF INTEREST

UNBLINKING AND UNHERALDED: CANADA'S ISR CONTRIBUTION TO OPERATION IMPACT 97
BY LIEUTENANT-COLONEL BRENDAN COOK, MSM, CD

EDITOR'S **MESSAGE**

The theme that runs through this issue of the *Royal Canadian Air Force Journal* is that of air-land integration. Given our engagements in Operations ATHENA, MOBILE and IMPACT, it is safe to say that the Royal Canadian Air Force (RCAF) will continue to be engaged in kinetic activities for the foreseeable future. As the RCAF rarely operates without land forces, exploring this complicated joint area of operations is fundamental to preparing for the next operational challenge.

This past summer, the RCAF's Major-General Wheeler took command of the Targeting Capability Implementation Team, which will lead the way for Canadian Armed Forces targeting in a joint and combined environment. However, the challenges of targeting today are not entirely new. There are echoes from the past and current arguments driving today's efforts to work more closely together in this battlespace, so to set the stage for the current situation, we offer Lieutenant-Colonel Paul Johnston's fascinating take on General McNaughton's efforts with air-land integration up to and including the Second World War.

Following the historical take on this topic, we have provided articles on current targeting issues and a possible game changer that could develop from the threat of small unmanned aircraft systems. There is much to consider in the air-land environment, whether it is targeting and destroying the enemy or dealing with small unmanned aircraft systems that can disrupt our operations. Much of the air-land integration achieved in recent operations is a legacy of Afghanistan, which strongly suggests that joint and combined interoperability will long be an important factor for all air forces. It is hoped that the historical background followed by current operational issues sparks interest and discussion—no matter where they take place—in the future of Canada's aerial warfighting capabilities.

Enjoy the read.

Sic Itur Ad Astra

Lieutenant-Colonel Doug Moulton, CD, MBA
Senior Editor

Members of 5 Canadian Mechanized Brigade Group participate in patrol reconnaissance training at Lac à l'Île located in the training areas of CFB Valcartier in Courcelette, Quebec, October 7, 2016. Photo: DND

McNaughton and the Evolution of Canadian Tactical Air Power: A Cautionary Tale of the Limits to Junior-Alliance-Partner Innovations

By Lieutenant-Colonel
Paul Johnston, CD

On 17 July 1944, in the midst of the most critical phase of the Normandy campaign, tactical aircraft swooped out of the sky to strafe a lone German staff car near Rouen, severely wounding Field Marshal Rommel.[1] How the rest of the campaign would have unfolded had the energetic Rommel not been removed in this manner can never be known, but the event was certainly a coup for tactical air power. The aircraft responsible for taking out Rommel has been the subject of some debate, but it now seems clear that it was Flight Lieutenant Charley Fox of No. 412 Squadron, Royal Canadian Air Force (RCAF), flying a Spitfire Mark IX.[2] Canada was, thus, responsible for one of the most famous exploits of tactical air power in the Second World War. Other exploits for tactical air power followed, from the destruction of the German counter-offensive at Mortain to the rout of the German armies through Falaise. Indeed, the Northwest-Europe Campaign that ended the Second World War in 1944–45 represented a high-water

mark for Canadian contribution to tactical air power and a highly developed state of air-land cooperation. But that state of affairs was only reached after a highly contentious development process. British land and air forces entered the war with starkly differing views on the optimal employment of air power, tactically or otherwise, and, as we shall see below, went through a years-long development process before the system existing in 1944 was created.[3]

Canada came to be a key participant in the *execution* of this system, providing approximately eight per cent of the Allied tactical air forces for Operation OVERLORD, a greater proportion compared to our population than the Americans.[4] However, Canada was not a major player in the debates that *developed* this system for tactical air power. Despite that, one Canadian figure stands out for his fascinating, if somewhat quixotic, role in this tale—Canadian Army Lieutenant-General Andrew McNaughton.

In the early 1930s as Chief of the General Staff (CGS) of Canada, McNaughton advocated a joint army-air contingent as a Canadian expeditionary force, and in the Second World War itself as the Commander of 1st Canadian Army, he continued to agitate for such a force—a spearhead to invade the continent. He was also a Canadian nationalist, determined to see such a force concentrate Canadian units, both land and air, in an all-Canadian entity under Canadian national command, and he applied his considerable intellect and energies towards efforts to realize such a force during the war.

However, it was not to be. While strong tactical air forces did eventually work with 1st Canadian Army, this was not due to McNaughton's efforts but, rather, followed from the resolution of the larger British (indeed Anglo–American) tactical air power debate—a debate in which Canada played no real part. Nor was McNaughton's nationalist vision of an all-Canadian air-land contingent to be realized—the strong tactical air forces that did eventually cooperate with 1st Canadian Army were primarily British, while the Canadian squadrons worked with British 2nd Army.

This article will provide an overview of the history of the development of tactical air power, from its origins in the First World War, through the interwar years—when expertise and emphasis upon tactical air power was largely lost—and into the Second World War—when strong tactical air forces were eventually developed, despite fierce interservice rivalry between the British Army and the Royal Air Force (RAF). This is important background for the Canadian experience, for at the time Canadian military practice was heavily influenced by the British model. It is all the more striking, therefore, how much McNaughton's arguments stand out. McNaughton was a visionary, but a frustrated one. In the end, he was unable to translate his innovative ideas into concrete reality, even though subsequent events in many ways vindicated his original vision. This failure can serve as a cautionary tale for the limits to originality open to a junior alliance partner, an issue that remains relevant today, as Canada ponders how best to contribute to the war against the Islamic State of Iraq and the Levant (ISIL).

First World War

The history of the evolution of air power from 1914 is generally well trod. When the First World War broke out, air power's original role was observation, but very quickly, it turned to both ground attack and to air-to-air. While bombing tended to concentrate upon deeper targets and the fighters fought for command of the air, what concerns us here is the developments in tactical air power—meaning air power dedicated to the defeat of ground forces, not merely at the front, but also throughout the full operational depth.[5] This role has generally received less attention than either strategic bombing or air-to-air fighting but was prominent in the First World War.[6]

The initial evolution of air power was quite rapid. The first wartime update of British air doctrine appeared in November of 1914 and noted that "aircraft are capable of offensive action against troops on the ground by means of machine guns and bombs."[7] By the spring of 1915, the Royal Flying Corps (RFC) had promulgated an official note on "bomb-dropping attacks," which recommended bombing from no more than 500 feet [153 metres] altitude. It also suggested that the most rewarding targets were not the front trench lines but, rather, columns of troops and transport in the immediate rear, road and rail chokepoints as well as supply dumps. In part, this was because of the difficulties of attacking the sort of dug in and dispersed targets typically found in the forward areas; it was also partly due to the attractiveness of using air attack as a means of reaching beyond artillery range.[8] By 1916, each British field army had an RFC "brigade" (several squadrons) attached to support its operations. For the most part, these brigades concentrated upon reconnaissance and, secondarily, fighting for control of the air. They did, however, conduct ground attack as a secondary role, which was generally known as "trench strafing" or "trench bombardment."[9]

The year of Vimy, 1917, was a time of great tactical developments on the Western Front, and tactical air procedures were no exception. By this time, the Canadian Corps had two squadrons directly assigned to it—Number 1 (Nieuports) and Number 41 (F.E.8s)—with close ground support as their primary role. In practice, this meant that they concentrated their attacks upon German airfields and transportation infrastructure (in particular train stations), but they would also strike German ground forces "in order to harass the enemy as much as possible and spoil the morale of his troops."[10]

By the summer of 1918, the RFC's procedures for what we would, today, call close air support had reached essentially their final form for the First World War, which were quite sophisticated, considering the technology available at the time. For offensive operations, ground-attack squadrons would establish forward-landing fields close behind the front lines. These were expedient landing strips where the aircraft could land, refuel, rearm and, most importantly, wait on alert. From these forward-landing fields, "scout" aircraft were sent off to patrol for targets among the enemy ground forces. When good targets were spotted, the scout aircraft would fly back to the advanced landing field, pick up the balance of the squadron which was waiting on alert and lead them to the target. Given that the advanced landing strips were only a few minutes' flying time behind the front and that the scouts did not even need to land (they simply circled the field to be seen by the waiting aircraft who would scramble and follow them back to the targets), this system could result in air attack upon targets of opportunity within less than 30 minutes.[11]

In the final Hundred Days of the war, when mobile warfare at last returned, ground-attack aircraft were used to considerable effect to disrupt the German retreat. Generally, they would be sent on patrols along the routes the Germans were following, often with devastating results. One No. 46 Squadron pilot recalled of this time:

> We found a long straight road filled with retreating German supply trains. … We formed a big circle and dropped our 25-lb [11 kilogram] bombs. When we got through with that road it was one unbelievable scene of chaos, with dead horses, lorries and dead soldiers all over the road.[12]

Thus, by the final battles of the First World War, tactical air power had reached a quite remarkable stage of development. And Canada had been intimately involved in these developments, both in the air and on the ground. Canadian flyers featured prominently among those flying the tactical air support, and the Canadian Corps was one of the main employers of this new form of armed force.

Interwar Years

The immediate aftermath of the First World War, however, saw a rapid loss of this rich heritage of experience in tactical air power. The RCAF was formed as an independent service in 1924, but throughout the interwar years, it was scarcely an armed force at all. Most of its work was focused upon transport and general-utility roles as well as air photography, in which capacity it did a great deal of work surveying the vast expanse of the Canadian north. Indeed, the RCAF of that time period has been termed a force of "bush pilots." Nor did the young RCAF participate in any expeditionary operations.[13]

The only thinking about war that the interwar RCAF did absorb came from the RAF. Canadian officers went to staff college in Britain; indeed, it was deliberate policy to encourage military standardization across the empire, in pursuit of what we would today call "interoperability." As the Canadian soldier-statesman Maurice Pope wrote in his memoirs, the Canadian military was "indeed British through and through."[14] And this British influence was decidedly slanted towards strategic bombing, tending to deprecate any tactical role for air power.[15] With regard to tactical air power, one of the few British officers to give the issue any attention at all was John Slessor, an RAF career officer who published a book on the subject in 1936.[16] Based upon a detailed historical analysis of air support in the First World War, Slessor argued that: "*the aeroplane is not a battle-field* weapon—the air striking force is not as a rule best employed in the actual zone in which the armies are in contact."[17][emphasis in original]

Slessor was of the opinion that it would be more profitable to use air power—or at least whatever air power might have to be diverted from the strategic bombing campaign—against the enemy's rear, particularly against their lines of communication at corps or higher level.[18] But Slessor's real feelings appear to have been that almost any dedication of air power to armies in the field was a waste.

> The ultimate reduction of the enemy nation may (and very likely will) be undertaken, not by the traditional methods of land invasion, or by continued assaults upon their armies in the field, but by air measures. That is to say it will become an air campaign, and the task of the army will be simply to protect the air bases.[19]

Slessor's book was based upon lectures he had given at the Army Staff College at Camberley as a wing commander in the early 1930s. One can just imagine the Army officers' reaction there to being told that their primary task would be "simply to protect the air bases." Still, Slessor was at least taking the time to address Army officers; throughout this period, there was little interaction of any kind between the two services.

McNaughton's First Air Force

Meanwhile, back in Canada, an officer with views quite different from Slessor and the RAF was to be found—Major-General Andrew McNaughton, the CGS in Ottawa in the early 1930s. He was a remarkable figure; as James Eayrs put it in his seminal history of Canadian defence policy, "McNaughton dominated his colleagues in the military establishment as a great oak dominates a scrub forest."[20]

McNaughton was an artillery officer who first came to prominence in the First World War; he had made his name there on the Canadian Corps' counter-battery staff, developing innovative solutions to the problems of trench warfare.[21] McNaughton was a technocrat, convinced that warfare was fundamentally a matter of developing ingenious scientific solutions to tactical problems.[22] Indeed, after retiring as CGS in 1935, he went to work for the National Research Council, returning to the colours in 1939 to command the 1st Canadian Infantry Division. During the Second World War, Tony Foster, who served under McNaughton and eventually rose to command a division, recalled that in meetings McNaughton was prone to what he called "attacks of the gadgets."[23] In a similar vein, Charles Carrington, an Oxford University don between the wars and the British Army's liaison officer at Bomber Command during the Second World War, referred to McNaughton in his memoirs by the nickname "the Gadget King."[24] Perhaps due to his forward-looking and technical mindset, McNaughton was a strong proponent of tactical air power, closely integrated with land forces, and actively lobbied for the establishment of such forces from an early date, long before it became the standard practice.

McNaughton's interest in air power dated back to his days on the Canadian Corps' counter-battery staff in the First World War. As a gunner and a technocrat, the aerial delivery of firepower had a natural appeal for him, and aircraft were heavily involved in the counter-battery work he had performed in the First World War. In the 1930s, he had even published an article in *Canadian Defence Quarterly* describing map surveying from the air.[25] McNaughton was known as a supporter of air power. Indeed, the official history of the RCAF offers the opinion that under McNaughton's influence, the RCAF was much less opposed to army co-operation work than the RAF was.[26]

One of the manifestations of McNaughton's enthusiasm for tactical air power was his support as CGS for the establishment of a robust collection of army co-operation squadrons in the RCAF.[27] At that time, in the early years of the Great Depression, he lobbied for the creation of a force of no less than 12 RCAF squadrons to support a Canadian expeditionary force. A plan known as Defence Scheme No. 3 formed the basis for planning for such an expeditionary force, which was originally envisioned as consisting of up to seven divisions, although latter versions reduced this to two infantry divisions.[28] What McNaughton appeared to be trying to build was a joint land-air expeditionary force—in which a corps-sized, Canadian Army contingent would work closely with at least a three-squadron-sized RCAF contingent—for mobile warfare. This was a notable organization for at least two reasons: firstly, it constituted a far more lavish scale of tactical air support (at least a squadron per division) than envisioned anywhere else at the time, and secondly, McNaughton's proposed arrangement appeared to envision a far closer degree of air-land integration than others, notably the RAF, were then contemplating.[29]

Rearmament and Early War

Back in Britain, the atmosphere of mutual disdain and disregard between the Army and the RAF began to come to a head in 1935, when the so-called "Western Plan" envisioned—for the first time since the First World War—a return to a continental commitment for the British Army. The War Office requested that seven bomber and five fighter squadrons of the RAF be allocated to the first contingent of any British field force that might be sent to the continent, with a further six bomber and four fighter squadrons for each of the potential three subsequent contingents.[30] The Air Ministry steadfastly opposed these requests, arguing against tying the RAF's limited resources down to any prearranged commitments.[31] In general, the RAF and Air Ministry continued to oppose any shift of policy away from a deterrent strategy based upon bombers.[32]

Things had scarcely improved when war did eventually come in 1939. In March of that year, the Chief of the Imperial General Staff, Lord Gort, with an eye to the envisioned 32-division programme, formally demanded that a strong striking force of bombers be included under the field force.[33] Convinced of the strategic importance of independent bombing, the Air Ministry resisted Gort's requests for bombers particularly fiercely. Slessor, by now an Air Vice-Marshal (A/V/M) and senior planning officer on the Air Staff, wrote that the War Office seemed bent on "a regrettable revival of the old idea which there had been some reason to think was dead, that when the soldiers talk about co-operation they really mean the subordination of the air force to the army."[34] At one interservice Whitehall meeting in June, the Assistant Chief of the Air Staff asserted that fundamentally all bombing was the same, regardless of the actual target; therefore, no specialization in training or command arrangements was necessary to meet the field force's needs.[35]

When the decision was finally taken later that year to dispatch a British Expeditionary Force (BEF) to the continent, the RAF realized that it would have to provide something to forestall Army demands for a separate air force under Army control, but the issue never was settled to either parties' satisfaction.[36] During the Battle of France, the BEF had the two bomber and four fighter squadrons the RAF had agreed to provide, plus six Army co-operation squadrons and two flights of very important person (VIP) transport aircraft.[37] The "Advanced Air Striking Force" or AASF, a force of medium bombers, went to France as well, but it remained under Bomber Command.[38]

After Dunkirk, the RAF quickly reverted to its pre-1935 philosophy when there had been little contemplation of a British continental land commitment. According to its own thinking, the RAF now had three major missions: protecting the home island from air attack (Fighter Command's job); mounting a strategic bombing campaign against Germany (Bomber Command's job); and supporting the Royal Navy for the Battle of the Atlantic (Coastal Command's job).[39] If all went well, in the RAF's view, the Army's role would be restricted to home defence of the British Isles should an invasion come and subsequent occupation of a Germany that had been defeated by the strategic bombing campaign.[40] Nevertheless, the Army could not be ignored entirely, and shortly after Dunkirk "Army Co-operation Command" was formed within the RAF under Air Marshal Sir Arthur Barratt. This command, however, came last in the RAF's priorities, and often languished with "more staff officers than aircraft."[41]

For its part, the Army remained mesmerized by the German performance in France and, bitter about the lack of any visible RAF presence over the beaches of Dunkirk, was obsessed with getting dive-bombers that could be quickly "whistled-up" (as one commentator put it) the way the Germans seemed to do.[42] The RAF opposed any such suggestion at every turn. Slessor even went so far as to write a paper specifically devoted to debunking the dive-bomber mania in the Army, pointing out that the Germans did not, in fact, devolve control of dive-bombers to lower army formations and were only able to use the obsolescent Junkers-87 dive-bombers where they enjoyed air superiority and their opponents lacked effective anti-aircraft artillery.[43] Slessor stuck to his original theories from *Air Power and Armies*, concluding "I do not believe in close support at all."[44] In general, the RAF maintained that the war-winning instrument would be strategic bombing; any allocation of scarce RAF resources to army support would inevitably compromise that decisive effort, violating the principle of concentration of force. In 1941, the Chief of the Air Staff himself, Sir Charles Portal, officially argued to the Cabinet that "the Army has no primary offensive role. … We aim to win the war in the air, not on land."[45]

The new Chief of the Imperial General Staff, Sir Alan Brooke, immediately strove to argue against this view. Brooke had been a corps commander at Dunkirk and personally felt strongly about what he considered to have been the RAF's inadequate support in that defeat.[46] In March of 1942, he demanded the establishment of a force of 109 squadrons to be trained in the tactical role as a part of the Army rather than the RAF.[47] The demand for an air force within the Army may have been a bureaucratic negotiating tactic, but it showed how seriously Brooke took the issue. After a series of acrimonious discussions, Portal and Brooke reached a minimal compromise at a Chiefs of Staff meeting on 19 May 1942. The RAF's Army Co-operation Command and No. 2 Group were to be expanded slightly, and 15 squadrons of Fighter Command were to be trained in ground support, but they could not agree on the contentious issue of command and control.[48]

McNaughton's Second Air Force

Canadians played no particular role in this fierce debate between the British air and ground forces, but just as it was coming to a head, McNaughton stepped into the line of fire. Upon mobilization in 1939, McNaughton was recalled to the colours to become the commander of the original Canadian Army overseas force, the 1st Canadian Infantry Division. As we have seen, McNaughton was an enthusiast for tactical air power, and he immediately began lobbying for a robust RCAF contingent specifically dedicated to supporting his command, just as he had in the early 1930s.

The RCAF's original thinking upon mobilization was for a three-squadron army co-operation wing "for despatch overseas if required."[49] At a time when the Canadian Army had only one division preparing for embarkation and, as yet, only aspired to form a single corps, this constituted a lavish scale of air resources for army support. Too lavish in fact. The plan that was eventually ironed out in November 1939 was for the RCAF to deploy one Army co-operation squadron, which would work with 1st Canadian Infantry Division, then en route for France. 1st Canadian Infantry Division would join IV British Corps, and the RCAF squadron would then become that corps' army co-operation squadron, in accordance with the standard British establishment of one squadron per army corps.[50]

The RCAF squadron in question was No. 110 (Army Co-operation [AC]) Squadron, equipped with the already obsolescent Lysander, a small observation and light utility aircraft.[51] 110 Squadron arrived in England in February 1940, still largely untrained; the intention being that it would work with 1st Canadian Infantry Division until both were judged ready for commitment to France with the BEF.[52] McNaughton certainly considered 110 Squadron part and parcel of a unified Canadian expeditionary force. On 8 May 1940, he wrote to the RCAF headquarters in Britain that it was my "understanding that 110 (AC) Squadron, RCAF, has been provided primarily for the purpose of working with the Canadian forces in the field, and I hope that there will be no doubt that our requirement in this connection will have priority."[53]

Only three days later, on 11 May 1940, the Canadian government formally offered Great Britain a second army co-operation squadron for active service.[54] This was No. 112 (AC) Squadron and was the second squadron of the RCAF's originally envisioned three-squadron army co-operation wing.[55] By coincidence, 11 May happened to be the day after the German offensive in the West began, and in the hectic aftermath of that debacle, the British informed Canada's High Commissioner in London that they would welcome No. 112, as well as anything else that Canada could make available, "as soon as possible."[56]

Only a few weeks later, the British were thrown off the continent at Dunkirk, transforming the strategic situation. McNaughton found himself promoted and given command of VII (British) Corps, consisting of 1st Canadian Infantry Division, a British armoured brigade and two brigades of New Zealand infantry. It comprised the entire operational reserve south of the Thames and was virtually the only mobile formation in the British Isles.[57] No. 110 (AC) Squadron became the corps army co-operation squadron.

Still equipped with Lysanders, No. 112 Squadron arrived in the United Kingdom (UK) in June of 1940 and was immediately sent to High Post, near the RAF Army Co-operation School, to begin operational training. Fortunately for all concerned, no German invasion of the British Isles materialized. In December of that year, VII Corps was dissolved, and the newly arrived 2nd Canadian Infantry Division was grouped with 1st Canadian Infantry Division to form the Canadian Corps (later I Canadian Corps). No. 110 (AC) Squadron duly became the corps' army co-operation squadron, but at the same time, No. 112 Squadron, which had been languishing in limbo, was officially redesignated a fighter squadron and re-equipped with Hurricanes.[58]

This left McNaughton with a corps to command and one RCAF army co-operation squadron to go with it—exactly the doctrinal British establishment of the time. However, McNaughton was not satisfied with this and continued agitating for a powerful, joint army/air all-Canadian force. "The Germans are using bombers as long range artillery and the stronger we can get the air component closely associated with the ground troops (and the Wing Commander close to the G.O.C.) the better."[59]

This was a theme that he harped on again and again, advocating not just army co-operation wings but also an actual tactical air force providing "not less than five squadrons for each division [of ground troops]."[60] The RCAF official history dryly notes that at the time this ratio "must have seemed ludicrous."[61]

However, there was little McNaughton could do until the further expansion of the Canadian Army. This was, however, not long in coming, and in May of 1941, with planning for a Canadian armoured division underway, McNaughton formally requested another army co-operation squadron so that armour and air "could grow up side by side."[62] The result was No. 414 Squadron, formed at Croydon, just south of London, unfortunately also equipped with Lysanders.

On Easter Monday in April of 1942, the Canadian Army overseas reached its final size when 1st Canadian Army was formally established, with a projected strength of at least five divisions, at least one of which would be armoured. Even by the British standards of the time, this would merit a three-squadron army co-operation wing, but the RAF was still stalling, and no new squadrons were being assigned to the Canadian Army. In exasperation, McNaughton appears to have turned to A/V/M Edwards, the senior officer at RCAF Overseas Headquarters. In May 1942, Edwards sent the Air Ministry a scathing paper condemning the RAF's approach to joint army/air operations.[63] Unfortunately, no known copy of the letter survives, but there is a copy of an early draft of it in McNaughton's papers, suggesting that McNaughton himself may actually have been the instigator. In any case, the letter was brutally frank, claiming that cooperation between the army and air force "still hardly exists" because of the "strong bias of senior Air Force officers in favour of strategic bombing."[64]

One of the limiting factors the British cited to explain why more air resources could not be allocated to 1st Canadian Army was the lack of an airfield suitable to house an army co-operation wing.[65] But the determined and ever resourceful McNaughton produced an answer to that objection—he would have his own Canadian Army engineers build an airfield.[66] Thus was born the air station of Dunsfold, Surrey, in the heart of the Canadian Army's garrison area. Work began in May 1942, and by dint of determined work from the Canadian engineers, it was ready by that October—considerably faster than the British, who usually took about a year to produce an operational airfield from scratch, even under the pressure of total war.[67] To go with this new airfield, on 12 September 1942, the long anticipated Canadian army co-operation wing was finally formed when No. 39 (AC) Wing, RCAF was established at nearby Leatherhead.[68]

On 12 January 1943, this two-squadron wing was joined by a third RCAF squadron, the newly established 430 Squadron. McNaughton and 1st Canadian Army finally had their three-squadron army co-operation wing, and in June of 1943, it moved into the Dunsfold airfield that McNaughton's engineers had strained to complete. Characteristically, McNaughton was not satisfied with this and agitated for an RCAF army co-operation wing of at least six squadrons to go with it, that is to say double the then doctrinal establishment.[69]

Canadianization

One of McNaughton's major themes was not simply a desire for a strong tactical air contingent directly supporting 1st Canadian Army, but that this air contingent should be Canadian. McNaughton was famously a nationalist, determined to keep the Canadian contribution to the war together as a national contingent under Canadian national command.[70] In this light, he wanted RCAF squadrons to provide tactical air power for the Canadian army, thus creating a joint army-air all-Canadian contingent that would constitute a spearhead for the British armies in the coming North West Europe campaign, rather in the manner that the Canadian Corps had been a spearhead in the battles of the final 100 days of the First World War.[71] This would require concentrating those RCAF elements engaged in tactical air power into one formation, something that brought McNaughton into the larger issue within the RCAF known as "Canadianization."

Canadianization was the RCAF's own term for their efforts to establish themselves as an independent entity with Canadian units grouped together into Canadian formations under Canadian administration and commanders, the way the Canadian Army was. Unlike the Army, however, this effort—while it generated considerable friction between Canada and Great Britain—was, at best, only partially successful.

Ironically, this curious state of affairs was partially due to Canadian Prime Minister Mackenzie King's efforts to limit Canada's role in the war by focusing upon an air contribution. Remembering the First World War's horrific toll of lives—and the divisive conscription crisis—at the outbreak of war, King was clearly hoping to avoid a major commitment of manpower-intensive ground troops to the European continent.[72] Yet at the same time, he was under pressure to make a substantial contribution to the war effort. King's solution was what became known as the British Commonwealth Air Training Plan (BCATP), a massive programme to train young men from around the Commonwealth as aircrew.[73] King intended this to be Canada's major contribution to the war and stressed this in the public announcement of the new plan that he made in December of 1939: "The United Kingdom Government has informed us that … the Plan … would provide for more effective assistance … than any other form of military cooperation which Canada can give."[74]

As C. P. Stacey concludes, King's intention was that the Canadian war effort should centre on the BCATP, rather than a large army contingent with all the prospects of casualties which that would raise.[75]

However, the personnel trained in the BCATP were to be fed into the RAF machine once they were ready for duty. Air power was not to be divided—there would be no truly separate Commonwealth air forces in Britain, merely the RAF. Recognizing this, Article Fifteen of the BCATP pledged that "the United Kingdom Government undertakes that pupils of Canada, Australia and New Zealand shall, after training, … be identified with their respective Dominions, either by … organizing Dominion units or in some other way."[76]

King was unsatisfied with this weak pledge, and a subsequent agreement was reached stating that:

> the United Kingdom accepts in principle as being consonant with the intention of Paragraph 15 of the Memorandum of Agreement that the United Kingdom Government, on the request of the Canadian Government, would arrange that Canadian pupils when passing out from the training scheme will be incorporated in or organized as units of the Royal Canadian Air Force in the field.[77]

On 7 January 1941, a supplementary agreement was reached stipulating that 25 RCAF squadrons would be established in Great Britain in this manner, and these became known as "Article 15" squadrons.[78]

Despite these intentions, the reality on the ground was not nearly so clear cut. First of all, while the BCATP was providing the aircrew, because of its tiny pre-war size, the RCAF lacked—at least initially—sufficient numbers of experienced officers to fill the command and staff billets needed to form RCAF squadrons and formations.[79] But even more seriously, while most of the aircrew were indeed Canadians graduated from the BCATP, most of the ground crew in the Article 15 squadrons remained British.[80]

Furthermore, the equipping and operating expenses of these squadrons were coming from the British government. Finally, and even more telling, there was no separate chain of command for Dominion air units. The RAF was organized into what were known as "commands"[81]—which were functional—and below that level they were grouped geographically. This allowed for the immediate concentration of all available air power, under radar-directed radio control, as necessary. This was, of course, the system that had famously won the Battle of Britain, and it reflected the flexibility of air power and the cardinal tenet of air doctrine that control of air power should be centralized to permit concentration of force. So, the RAF considered it impossible to form an RCAF "separate" from the RAF the way the Canadian Army was separate from the British Army.[82] Indeed, the only thing Canadian about many of the Article 15 RCAF squadrons was the aircrew. Similarly, many RCAF personnel were posted throughout the RAF in "non-RCAF" units and positions. Canada did not even control the postings of RCAF personnel, they simply went into the general RAF pool, for posting as necessary—although the British Air Ministry was supposed to respect the spirit of the agreement reached between Mackenzie King and London.[83] Further confusing the situation were units such as No. 242 "All Canadian" Squadron, which was an RAF (not RCAF) unit but which the RAF filled with all Canadian aircrew (but not ground crew). In sum, outside of Canada, there was not really any such institutional entity as the RCAF; there was simply a large number of RCAF personnel employed within the RAF.

This state of affairs quickly became a bone of contention between Canada and the British government, as the Canadian government could not even be sure where all its volunteer citizen airmen were posted within the RAF, nor even—in at least a few instances—whether they had become casualties. On 23 June 1941, Canada's Minister of National Defence for Air, C. G. "Chubby" Power, wrote to Mackenzie King to express his concerns about the situation:

> There are today in Great Britain, and probably spread elsewhere throughout the war zone, well over five thousand of our young Canadian men, members of the RCAF, who are our moral, if not the legal responsibility of the Canadian Government. …
>
> … we cannot … completely divest ourselves of the duty which we owe to the Canadian people and to the parents of these boys … .[84]

In light of these concerns, in July 1941, Mr. Power and the Canadian Chief of the Air Staff went to the UK for a tour of RCAF facilities and discussions with the British, where they voiced their concerns. The British did not receive their message warmly. Fully absorbed with fighting a total war, they looked upon the Canadian demands as parochial. Britain's Undersecretary of State for Air, Harold Balfour, acknowledged the "national demand in Canada for the close affiliation of RCAF personnel," but he wondered how this could be effected given the RAF's single "channel of direct command."[85] Postings and promotions had to be "treated as a whole throughout the personnel serving with the Royal Air Force … it was undesirable that there should be watertight compartments dealing with postings of personnel for a particular Dominion or Allied country."[86]

These concerns led to the campaign which came to be known as "Canadianization," and promoting this campaign came to be the major task of the RCAF Overseas Headquarters. In November of 1941, A/V/M Edwards was posted in to command the Overseas Headquarters with this very mandate, and he tirelessly pursued it, lobbying (unsuccessfully) for a seat on the Air Council and for influence over not just personnel matters but also consultation on operational matters affecting Canadian units. It was an uphill battle, and in the spring of 1942, he remarked in a letter, "as far as my own position is concerned, in spots it is ludicrous. … [I am] tired of breaking [my] way in, with the consequent nuisance and unpopularity."[87]

Photo: DND

403 Squadron, formed on March 1, 1941, was the first RCAF 400-series squadron formed overseas as a direct result of Article 15 of the British Commonwealth Air Training Plan.

Outflanked: The Creation of 2nd Tactical Air Force

Even while McNaughton and Edwards were being frustrated in their lobbying efforts for a robust all-Canadian army-air force, the larger British land-air doctrinal debate was reaching its conclusion. Despite the RAF's traditional bias against tactical air power, experience was beginning to tell. In neglected Army Co-operation Command of the RAF, in the far backwater of Northern Ireland, a small group of officers had been brought together under the leadership of Group Captain Wann of the RAF and Brigadier Woodall of the British Army. Veterans of the debacle in France, both were determined to create a better tactical air power system. They produced what came to be called the "Wann/Woodall" report, which outlined a system of control for air support that formed the basis of the eventual tactical air force (TAF) doctrine. The essentials of the Wann/Woodall system were the establishment of a joint Army/RAF headquarters which would control a composite group of aircraft and the creation of a radio network outside of the normal Army chain of command, specifically for the purpose of controlling air support.[88]

Also just at this time, a major technological development occurred, essentially by coincidence. Languishing somewhat since its glory days in the Battle of Britain, Fighter Command was casting about for an offensive role. Apparently on his own initiative, the commander of No. 11 Group, Air Marshal Trafford Leigh-Mallory, began experiments in the modification of fighters to carry bombs and attack ground targets.[89] Thus the "fighter-bomber" was born, ironically by a process completely unrelated to the Army's (much less McNaughton's) long and persistent demands for effective air support.

The first implementation of these new ideas—the Wann/Woodall system and the fighter-bomber concept—came in the Western Desert, far from the doctrinal squabbling at Whitehall, and achieved considerable success. In Britain, however, acrimony between the RAF and Army remained fierce, and by October 1942, the debate had escalated to the level of Churchill himself. On 7 October 1942, he produced a compromise slightly favourable to the RAF.

> Above all, the idea of keeping standing patrols [of aircraft] over [Army] columns should be abandoned. It is unsound to distribute aircraft in this way. ... The Army Commander-in-Chief will specify to the Air Officer Commanding-in-Chief the targets and tasks which he requires to be performed. … It will be for the Air Officer Commanding-in-Chief to use his maximum force for those objects in the manner most effective.[90]

Churchill's ruling settled the debate, and Brooke reluctantly conceded to the dissolution of Army Co-operation Command and the establishment of a new TAF within Fighter Command of the RAF, rather than as part of the Army.[91]

In this environment, with it having become policy to form strong tactical air forces to cooperate with the land armies, McNaughton and Edwards continued working together to lobby for their vision of a joint all-Canadian army-tactical air force spearhead force. By that time, McNaughton was lobbying for the creation of not just an army co-operation wing (three squadrons) but also a composite group of fighters and ground-attack aircraft to work with his 1st Canadian Army. A/V/M Edwards had begun lobbying from his end for such an organization in February 1943. However, this proposal was wrecked on the shoals of the Canadianization debate. The Director Policy at the Air Ministry in London advised that:

> As regards the Canadian Composite Group, I think we should discourage this proposal since the segregation of Dominion Air Forces into such a Group would inevitably destroy some of its flexibility for employment.

> … There would also be the natural tendency to demand that a Canadian Composite Group, if formed, should be employed in the same operational area in which Canadian land troops are located. This might prove a further embarrassment.[92]

As it turned out, McNaughton's and Edward's scheming for a Canadian composite group was overtaken by events. Given the success of the tactical air force that had been formed in North Africa (what was known as the Desert Air Force or DAF), it was decided to form another tactical air force, modeled on the DAF, which would be known as the 2nd Tactical Air Force, or 2 TAF.[93]

2 TAF was to consist of four groups, No. 2 Group (light bombers), No. 83 and No. 84 Composite Groups, (fighter-bombers, for both air superiority and ground attack) and No. 85 Group (air defence and night fighters).[94] Most of the RCAF units allocated to 2 TAF were in No. 83 Composite Group, where they comprised 14 out of 28 squadrons. Originally, it had been intended that this group would support 1st Canadian Army, while No. 84 Group (which was comprised mainly of British squadrons) would support 2nd British Army.[95] It should be noted that this worked out to a ratio of almost four squadrons per division—roughly the ratio McNaughton had called for earlier and which the British had so peremptorily dismissed as unrealistic.

However, this fulfilment of McNaughton's dream of a national Canadian air force working hand in glove with a national Canadian army was not to be. In December of 1943, McNaughton was removed from command of 1st Canadian Army,[96] and shortly thereafter, it was decided that 83 Group—notwithstanding its heavy RCAF composition—would support 2nd British Army and that 1st Canadian Army would be supported by 84 Group. The reason for this was eminently sound—83 Group was the more experienced formation. The 2nd British Army would be responsible for the perilous assault landing on D-Day, so it was decided to place the more experienced group in their support.[97] Prudent as that clearly was, indeed flattering for the RCAF, it nevertheless scuppered the possibility of any sort of all-Canadian national contingent for the Western Allies' decisive campaign of the war.

Consideration: The Limits on a Junior Alliance Partner

As tactical air power evolved, Canada was never in the driver's seat. As we have seen, the larger debates over the organization and role of tactical air power were played out between the highest levels of the RAF and the British Army, ultimately rising for adjudication to the very highest level possible—Prime Minister Churchill. The ideas and arguments of a Canadian general were not a factor. There is something of an irony in this: the final establishment of the composite groups that directly supported the field armies was approximately 30 squadrons, or about five per division—almost exactly the level of air support that McNaughton had first envisioned and that had been so peremptorily dismissed as unrealistic.

It has been widely observed that, as a junior alliance partner, during the Second World War Canada left strategic thought to others, in particular the British, focusing instead upon raising forces that would be sent off to join the fight.[98] But while Canadian policy may have been thus focused upon raising forces, this leaves open the question of the doctrinal structure and practice of those forces, and it was in this area that McNaughton was trying to be innovative. In this regard, his efforts reflected a heritage that was for him very personal—the Canadian Corps in the First World War. While the Canadian Army began that war with standard British doctrine, they developed it from there, and by 1918, the Canadian Corps was markedly different in certain key respects from the British model.[99] It had a different structure, and in particular, its organization and employment of machine guns were "a year ahead of all other armies" and were recognized as such by the British.[100] It was this heritage of innovation that McNaughton was striving for.

In contrast to the recognized success that Canadian innovation achieved in the First World War, in the Second, McNaughton was unsuccessful at realizing a unique vision. The reasons for this, as we have seen, were many and varied—the allocation of scarce resources; the complexity of the issues involved; the level at which they were resolved; and with regard to McNaughton's "all Canadian" vision, the fact that the command of land and air forces was centralized at a far higher level than that at which the Canadian commanders worked. This remains a fundamental tension between Canadian joint and combined operations to this day: Canadian land forces sent to a theatre of operations become part of the land component within that theatre, while Canadian air forces sent to the same theatre become part of the air component within the theatre. Therefore, the air component is not necessarily directly associated with the Canadian land component.[101] It was this issue more than any other that frustrated McNaughton and Edward's Canadianization efforts. It remains true to this day that Canada contributes forces to campaigns led by others, something the current Chief of the Defence staff once referred to as "contribution warfare."[102] The ability of junior alliance partners to be different and unique remains a vexed challenge.

Conclusion

The development of tactical air power from the First World War to the North West Europe campaign was a long, complex and contentious process. Despite having begun life with a strong experience of tactical air power in the First World War, the RAF turned away from this heritage and only returned to a strong investment in the tactical air power role after some heated debate with the British Army. Canada was not a significant player in this debate, which ultimately rose beyond the level of the service chiefs to Prime Minister Churchill, himself, for adjudication. However, one Canadian officer, in particular, exerted strong efforts to achieve, at least within the Canadian contingent, a unique vision for tactical air power—Lieutenant-General Andrew McNaughton.[103]

As we have seen, McNaughton was a keen proponent of tactical air power from as far back as the early 1930s, probably due to his technocratic nature and restive intellectual energies. Upon mobilization in 1939, he consistently fought for stronger tactical air forces assigned to his command, far stronger tactical air forces than standard British doctrine originally called for. Further, he wanted those tactical air forces to be RCAF squadrons, thus forming an "all Canadian" joint land-air team that would constitute the spearhead of the British forces, just as the Canadian Corps had in the First World War. McNaughton's efforts in this regard were remarkable, extending to not just persistent requests and lobbying but also creative efforts, such as the use of his own army-engineer assets to build his own airfield.

However, in the end, McNaughton's efforts were unsuccessful. He did not convince the authorities to grant him larger tactical air forces, and when strong tactical air forces were eventually assigned to the support of 1st Canadian Army for Operation OVERLORD, this development resulted not from McNaughton's efforts but from the larger overall redesign of all tactical air power. In the end, while 1st Canadian Army wound up with a scale of tactical air power almost exactly that which McNaughton had originally called for in the face of British opposition, this was exactly the same amount of tactical air support as 2nd British Army was allocated—one composite group (roughly two dozen squadrons). Nor was McNaughton's "all Canadian" vision realized, as the centralized command structure of the tactical air forces, and various exigent factors of the campaign, resulted in the RCAF squadrons working with 2nd British Army, while 1st Canadian

Army received its air support from a predominantly British group. This serves as something of a cautionary tale as to the limits on the originality open to a junior partner in a grand alliance.

Lieutenant-Colonel Paul Johnston is an RCAF intelligence officer, currently employed as the A2 of 1 Canadian Air Division in Winnipeg. Lieutenant-Colonel Johnston's career has ranged from tactical positions in the fighter community, to operational-level headquarters, to the strategic level in Ottawa. His most recent deployment was as the Chief Assessments Officer of the Joint Intelligence Centre at International Security Assistance Force (ISAF) Headquarters in Kabul. Lieutenant-Colonel Johnston is also a doctoral student at Queen's University in the history programme; his area of research interest is the evolution of tactical air power within the North Atlantic Treaty Organization.

Abbreviations

A/V/M	air vice-marshal
AC	Army Co-operation
AEAF	Allied Expeditionary Air Forces
BCATP	British Commonwealth Air Training Plan
BEF	British Expeditionary Force
CAS	close air support
CGS	Chief of the General Staff
DAF	Desert Air Force
DHH	Directorate of History and Heritage
RAF	Royal Air Force
RCAF	Royal Canadian Air Force
RFC	Royal Flying Corps
TAF	tactical air force / Tactical Air Force
TNA	The UK National Archives
UK	United Kingdom
US	United States

Notes

1. Most of the occupants of the staff car were killed outright, but Rommel himself survived. He was medically evacuated and never resumed command of Army Group B. Still recovering from his wounds, he was implicated in the July bomb plot against Hitler. Offered the choice between a public trial or private suicide, he opted for the latter and was buried with full military honours.

2. Debate about exactly which Allied fighter-bombers strafed Rommel's staff car has long been heated, but Fox now seems the most likely candidate. See "Who Shot Rommel? A New Look at the Evidence," Reginald Byron, Tangmere Military Aviation Museum, accessed August 4, 2016, http://www.tangmere-museum.org.uk/articles/who-shot-rommel. For more about Charley Fox, see William W. Beatty, Glenn Dean and Peter Yip, "Honorary Colonel Charley Fox: An American Perspective," *The Canadian Air Force Journal* 2, no. 1 (Winter 2009), accessed August 4, 2016, http://airforceapp.forces.gc.ca/CFAWC/eLibrary/Journal/Vol2-2009/Iss1-Winter/AF_JOURNAL-Vol2-2009-Iss1-Winter_e.pdf

[3] The most recent book-length scholarly study of this is David Hall, *Strategy for Victory: The Development of British Tactical Air Power, 1919–1943* (Westport, CT: Praeger, 2008). See also Paul Johnston, "The Question of British Influence on US Tactical Air Power in World War II," *Air Power History* (Spring 2005); and Paul Johnston, "Tactical Air Power Controversies in Normandy: A Question of Doctrine," *Canadian Military History* 9, no. 2 (Spring 2000).

[4] Canada provided 18 squadrons to the Allied Expeditionary Air Forces (AEAF) total of 225 on D-Day, from a population of about 12 million, approximately 1.5 squadrons per million populace. The United States (US) provided a whopping 68 per cent of the AEAF (130 squadrons), but with a population of about 130 million, that represented only about one squadron per million populace. On a per capita basis, Canada thus provided almost a third more tactical air forces to the AEAF than the US.

[5] Thus conceived, tactical air power includes more than just close air support (CAS), which is specifically defined as air attack on targets in close proximity with one's own ground forces, whereas tactical air power is broader in conception and includes attack on targets important to opposing ground forces through the full operational depth of the theatre—not merely those targets which are close. In contemporary terms, tactical air power includes air interdiction (AI) as well as CAS. This "tactical" role is usually contrasted with the "strategic" bombing of targets (often cities) not directly associated with enemy ground forces.

[6] For excellent summary histories, see Lee Kennett, *The First Air War, 1914–1918* (New York: Free Press, 1991); and Williamson Murray, *War in the Air 1914–45* (London: Cassell, 1999). For more of a focus upon the ground-attack role, see Richard Hallion, *Strike from the Sky: The History of Battlefield Air Attack, 1911–1945* (Tuscaloosa, AB: The University of Alabama Press, 2010, originally published 1989). The most recent scholarly study is Hall's *Strategy for Victory.*

[7] [UK] War Office, *Field Service Regulations*, Part I *Operations 1914* (London: His Majesty's Stationary Office, 1914), 21.

[8] Kennett, *First Air War*, 48.

[9] For excellent summary histories, see Kennett, *First Air War*; and Murray, *War in the Air*, Chapter 1.

[10] S. F. Wise, *The Official History of the Royal Canadian Air Force*, vol. 1, *Canadian Airmen and the First World War* (Ottawa: Canadian Government Publishing Centre, 1980), 411.

[11] Ibid., 528.

[12] Ibid., 570.

[13] Brereton Greenhous et al., *The Crucible of War, 1939–1945*, vol. 3, *The Official History of the Royal Canadian Air Force* (Toronto: University of Toronto Press, 1994), 172.

[14] Maurice Pope, *Soldiers and Politicians: The Memoirs of Lieutenant-General Maurice A. Pope* (Toronto: University of Toronto Press, 1962), 53.

[15] Barry Powers, *Strategy Without Slide-Rule* (London: Croom Helm, 1976), 167.

[16] John Slessor (then a wing commander), *Air Power and Armies* (London: Oxford University Press, 1936).

17. Ibid., 90.

18. Ibid., 90–92.

19. Ibid., 3.

20. James Eayrs, *In Defence of Canada: From the Great War to the Great Depression* (Toronto: University of Toronto Press, 1965), 258.

21. For McNaughton's biography, see the now somewhat dated John Swettenham, *McNaughton*, vols. 1, 2 and 3 (Toronto: Ryerson Press, 1968, 1969). More recently, there has been a chapter in Jack Granatstein, *The Generals: The Canadian Army's Senior Commanders in the Second World War* (Toronto: Stoddart, 1993) and the excellent new study by John Nelson Rickard, *The Politics of Command: Lieutenant-General A. G. L. McNaughton and the Canadian Army, 1939–1943* (Toronto: University of Toronto Press, 2010), Part One of which is a biography.

22. Stephen Harris discusses this in *Canadian Brass: The Making of a Professional Army, 1860–1939* (Toronto: University of Toronto Press, 1988), 206–207 and 210–211, as does Granatstein in *The Generals*, Chapter 3 and John A. English, *The Canadian Army and the Normandy Campaign: A Study of Failure in High Command* (Westport, CT: Praeger, 1991), 42–47.

23. Tony Foster, *Meeting of Generals* (Toronto: Meuthen & Co. Ltd, 1986), 165.

24. Charles Carrington, *Soldier at Bomber Command* (London: Leo Cooper, 1987), 36.

25. Major-General A. G. L. McNaughton, "The Progress of Air Survey in Canada," *Canadian Defence Quarterly* 14, no. 3 (April 1937): 311–16.

26. Greenhous et al., *Crucible of War*, 172.

27. At the time, the RCAF reported to the Army CGS, i.e., McNaughton.

28. Harris, *Canadian Brass*, 179–86; and Eayrs, *Defence of Canada*, 83–85.

29. Mathias Joost, "McNaughton's Air Force: The Creation of the First Non-Permanent Active Air Force Squadrons, 1931–1933" (master's thesis, Royal Military College, 2008), in particular 6, 141–42, 147 and 153.

30· Greenhous et al., *Crucible of War*, 323.

31· Ibid.

32· H. Montgomery Hyde, *British Air Policy Between the Wars* (London: Heinemann, 1976), 408–10.

33. Ibid., 324.

34. Note by D Plans [Directorate Plans], "Services Required from the RAF for the Field Force," May 1939, The UK National Archives (TNA) AIR 8/272, quoted in Malcolm Smith, *British Air Strategy Between the Wars* (Oxford: Oxford University Press, 1984), 91.

35· Ibid., 322–23.

36. W. A. Jacobs, "Air Support for the British Army, 1939–1943," *Military Affairs* 46, no. 4 (December 1982): 175.

37. Ibid., 326. It should be noted that equipped as they were with Lysander aircraft, the Army Co-operation squadrons were not expected to do anything beyond reconnaissance and liaison.

38. Ibid.

39. TNA CAB 80/58, The Air Program, 21 May 40, quoted in David Syrett, "The Tunisian Campaign, 1942–43" in *Case Studies in the Development of Close Air Support*, ed. B. F. Cooling (Washington: Office of Air Force History, 1990), 158.

40. Ibid.

41. Carrington, *Soldier at Bomber Command*, 26–27; and John Terraine, *The Right of the Line: The Royal Air Force in the European War, 1939–1945* (London: Hodder & Stoughton, 1985), 350–51.

42. Charles Carrington, "Army/Air Co-operation, 1939–1943," *RUSI Journal* (December 1970): 38.

43. Ibid.

44. A/V/M Slessor, memorandum "Use of Bombers in Close Support of the Army", 6 May 1941, TNA AIR 20/2970, quoted in Peter C. Smith, *Close Air Support: An Illustrated History 1914 to the Present* (New York: Orion Books, 1990), 64. When Slessor wrote this in 1941, he was once again a senior planner on the Air Staff and was perhaps the RAF's most influential thinker.

45. TNA COS(41)83(0), "The Air Programme," 21 May 1941, CAB 80/58, quoted in Jacobs, "Air Support for the British Army, 1939–1943," 175.

46. Jacobs, "Air Support for the British Army, 1939–1943," 178.

47. Ibid., 176.

48· Minutes COS(42) 155th (19 May 1942), quoted ibid.

49. "Notes for CAS," 12 September 1939, Canada, Department of National Defence, Directorate of History and Heritage (DHH) file 77/743, quoted in Greenhous et al., *Crucible of War*, 173.

50. This arrangement was agreed upon at a meeting on 24 November 1939 in London, between Canada's Chief of the Air Staff, Air Commodore L. S. Breadner; the British Secretary of State for Air Sir Kingsley Wood; Canadian High Commissioner Vincent Massey; and the RCAF's liaison officer to the RAF, Wing Commander V. Heakes. Greenhous et al., *Crucible of War*, 173.

51. This became No. 400 Squadron. Samuel Kostenuk and John Griffin, *RCAF Squadron Histories and Aircraft* (Toronto: Samuel Stevens Hakkert, 1977), 80.

52. Greenhous et al., *Crucible of War*, 173.

53. DHH 181.009 (D4791).

54. Greenhous et al., *Crucible of War*, 175.

[55] This became No. 402 Squadron, Kostenuk and Griffin, *RCAF Squadron Histories*, 84.

[56] Quoted in Greenhous et al., *Crucible of War*, 175.

[57] C. P. Stacey, *Official History of the Canadian Army in the Second World War*, vol. 1, *Six Years of War* (Ottawa: Queen's Printer, 1955), 234–35.

[58] Greenhous et al., *Crucible of War*, 176.

[59] Quoted in Swettenham, *McNaughton*, vol. 2, 42. G.O.C. is general officer commanding, i.e., the divisional commander.

[60] Greenhous et al., *Crucible of War*, 244.

[61] Ibid.

[62] "Provision of an Army Cooperation Squadron for Canadian Armoured Division," 21 May 1941, DHH, 181.009 (D4790).

[63] Greenhous et al., *Crucible of War*, 226.

[64] DHH 181.003 (D1171).

[65] Greenhous et al., *Crucible of War*, 227.

[66] Ibid.

[67] Swettenham, *McNaughton*, vol. 2, 210.

[68] Kostenuk and Griffin, *RCAF Squadron Histories*, 220.

[69] Greenhous et al., *Crucible of War*, 227.

[70] Granatstein, *The Generals*, 66–67.

[71] For an excellent overview of the spearhead role of the Canadian Corps in the final days of World War I, see Shane Schreiber, *Shock Army of the British Empire: The Canadian Corps in the Last 100 Days of the Great War* (Westport, CT: Praeger, 1997).

[72] Indeed, when defence spending finally began to rise in the late 1930s, most of the funding went to the RCAF. See Eayrs, *Defence of Canada*, 144–52.

[73] Or Empire Air Training Plan (EATP), as the British revealingly persisted in calling it.

[74] Quoted in F. J. Hatch, *Aerodrome of Democracy: Canada and the British Commonwealth Air Training Plan* (Ottawa: Directorate of History and Heritage, 1983), 23.

[75] C. P. Stacey, *Arms Men & Governments: The War Policies of Canada, 1939–1945* (Ottawa: Queen's Printer, 1970), 25.

[76] Quoted in Hatch, *Aerodrome of Democracy*, 23.

[77] Hatch, *Aerodrome of Democracy*, 25.

[78] Kostenuk and Griffin, *RCAF Squadron Histories*, 75.

79. A problem that would, of course, dog the Army too.

80. Hatch, *Aerodrome of Democracy*, 24.

81. Army Co-operation Command, Bomber Command, Coastal Command, Fighter Command, Flying Training Command and Transport Command.

82. Of course, when the US entered the war, there was never any question that the United States Army Air Forces would not be independent of the RAF's command system.

83. That the British did so only unevenly became a constant source of Anglo–Canadian friction.

84. Greenhous et al., *Crucible of War*, 44.

85. Ibid., 46.

86. Ibid., 44.

87. Quoted in Greenhous et al., *Crucible of War*, 62.

88. An official account of this is given in the originally classified report UK Air History Branch, *Air Support, The Second World War 1939–1945: Royal Air Force* (Air Ministry: Air Publication 3235, 1955). For the most recent scholarly examination, see Hall, *Strategy for Victory*, 65–67, 91–92 and 106. For a more personal account see Charles Carrington's memoir *Soldier at Bomber Command*. See also Shelford Bidwell and Dominick Graham, *Fire-Power: The British Army Weapons and Theories of War, 1904–1945* (Barnsley, UK: Pen & Sword Military Classics, 1982), 264–65; and Richard Townsend Bickers, *Air War Normandy* (London: Leo Cooper, 1994), 150–67.

89. Jacobs "Air Support for British Army, 1939–1943," 177.

90. TNA CAB 69/4, DO(41)17 (7 October 1942), cited ibid., 180; see also Churchill's own account in, *The History of the Second World War*, vol. 3, *The Grand Alliance* (London: Cassell, 1950), 443.

91. Hall, *Strategy for Victory*, 117–27; and Jacobs "Air Support for the British Army, 1939–1943," 178–81.

92. Quoted in Greenhous et al., *Crucible of War*, 256.

93. The DAF, which had meanwhile moved across to Italy with the British Eighth Army, was the 1st TAF. See Terraine, *Right of the Line*, 395–401.

94. See Terraine, *Right of the Line*; and Greenhous et al., *Crucible of War* for the orders of battle.

95. On the organization of 2 TAF, see Johnston, "Tactical Air Power Controversies in Normandy," 61–63.

96. The reasons for McNaughton's removal are still debated. John Swettenham, his biographer and proponent, claims that it was political—motivated by his courageous and principled stand against splitting 1st Canadian Army between theatres. See Swettenham, *McNaughton*, vol. 2, Chapter 10, "The Shoals of Politics." More contemporary—and more critical—historians such as Jack English and Jack Granatstein are quite firmly convinced that McNaughton was simply unfit for higher command in war and that the British had him eased out with as few ruffled feathers as possible. Certainly, he was not the only senior commander replaced by Montgomery.

See Granatstein, *The Generals*, Chapter 3, "McNaughton: The God That Failed." The chapter titles give a clear indication of Granatstein's interpretation. More recently, Rickard has argued that the reason for McNaughton's replacement boils down to personality clashes. See Rickard, *Politics of Command*, 223–29.

97. Greenhous et al., *Crucible of War*, 257.

98. Scot Robertson, "Years of Innocence and Drift: The Canadian Way of War in the Post-Cold War Era," in *The Canadian Way of War: Serving the National Interest*, ed. Bernd Horn (Toronto: Dundurn Press, 2006), 369.

99. For a survey of this development, see William Rawling, *Surviving Trench Warfare: Technology and the Canadian Corps, 1914–1918* (Toronto: University of Toronto Press, 1992); Schreiber, *Shock Army of the British Empire*; or Andrew Godefroy, "Canadian Military Effectiveness in the First World War," in *Canadian Way of War*.

100. Stephen Harris, "A Canadian Way of War," in *Canadian Way of War*. On the considerably more unoriginal performance by the Canadian Army in the Second World War, see for instance English, *The Canadian Army and the Normandy Campaign*, 308–309. To be fair, a contrary school of thought has emerged, typified by Terry Copp, and in particular his *Cinderella Army: The Canadians in Northwest Europe, 1944–1945* (Toronto: University of Toronto Press, 2006) and more recently Mark Milner, *Stopping the Panzers: The Untold Story of D-Day* (Leavenworth: University Press of Kansas, 2014). It seems fair to conclude, however, that unique Canadian innovation was markedly less in the Second World War than the First.

101. This tension has been remarked upon in various places. See for instance, F. Boomer, "Joint or Combined Doctrine?: The Right Choice for Canada" (Advanced Military Studies Course 1, Canadian Forces College, 1998) in particular pages 12 and 20; and Paul F. Wynnyk, "Jointness: The Need for the Canadian Forces to Go Farther" (Horizons Paper, Canadian Forces College, 1997). It should also be noted that helicopters, while considered air units in Canada, are normally grouped within land components.

102. J. H. Vance, "Tactics without Strategy or Why the Canadian Forces Do Not Campaign," in *The Operational Art: Canadian Perspectives, Context and Concepts*, ed. Allan English et al. (Kingston: Canadian Defence Academy Press, 2005), 281.

103. In the assessment of the authors of the RCAF official history, McNaughton's ideas on tactical air power "went deeper than those of any British general except, perhaps, Montgomery." Greenhous et al., *Crucible of War*, 244.

COUNTERING THE SMALL-UNMANNED-AIRCRAFT-SYSTEM THREAT TO THE CANADIAN ARMED FORCES

BY MAJOR DAN WALTERS, CD, MDS

Editor's note: This paper was written by a candidate attending the Canadian Forces College in fulfilment of one of the requirements of the course of studies.

AIM

The recent rapid expansion of the consumer small unmanned aircraft system (sUAS) industry has made tools that were once the exclusive purview of nation states and researchers available to almost anyone. A variety of groups has demonstrated both the capability and the intent to use this technology for malicious purposes. Hostile use of sUASs presents unique challenges to the Canadian Armed Forces (CAF) for both domestic and expeditionary operations. The aim of this article is to examine the implications of sUAS proliferation for CAF and to recommend a way ahead.

INTRODUCTION

There are two main implications of an sUAS threat to CAF. First, the North American Aerospace Defence Command (NORAD) has a standing mission under Operation NOBLE EAGLE (ONE) to protect the civilian population of North America from a terrorist air attack.[1] Second, all CAF force generators and force employers have a responsibility for force protection.[2] sUASs present several unique challenges for engagement. They are inexpensive, particularly when compared to the cost of military air-defence systems. They are able to launch when they are close to potential targets, and based on their small size and signatures, they can be difficult to detect and engage. They can be massed and used to swarm a target, overwhelming some conventional defences. Lastly, engagement with traditional kinetic defences can easily cause more collateral damage than the sUAS itself.

This article begins with defining an sUAS and discussing the threat that it can pose. It then discusses the threat posed by three categories of users: benign users, insurgents and terrorists. Next, it reviews CAF's potential defensive measures, including readiness, detection and tracking, as well as passive and active defences. Lastly, it draws conclusions and makes a recommendation for a way forward for CAF.

DEFINITION

There are varying military and civilian definitions, terminologies and categories used for unmanned aircraft, such as unmanned aerial vehicles (UAVs), remotely piloted aircraft systems (RPAS), unmanned aircraft systems (UAS) and drones. For simplicity, this article will use the Federal Aviation Administration (FAA) and Transport Canada (TC) definition of an sUAS being an unmanned aircraft that weighs less than 25 kilograms,[3] as this definition has specific implications on ease of purchase and legal use.[4] Some authors differentiate between UASs and cruise missiles based on operator intent to recover the vehicle; however, again for simplicity, this article will use the term UAS regardless of user intent.[5]

THREAT

The massive proliferation of sUASs in recent years is astounding. In 2014, the United States (US) FAA estimated that 200,000 recreational sUASs were operating in the US National Airspace System (NAS), not including those used commercially. They estimate another 1.6 million were sold in 2015 and expect 1.9 million in 2016, plus another 600,000 for commercial use.[6] The growth in Canada has been similar; in fact worldwide, there is one estimate that 200,000 sUASs per month were sold globally in 2014.[7]

As recently as 2008, threat assessments generally concluded that malicious use of UASs by terrorist organizations was unlikely, based on the technical skills required and the other available means of attack.[8] However, three important factors have changed in recent years. First, sUASs have become cheap and have proliferated widely, with very capable models available off the shelf for a few hundred dollars. Second, advances in inexpensive miniaturized autopilot systems mean that very little experience is required to effectively operate an sUAS. Third, the widespread mobile access to the Internet now allows sUASs to be controlled from a distance.[9] These changes have led several more recent academic assessments of the threat to generally agree that hostile sUASs present a realistic security threat.[10]

A French UAS hovers in front of an assembled crowd during the fourth biennial Brunei Darussalam International Defense Exhibition in Bandar Seri Begawan, Brunei, Dec. 5, 2013. (Department of Defense photo by Master Sergeant Jerome S. Tayborn, United States Air Force / Released)

BENIGN USERS

The first category of sUAS users is those that have no intention of deliberately causing physical harm to CAF personnel or civilians. This broad category includes uneducated recreational users, criminals and activists. These users may pose an actual threat, for example, by accidentally flying into the flight path of aircraft. More importantly, they often serve to highlight the vulnerabilities of vital assets to sUASs.

In 2015, the FAA received 1,133 UAS incident reports, over four times as many as were received in 2014. This included "reports of unmanned aircraft at high altitudes in congested airspace, unmanned aircraft operations near passenger-carrying aircraft or major airports, and interfering with emergency operations such as efforts to combat wildfires."[11] TC has had similar problems, launching over 50 investigations since 2010 into "reckless and negligent" UAS use.[12] An accidental crash of an sUAS on the White House lawn in January 2015 prompted a significant response in the US, including a congressional hearing on the issue.[13] Both the FAA and TC have launched education campaigns and reviews of UAS regulations. However, the trend indicates that CAF may need to protect airfields and other airspace from inadvertent entry. Prompted by similar incidents in the United Kingdom (UK), one study warned against the possibility of sUASs being used deliberately as "mechanical bird strikes."[14]

Criminal use of sUASs has also been increasing. This has included cross-border drug smuggling as well as delivering contraband weapons and drugs into prisons (including one in Quebec).[15] CAF units on stability operations may have a requirement to halt such operations without causing collateral damage.

Perhaps some of the most dramatic demonstrations of potentially hostile sUAS capability, without necessarily hostile intent, have been activist stunts. For example, in September 2013 an activist managed to fly an sUAS a few feet [approximately 1 metre] from German Chancellor Angela Merkel at a press conference.[16] A string of sUAS sightings in France in 2014–2015 around nuclear plants, a submarine base, the Eiffel Tower, the US embassy in Paris and the Charlie Hebdo offices has prompted the French government to adopt countermeasures.[17] On three occasions in 2015, sUASs, whose operators were not located, were able to fly close to President Obama.[18] In April 2015, an activist landed a small radioactive package on the roof of the Japanese Prime Minister's office.[19] These incidents, while not necessarily hostile, highlight the vulnerability of some of the world's best protected people and sites to sUASs.

INSURGENTS

Perhaps the most acute threat sUASs pose to CAF units deployed abroad is from insurgents. Both insurgents and terrorists can use sUASs for two primary missions: intelligence, surveillance and reconnaissance (ISR) as well as attack. Hamas and Hezbollah both have long histories of using UASs, including some military models supplied by Iran.[20] Initially mostly used for reconnaissance, several incidents have shown a shift to using UASs for attacks, such as the July 2006 attack on an Israeli warship and the September 2014 attack on a Syrian rebel base.[21] sUASs continue to play a significant role for both sides of the conflict in the Ukraine, primarily for ISR, including for artillery spotting.[22] The Islamic State of Iraq and the Levant (ISIL) has also been using sUASs on the battlefield. There are several reports of ISIL using sUASs for reconnaissance, such as prior to their successful attack on Syria's Tabqa air base.[23] There has also been one report of ISIL attempting to use an sUAS as an airborne improvised explosive device.[24]

TERRORISTS

To date, no terrorist plan to use an sUAS has been successful. Several terrorists considered the use of remote control aircraft, including members of Aum Shinrikyo in the 1995 sarin gas attack in Tokyo, Osama Bin Laden in a 2001 plot to kill US President George W. Bush, and al-Qaeda member Christopher Paul in his 2008 plot to attack targets in the US and Europe.[25] Perhaps the first credible attempt was by an al-Qaeda affiliate, Rezwan Ferdaus, in September 2011. He had planned to fly three model aircraft, guided by a global positioning system (GPS) and loaded with C4 explosive into the Pentagon and Capitol Building.[26] Another al-Qaeda attack using a remote-controlled aircraft in Spain was foiled in August 2012.[27] Two plots to use unmanned aircraft were foiled in Germany in 2013, the first a terrorist attack in June and the second a political assassination in September.[28]

Subsequent to these events, concerns related to sUAS terrorism have been raised by several law enforcement agencies worldwide, including New York City's police department, British counter-terrorism police, the Department of Homeland Security and the Royal Canadian Mounted Police.[29] In July 2015, British counterterrorism officials warned that ISIL has been planning a terror attack using a "multi-drone attack on large numbers of people in a synchronised attack."[30] Clearly, the potential for sUASs to be used maliciously against civilian targets in North America and against CAF assets is a real concern that must be addressed.

DEFENSIVE MEASURES

Prior to discussing specifics of possible counter-sUAS defensive measures, it is important to note that CAF will need to coordinate its efforts with allies and other government agencies, particularly for domestic force protection and the ONE mission. In particular, plans and responsibilities will need to be synchronized with TC, Industry Canada and Public Safety Canada. It is also necessary to highlight that since the retirement of the air defence anti-tank system (ADATS), the Canadian Army has no air-defence systems.[31]

Readiness

As with any threat, a critical component of defence is readiness. This includes keeping abreast of the latest technology as well as tactics, techniques and procedures (TTP) for countering a threat. To this end, the US regularly runs a counter-UAS technology exercise called BLACK DART and a counter-UAS TTP exercise called BLUE KNIGHT.[32] Australia also plans to host an annual counter-UAS exercise, as a result of the limited participation allowed by the US exercises.[33]

sUASs present a challenge to standard detection and tracking systems, especially radar, since they typically have very small radar cross sections. They are often mistaken by display filters as birds.[34]

Detection and Tracking

sUASs present a challenge to standard detection and tracking systems, especially radar, since they typically have very small radar cross sections. They are often mistaken by display filters as birds.[34] However, specialized radar systems are available, in particular as part of integrated sUAS defence systems such as the British built Anti-UAV Defence System (AUDS), the SRC LSTAR radars, the CACI SkyTracker and the Airbus Counter-UAV System.[35] The British government deployed LSTAR radars for the 2012 London Olympics, the 2013 G8 Summit and the 2014 North Atlantic Treaty Organization Summit.[36] They plan to deploy the AUDS to major public events in the future.[37] The FAA signed an agreement in 2015 to test SkyTracker's ability to protect airports from sUAS incursions.[38]

In addition to modified radars, most of the integrated sUAS defence systems incorporate a combination of passive radio frequency (RF), electro-optical, infrared and acoustic methods for detection and tracking. Several other systems employ these methods without radar, including Dedrone, Domestic Drone Countermeasures and DroneShield.[39] Typically, the passive RF systems are able to detect both the sUAS and the operator.[40] Droneshield's acoustic detection system was deployed for the 2015 Boston Marathon.[41] Of course, human observers remain one of the most effective measures, particularly in congested areas.

Passive Defences

Some of the most effective defences against an sUAS threat are also the simplest and cheapest. These can include camouflage and concealment, static nets and simply being indoors.[42] One effective passive defence for unskilled sUAS users is manufacturer imposed geofencing. Geofencing involves an sUAS manufacturer building automatic limitations on vehicle use based on GPS position, such as not allowing it to take off or forcing it to land. DJI, one of the main consumer sUAS makers, has implemented geofencing in its products around 10,000 North American airports and around Washington, District of Columbia.[43] The FAA's future plans for control of sUASs in the NAS include the possible use of dynamic geofencing, for example around active wildfires.[44]

Active Defences

Several different types of active defences against sUASs have been developed. Some of the more traditional military solutions, such as Lockheed Martin's Extended Area Protection and Survivability (EAPS) Counter Rocket Artillery Mortar (C-RAM) weapon or the Israeli Iron Dome are expensive and have the potential to cause more collateral damage than an sUAS itself.[45] The EAPS C-RAM, for example, launches a 10 pound [4.5 kilogram] interceptor that costs $16,000 per round.[46]

Directed energy weapons have also been proposed for counter-UAS systems, such as the Rafael Iron Beam, the United States Navy Laser Weapon System, the Boeing High Energy Laser Mobile Demonstrator and an unnamed Chinese system.[47]

A much cheaper alternative to these systems is to use small arms. Snipers can be effective against sUASs, but shots can be challenging and collateral damage remains a concern.[48] Shotguns, on the other hand, have proven to be very effective.[49] According to some experts, a shotgun loaded with birdshot would cause very little collateral damage due to the low terminal velocity of the small grains.[50]

Net guns have been proposed as another low-collateral-damage option. Droneshield deployed net guns as part of their defensive system for the 2015 Boston Marathon.[51] Similar systems can be mounted on sUASs in order to function as interceptors. Some examples of this include the MALOU net-carrying interceptors, the Rapere wire-dangling sUAS and the Delft Dynamics sUAS-mounted net gun.[52] France and Japan have already deployed net-carrying interceptors, while South Korea is actively researching the technology.[53]

Jamming RF signals is currently the most widely accepted solution for protecting assets where collateral damage is a concern.

An unconventional means to counter sUASs is to train and equip hawks or eagles for the task. The Dutch National Police recently announced that they are pursuing this tactic.[54] Hacking presents another possible defence, particularly for countering off-the-shelf sUASs. Several experts have demonstrated the ability to seize control of an sUAS.[55] Some have even used malware to have one sUAS take over others, who in turn take over other vehicles.[56]

Jamming RF signals is currently the most widely accepted solution for protecting assets where collateral damage is a concern. Most of the integrated defence systems—such as AUDS and Skytracker—employ RF jamming.[57] This will often either freeze the sUAS or cause it to crash. These systems are also mostly highly directional, minimizing collateral jamming effects. RF jamming also has the potential to be effective against large swarms of sUASs.[58] As an alternative to larger, more expensive systems, Battelle's DroneDefender RF jamming system is about the size of a rifle and claims to jam control, detonation and GPS signals.[59]

The variety of counter-sUAS defences available to CAF comes in a broad range of costs and with different levels of effectiveness in different environments. The correct mix of equipment to defend the wide array of assets for which CAF is responsible will likely require an equally wide range of equipment, with costs proportionate to the value of assets and the threat posed to them.

CONCLUSION

The probability of CAF encountering malicious sUAS users is ever increasing. Both for the ONE mission and for force protection, CAF has a responsibility to consider this threat and how to counter it. There are clearly many options for defence, with widely varying costs, target effects and collateral-damage concerns. These options must be considered in the context of the operating environment and closely coordinated with our allies and other government agencies.

Prior to implementing countermeasures, it is vital that CAF first consider what it needs to defend then conduct a risk analysis. The result should be a tiered defence strategy with simple, inexpensive measures for lower-value, lower-risk assets and more robust measures for vital, high-risk assets.

RECOMMENDATION

CAF should conduct a thorough risk analysis of the threat posed by hostile sUASs in the contexts of the ONE mission and force protection and should develop an integrated, coherent and tiered strategy for sUAS defence.

Major Walters, a pilot with 1,800 hours on the CF188, has spent tours at 409 Tactical Fighter Squadron, 410 Tactical Fighter (Operational Training) Squadron and 4 Wing Operations. He is currently serving at NORAD headquarters in Colorado Springs.

ABBREVIATIONS

AUDS	Anti-UAV Defence System
CAF	Canadian Armed Forces
CARAC	Canadian Aviation Regulations Advisory Council
C-RAM	Counter Rocket Artillery Mortar
EAPS	Extended Area Protection and Survivability
FAA	Federal Aviation Administration
GPS	global positioning system
ISIL	Islamic State of Iraq and the Levant
ISR	intelligence, surveillance and reconnaissance
NAS	National Airspace System
NORAD	North American Aerospace Defence Command
ONE	Operation NOBLE EAGLE
RF	radio frequency
sUAS	small unmanned aircraft system
TC	Transport Canada
TTP	tactics, techniques and procedures
UAS	unmanned aircraft systems
UAV	unmanned aerial vehicles
UK	United Kingdom
US	United States

NOTES

1. "Canadian NORAD Region," North American Aerospace Defense Command, accessed August 18, 2016, http://www.norad.mil/AboutNORAD/CanadianNORADRegion.aspx.

2. Canada, Department of National Defence, B-GJ-005-314/FP-000, Canadian Forces Joint Publication 3-13, *CF Joint Force Protection Doctrine* (Ottawa: DND Canada, 2006), 1-3.

3. Note, this is only the weight of the unmanned aircraft; it does not include all of the associated systems.

4. United States Congress, *Public Law 112-95: FAA Modernization and Reform Act of 2012* (Washington, DC: U.S. Government Publishing Office, 14 February 2012), 126 Stat. 72, accessed August 18, 2016, https://www.gpo.gov/fdsys/pkg/PLAW-112publ95/pdf/PLAW-112publ95.pdf; and Canada, TC, Canadian Aviation Regulations Advisory Council (CARAC), "Notice of Proposed Amendment (NPA): Unmanned Air Vehicles" (Ottawa: TC, May 28, 2015), 9 and 12, accessed August 18, 2016, http://wwwapps.tc.gc.ca/Saf-Sec-Sur/2/NPA-APM/doc.aspx?id=10294.

5. Dennis Gormley, "UAVs and Cruise Missiles as Possible Terrorist Weapons," in *New Challenges in Missile Proliferation, Missile Defense, and Space Security*, ed. James Clay Moltz (Monterey: Monterey Institute of International Studies, Center for Nonproliferation Studies, Occasional Paper 12, 2003), 3; and Lynn E. Davis et al., "Armed and Dangerous? UAVs and U.S. Security" (Santa Monica: RAND Corporation, 2014), 4, accessed August 18, 2016, http://www.rand.org/pubs/research_reports/RR449.html.

6. US, Department of Transportation, "Registration and Marking Requirements for Small Unmanned Aircraft; Final Rule," *Federal Register* 80, no. 241 (Washington, DC: U.S. Government Publishing Office, 16 December 2015), 78597–78598, accessed August 18, 2016, https://www.gpo.gov/fdsys/pkg/FR-2015-12-16/pdf/2015-31750.pdf.

7. Canada, TC, CARAC, "Notice of Proposed Amendment (NPA)," 2; and Barbara Booth, "Is It Time to Buy Your Kid a Drone for Christmas?" *CNBC*, December 22, 2014, accessed August 18, 2016, http://www.cnbc.com/2014/12/22/kids-and-drones-booth-change-the-world-ec-141218.html.

8. Gormley, "UAVs and Cruise Missiles"; and B. A. Jackson et al., *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles* (Santa Monica: RAND Corporation, 2008), 69, accessed August 18, 2016, http://www.rand.org/pubs/monographs/MG626.html.

9. David L. Chandler, "Using a Phone to Fly a Drone: Pilotless Planes at MIT Controlled via iPhones in Seattle," *MIT News*, November 8, 2012, accessed August 18, 2016, http://news.mit.edu/2011/iphone-drone-control-1108.

10. C. Abbott et al., "Hostile Drones: Supplementary Risk Assessment" (London: Open Briefing, January 12, 2016), 1, accessed August 18, 2016, http://www.openbriefing.org/think-tank/publications/hostile-drones-supplementary-risk-assessment/; Ryan J. Wallace and Jon M. Loffi, "Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis," *International Journal of Aviation, Aeronautics, and Aerospace* 2, no. 4 (October 2015): 24, accessed August 18, 2016, http://commons.erau.edu/cgi/viewcontent.cgi?article=1084&context=ijaaa; Bryan Card, "The Commercialization of UAVs: How Terrorists Will Be Able to Utilize UAVs to Attack the United States" (University of Texas at El Paso, 2014), 1; University of Birmingham,

Birmingham Policy Commission, *The Security Impact of Drones: Challenges and Opportunities for the UK* (Birmingham: University of Birmingham, October 2014), 74–75, accessed August 18, 2016, http://www.birmingham.ac.uk/Documents/research/policycommission/remote-warfare/final-report-october-2014.pdf; and Davis et al., "Armed and Dangerous?," 1.

11. US, Department of Transportation, "Registration and Marking Requirements," 78597.

12. Canada, TC, CARAC, "Notice of Proposed Amendment (NPA)," 3.

13. US, House of Representatives, Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency, "Unmanned Aerial System Threats: Exploring Security Implications and Mitigation Technologies: Statement of Subcommittee Chairman Scott Perry," March 18, 2015, accessed August 18, 2016, https://homeland.house.gov/files/documents/3-18-15-Perry-Open.pdf.

14. University of Birmingham, Birmingham Policy Commission, *Security Impact of Drones*, 75.

15. Marc Goodman, "Criminals and Terrorists Can Fly Drones Too," *Time*, January 31, 2013, accessed August 18, 2016, http://ideas.time.com/2013/01/31/criminals-and-terrorists-can-fly-drones-too/; Brian Anderson, "How Drones Help Smuggle Drugs Into Prison," *Motherboard*, March 10, 2014, accessed August 18, 2016, http://motherboard.vice.com/read/how-drones-help-smuggle-drugs-into-prison; and "Domestic Drone Threats," Dan Gettinger, Center for the Study of the Drone at Bard College, March 20, 2015, accessed August 18, 2016, http://dronecenter.bard.edu/what-you-need-to-know-about-domestic-drone-threats/#.

16. Sean Gallagher, "German Chancellor's Drone 'Attack' Shows the Threat of Weaponized UAVs," *ARS Technica*, September 18, 2013, accessed August 18, 2016, http://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/.

17. John Lichfield, "French Government on High Alert After Unexplained Drone Flights Over Nuclear Power Stations," *The Independent*, November 9, 2014, accessed August 18, 2016, http://www.independent.co.uk/news/world/europe/french-government-on-high-alert-after-unexplained-drone-flights-over-nuclear-power-stations-9850138.html; and Henry Samuel, "Drone Spotted Near Charlie Hebdo as 10 More Fly Over Paris," *The Telegraph*, March 4, 2015, accessed August 18, 2016, http://www.telegraph.co.uk/news/worldnews/europe/france/11449981/Drone-spotted-near-Charlie-Hebdo-as-10-more-fly-over-Paris.html.

18. Kellan Howell, "Drone Spotted Flying Near Obama While He Played Golf," *Washington Times*, August 25, 2015, accessed August 18, 2016, http://www.washingtontimes.com/news/2015/aug/25/drone-spotted-flying-near-obama-while-he-played-go/.

19. "Japan Radioactive Drone: Tokyo Police Arrest Man," *BBC News*, April 25, 2015, accessed August 18, 2016, http://www.bbc.co.uk/news/world-asia-32465624.

20. "A Brief History of Hamas and Hezbollah's Drones," Dan Gettinger and Arthur Holland Michel, Center for the Study of the Drone at Bard College, July 14, 2014, accessed August 18, 2016, http://dronecenter.bard.edu/hezbollah-hamas-drones/.

21. Ibid.; and Adiv Sterman, "Hezbollah Drones Wreak Havoc on Syrian Rebel Bases," *The Times of Israel*, September 21, 2014, accessed August 18, 2016, http://www.timesofisrael.com/hezbollah-drones-wreak-havoc-on-syrian-rebel-bases/.

22. Patrick Tucker, "In Ukraine, Tomorrow's Drone War Is Alive Today," *Defense One*, March 9, 2015, accessed August 18, 2016, http://www.defenseone.com/technology/2015/03/ukraine-tomorrows-drone-war-alive-today/107085/.

23. Brian Barrett, "When Good Drones Go Bad," *Wired*, January 18, 2016, accessed August 18, 2016, http://www.wired.com/2016/01/when-good-drones-go-bad/; and Jamie Condliffe, "ISIS Militants Use the Same Drones as Ordinary Folks," *Gizmodo*, August 29, 2014, accessed August 18, 2016, http://gizmodo.com/isis-militants-use-the-same-drones-as-ordinary-folks-1628376186.

24. David Hambling, "ISIS Is Reportedly Packing Drones with Explosives Now," *Popular Mechanics*, December 16, 2015, accessed August 18, 2016, http://www.popularmechanics.com/military/weapons/a18577/isis-packing-drones-with-explosives/.

25. John Villasenor, "The Drone Threat – in the U.S.," *Los Angeles Times*, March 27, 2012, accessed August 18, 2016, http://articles.latimes.com/2012/mar/27/opinion/la-oe-villasenor-license-domestic-drones-20120327; Eugene Miasnikov, "Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects" (Moscow: Center for Arms Control, Energy and Environmental Studies, Moscow Institute of Physics and Technology, 2005), 25, accessed August 18, 2016, http://www.armscontrol.ru/UAV/report.htm; and Peter Finn, "Mass. Man Accused of Plotting to Hit Pentagon and Capitol with Drone Aircraft," *The Washington Post*, September 28, 2011, accessed August 18, 2016, http://www.washingtonpost.com/national/national-security/mass-man-accused-of-plotting-to-hit-pentagon-and-capitol-with-drone-aircraft/2011/09/28/gIQAWdpk5K_story.html.

26. Finn, "Mass. Man Accused of Plotting."

27. "Al Qaeda in Spain," Soeren Kern, Gatestone Institute, August 15, 2012, accessed August 18, 2016, https://www.gatestoneinstitute.org/3275/al-qaeda-spain.

28. Jeevan Vasagar, "Students 'Planned Terror Attack Using Remote Control Planes,'" *The Telegraph*, June 25, 2013, accessed August 18, 2016, http://www.telegraph.co.uk/news/worldnews/europe/germany/10140642/Students-planned-terror-attack-using-remote-control-planes.html; and "German Police Bust Far-Right Model Plane Explosive Plot," *The Telegraph*, September 10, 2013, accessed August 18, 2016, http://www.telegraph.co.uk/news/worldnews/europe/germany/10298734/German-police-bust-far-Right-model-plane-explosive-plot.html.

29. "NYPD: Threat of Terrorists with Drones Is a Growing Concern," *CBS News*, October 29, 2014, accessed August 18, 2016, http://newyork.cbslocal.com/2014/10/29/nypd-threat-of-terrorists-with-drones-is-a-growing-concern/; Ian Drury, "Model Plane Enthusiasts? Watch Out, They Might Be Terrorists: Police Fear Some of Those Practising the Hobby Could Training for an Attack," *Daily Mail*, July 12, 2014, accessed August 18, 2016, http://www.dailymail.co.uk/news/article-2689474/Model-plane-enthusiasts-Watch-terrorists-Police-fear-practising-hobby-training-attack.html; Jeff Pegues, "Homeland Security Warns Drones Could Be Used in Attacks," *CBS News*, July 31, 2015, accessed August 18, 2016, http://www.cbsnews.com/news/homeland-security-warns-drones-could-be-used-in-attacks/; Kellan Howell, "Drones Over JFK Airport Prompts Federal Terror Alert," *Washington Times*, August 4, 2015, accessed August 18, 2016, http://www.washingtontimes.com/news/2015/aug/4/terrorist-alert-issued-following-third-drone-sight/; Tonda MacCharles, "RCMP Warned Ottawa Last Year of Possible Drone Terror Threat," *Toronto Star*, March 1, 2015, accessed August 18, 2016, http://www.thestar.com/news/canada/2015/03/01/rcmp-warned-ottawa-last-year-of-possible-drone-terror-threat.html; and Douglas Quan, "RCMP Fears Terrorists Could Use Off-the-Shelf Drones to Attack VIPs, Internal Documents Reveal," *National Post*, December 29, 2014, accessed August 18, 2016, http://news.nationalpost.com/news/canada/rcmp-fears-terrorists-could-use-off-the-shelf-drones-to-attack-vips.

30. Chris Hughes, "ISIS Planning to Use Toy Helicopters as Bombing Drones Fear Security Chiefs," *Mirror*, July 22, 2015, accessed August 18, 2016, http://www.mirror.co.uk/news/world-news/isis-planning-use-toy-helicopters-6119888.

31. David Pugliese, "Canadian Forces Selling Equipment, Mothballing Base Housing to Meet Cuts," *Ottawa Citizen – Defence Watch*, April 11, 2012, accessed August 18, 2016, http://www.ottawacitizen.com/technology/canadian+forces+selling+equipment+mothballing+base+housing+meet+cuts/6443814/story.html.

32. "Blue Knight 2010 Demonstration Concludes in Nevada," Defense-aerospace.com, November 22, 2010, accessed August 18, 2016, http://www.defense-aerospace.com/article-view/release/120324/us-exercise-looks-at-counter_uav-capabilities.html; and Ryan Faith, "Inside 'Black Dart,' the US Military's War On Drones," *Vice News*, October 28, 2014, accessed August 18, 2016, https://news.vice.com/article/inside-black-dart-the-us-militarys-war-on-drones.

33. "An Australian Counter Unmanned Aircraft System – 'Drone' – Security Initiative," Australian Certified UAV Operators Inc, accessed August 18, 2016, http://www.acuo.org.au/assets/docs/blog/ACUO-Press-Release-01-2015.pdf.

34. Wallace and Loffi, "Examining Unmanned Aerial System," 16.

35. "Blighter AUDS Anti-UAV Defence System," Blighter Surveillance Systems, accessed August 18, 2016, http://www.blighter.com/products/blighter-auds-anti-uav-defence-system.html; Joe Charlaff, "Analysis: Hostile UAVs … And the Defenses Against Them," *Homeland Security Today*, September 8, 2015, accessed August 18, 2016, http://www.hstoday.us/briefings/daily-news-analysis/single-article/analysis-hostile-uavs-and-the-defenses-against-them/50fd208f81aa7e50c412bd3458cecb2d.html; "SkyTracker – Overview," CACI International Inc., accessed August 18, 2016, http://www.caci.com/skytracker/index.shtml; and "Counter-UAV System from Airbus Defence and Space Protects Large Installations and Events from Illicit Intrusion," Airbus Defence & Space, accessed August 18, 2016, https://airbusdefenceandspace.com/newsroom/news-and-features/counter-uav-system-from-airbus-defence-and-space-protects-large-installations-and-events-from-illicit-intrusion/.

36. Charlaff, "Analysis."

37. Corey Charlton, "Sophisticated Drone-Jamming Technology Is to be Deployed by Anti-terror Officers at Major Events After a Successful Trial at Remembrance Sunday," *Daily Mail*, December 27, 2015, accessed August 18, 2016, http://www.dailymail.co.uk/news/article-3375435/Sophisticated-drone-jamming-technology-deployed-anti-terror-officers-major-events-successful-trial-Remembrance-Sunday.html.

38. "FAA Expands Unmanned Aircraft Pathfinder Efforts," US, FAA, October 7, 2015, accessed August 18, 2016, https://www.faa.gov/news/updates/?newsId=83927.

39. "Multi-Sensor Drone Warning System," Dedrone, accessed August 18, 2016, http://www.dedrone.com/en/dronetracker/drone-detection-hardware; "Domestic Drone Countermeasures," Domestic Drone Countermeasures, accessed August 18, 2016, http://www.ddcountermeasures.com/home.html; and "DroneShield," DroneShield, accessed August 18, 2016, https://www.droneshield.com/.

40. "Blighter AUDS Anti-UAV Defence System"; "SkyTracker – Overview"; and "Counter-UAV System from Airbus Defence."

41. Kelsey D. Atherton, "Drone-Proofing the Boston Marathon," *Popular Science*, April 21, 2015, accessed August 18, 2016, http://www.popsci.com/drone-protection-company-brought-net-guns-boston-marathon.

42. B. A. Jackson et al., *Evaluating Novel Threats*, 80–81.

43. Mario Aguilar, "Maker of Drone that Crashed at White House Will Block Flights Over DC," *Gizmodo*, January 28, 2015, accessed August 18, 2016, http://gizmodo.com/maker-of-drone-that-crashed-at-white-house-will-block-f-1682262818.

44. US, National Aeronautics and Space Administration, "UTM: Air Traffic Management for Low-Altitude Drones," accessed August 18, 2016, http://www.nasa.gov/sites/default/files/atoms/files/utm-factsheet-11-05-15.pdf.

45. Brief History of Hamas and Hezbollah's Drones"; and "Extended Area Protection and Survivability," Lockheed Martin, accessed August 18, 2016, http://www.lockheedmartin.ca/us/products/eaps.html.

46. "Extended Area Protection and Survivability."

47. Gareth Jennings, "ADEX 2015: Rafael Showcases Iron Beam C-RAM & C-UAV Laser," *IHS Jane's Defence Weekly*, October 20, 2015, accessed August 18, 2016, http://www.janes.com/article/55364/adex-2015-rafael-showcases-iron-beam-c-ram-c-uav-laser; Sean Gallagher, "Navy Will Deploy First Ship with Laser Weapon this Summer," *ARS Technica*, March 6, 2014, accessed August 18, 2016, http://arstechnica.com/information-technology/2014/03/navy-will-deploy-first-ship-with-laser-weapon-this-summer/; Jordan Golson, "Army's New Laser Cannon Blasts Drones Out of the Sky, Even in Fog," *Wired*, September 5, 2014, accessed August 18, 2016, http://www.wired.com/2014/09/armys-new-laser-cannon-blasts-drones-out-of-the-sky-even-in-fog/; and "China Develops Anti-drone Laser," *Xinhua,* November 2, 2014, accessed August 18, 2016, http://news.xinhuanet.com/english/china/2014-11/02/c_133760714.htm.

48. "China Develops Anti-drone Laser"; Eric Limer, "How to Shoot Down a Drone," *Popular Mechanics*, August 6, 2015, accessed August 18, 2016, http://www.popularmechanics.com/flight/drones/how-to/a16756/how-to-shoot-down-a-drone/; David Pugliese, "Open Season on Drones… Just How Do You Shoot Down Unmanned Aerial Vehicles?" *Ottawa Citizen – Defence Watch*, September 1, 2015, accessed August 18, 2016, http://ottawacitizen.com/news/national/defence-watch/open-season-on-dronesjust-how-do-you-shoot-down-unmanned-aerial-vehicles; "Can You Be Killed by a Bullet Falling From the Sky?" Stephanie Chasteen, Sciencegeekgirl, December 29, 2009, accessed August 18, 2016, http://blog.sciencegeekgirl.com/2009/12/29/can-you-be-killed-by-a-bullet-falling-from-the-sky/; and "Celebratory Gunfire in Dallas," Dean Weingarten, Ammoland Shooting Sports News, January 4, 2015, accessed August 18, 2016, http://www.ammoland.com/2015/01/celebratory-gunfire-in-dallas/#axzz3z1qztGD9.

49. Limer, "How to Shoot Down"; Cyrus Farivar, "Kentucky Man Shoots Down Drone Hovering over his Backyard," *ARS Technica*, July 29, 2015, accessed August 18, 2016, http://arstechnica.com/tech-policy/2015/07/kentucky-man-shoots-down-drone-hovering-over-his-backyard/; and Wallace and Loffi, "Examining Unmanned Aerial System," 21 and 23.

50. Limer, "How to Shoot Down"; "Can You Be Killed by a Bullet"; and "Celebratory Gunfire in Dallas."

51. Atherton, "Drone-Proofing the Boston Marathon."

52. "Mission Aérienne Légère à Organisation Unique," M.A.L.O.U., accessed August 18, 2016, http://www.malou-tech.fr/indexUS.php; "Rapere Interceptor Drone," Rapere, accessed December 22, 2015, http://rapere.io/ (content not available); and "DroneCatcher Catches Drone," Delft Dynamics, accessed August 18, 2016, http://www.delftdynamics.nl/index.php/en/news-en/117-dronecatcher-catches-drone.

53. Kelsey D. Atherton, "France Tests Kamikaze, Netted Interceptor Drones to Protect Nuclear Reactors," *Popular Science*, February 10, 2015, accessed August 18, 2016, http://www.popsci.com/france-tests-kamikaze-netted-interceptor-drones-protect-nuclear-reactors; James Vincent, "Tokyo Police Unveil Net-Wielding Interceptor Drone," *The Verge*, December 11, 2015, accessed August 18, 2016, http://www.theverge.com/2015/12/11/9891128/tokyo-interceptor-net-drone; and Kelsey D. Atherton, "South Korea Gets Ready For Drone-On-Drone Warfare with North Korea," *Popular Science*, April 2, 2015, accessed August 18, 2016, http://www.popsci.com/south-korea-gets-ready-drone-drone-warfare.

54. Michael Rundle, "Police Train Eagles to Take Down Drones on Sight," *Wired*, February 1, 2016, accessed August 18, 2016, http://www.wired.co.uk/news/archive/2016-02/01/eagle-vs-drone.

55. "Aerial Sports," Aerial Sports League, accessed August 18, 2016, http://aerialsports.tv/; and Thomas Fox-Brewster, "Maldrone: Watch Malware that Wants to Spread its Wings Kill a Drone Mid-Flight," *Forbes*, January 27, 2015, accessed August 18, 2016, http://www.forbes.com/sites/thomasbrewster/2015/01/27/malware-takes-down-drone/#27ef43d2c895.

56. "Samy Kamkar – SkyJack: Autonomous Drone Hacking," Samy Kamkar, accessed August 18, 2016, http://samy.pl/skyjack/; and Andrew Tarantola, "This Virus-Copter is a Digital Typhoid Mary," *Gizmodo*, December 10, 2012, accessed August 18, 2016, http://gizmodo.com/5967209/this-virus-copter-is-a-digital-typhoid-mary.

57. "Blighter AUDS Anti-UAV Defence System"; and "SkyTracker – Overview."

58. Laurent Beaudoin et al., "Potential Threats of UAS Swarms and the Countermeasure's Need," (paper, 10th European Conference on Information Warfare and Security, Tallinn, Estonia, 7–8 July 2011), 6, accessed August 18, 2016, https://www.researchgate.net/publication/261633504_Potential_Threats_of_UAS_Swarms_and_the_Countermeasure%27s_Need.

59. David Szondy, "Battelle's DroneDefender Anti-drone Beam Gun Grounds UAVs," *Gizmag*, October 16, 2015, accessed August 18, 2016, http://www.gizmag.com/battelles-dronedefender-beam-gun-uavs/39885/.

COMMAND IMPERATIVE TO TARGETING

CANADIAN ARMED FORCES EFFECTIVENESS IN TARGETING WITH AIR POWER DURING OPERATIONS MOBILE AND IMPACT

BY LIEUTENANT-COLONEL JARED PENNEY, CD

Editor's note: This paper was written by a candidate attending the Canadian Forces College in fulfilment of one of the requirements of the course of studies.

Often cited as a critical function in joint exercises and in recent operations, there has been emphasis of late placed on the importance of targeting within the Canadian Armed Forces (CAF), with the formation of the CAF Targeting Implementation Initiative.[1] Targeting ranges in complexity from conceptual design and analysis to planning and execution. It spans the strategic, operational and tactical levels and can be deliberate or dynamic.[2] By definition, targeting is aiming or directing, such as aiming a weapon at a target.[3] At the operational level, it is the systematic process of matching capabilities to targets and is complementary to the joint air tasking cycle. Targeting also comprises a conceptual design process that is used to analyse complex system of systems. The "butterfly effect" serves as a metaphor of this concept, as one of the theoretical challenges for targeting is accounting for unintended second- and third-order effects. It is the elasticity of targeting that has caught the attention of senior leadership within CAF and, conversely, developed into a quagmire that potentially threatens combat effectiveness.

The operational level of targeting warrants closer examination, since it bridges the tactical and strategic levels of war and there are design, planning and execution considerations. CAF's recent air operations over Libya and Iraq offer a unique opportunity to analyse operational targeting with air power. Operation (Op) MOBILE, Canada's named operation in support of Operations ODYSSEY DAWN (OOD) and UNIFIED PROTECTOR (OUP), demonstrated the potential of air power capabilities during an armed intervention. The unprecedented responsiveness and challenges in directing air power capabilities also exhibited the importance of targeting. Although initially ad hoc and heuristic in its application, CAF proved quite effective in achieving the desired effects and identified many lessons. Four years later, CAF had the opportunity to apply those lessons during another air-centric operation, Op IMPACT, Canada's named operation in support of Op INHERENT RESOLVE (OIR).

This article argues that CAF's enthusiasm with targeting has strayed from its pragmatic application during Op MOBILE that focused on enabling combat employment and achieving effects into a risk-management bureaucratic process that hampered effectiveness during Op IMPACT. The latter operation was less effective because targeting authorities were not commensurate with the competency of commanders, resulting in the situation of ineffectual command, as described by the Pigeau and McCann Balanced Command Envelope.[4]

It is challenging to evaluate all of the relevant evidence provided by these two operations because of the classification of much of the information and sensitivity around targeting directives during an ongoing operation. However, open-source data and discussions with key personnel involved in the targeting process of both operations contribute to our understanding of the process and offer insight to evaluate CAF's performance and effectiveness in broad terms and allow us to draw conclusions on why effectiveness was impaired during Op IMPACT. By providing context and explaining the operational assessment, targeting will be discussed as it relates to these two air-centric operations. Finally, this article demonstrates how some of the targeting policies and processes put in place during Op IMPACT promoted ineffectual command and impacted combat effectiveness.

OPERATIONAL ASSESSMENT OF TARGETING

The joint targeting cycle, depicted in Figure 1, is an iterative process that provides a useful framework for conducting deliberate and dynamic joint targeting.[5] The cycle begins with the end state and commander's objectives and ends with the assessment. An important activity in these stages is the development of observable, achievable, and reasonable measures and indicators (such as measures of effectiveness [MOEs] and measures of performance [MOPs]) to assess whether the effects and objectives are being or have been attained. Measures and indicators help focus target development within the joint targeting process, and are critical to enable assessment.[6]

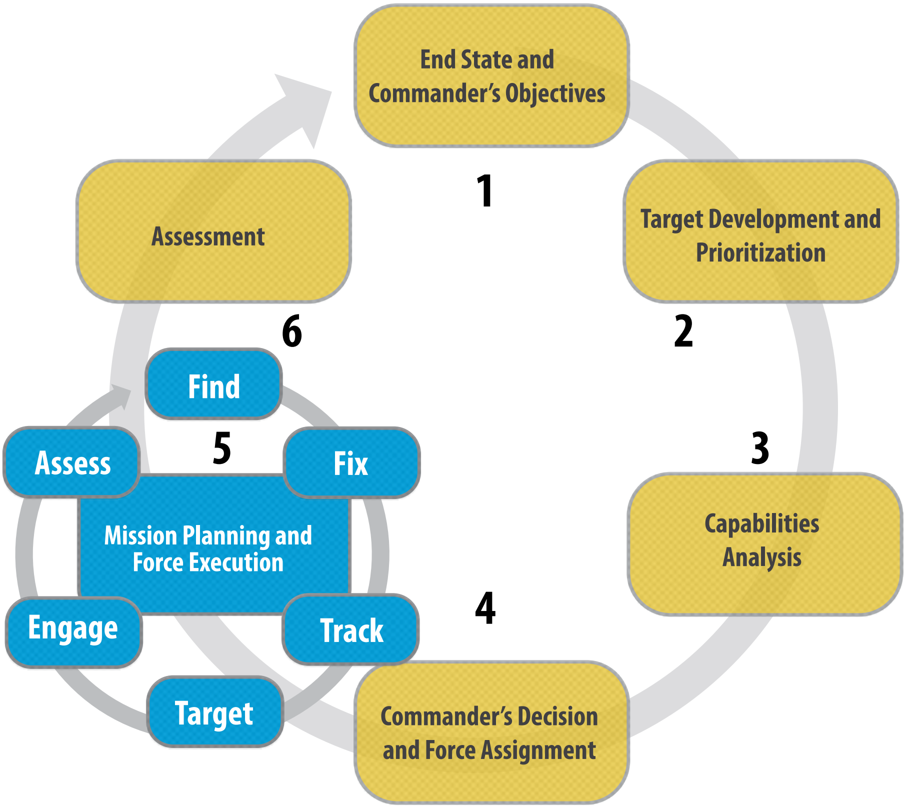

End State and Commander's Objectives
1
Target Development and Prioritization
2
3
Capabilities Analysis
4
Commander's Decision and Force Assignment
5
Mission Planning and Force Execution
Find
Fix
Track
Target
Engage
Assess
6
Assessment

Figure 1. Joint targeting cycle (dynamic and deliberate)[7]

MOPs are indicators used to assess friendly actions and measure task accomplishment. They are generally quantitative but may also apply qualitative attributes to task accomplishment.[8] MOPs help answer the question, "are we doing things right?"[9] MOEs are indicators used to help gauge the attainment of end-state conditions, achievement of objectives or creation of effects.[10] They do not measure task accomplishment or performance. MOEs are typically more subjective than MOPs and can be crafted as either qualitative or quantitative.[11] MOEs help answer the question, "Are we doing the right things to create the effect(s) on the operational environment (OE) that we desire?"[12]

This article will use MOP and MOE within the operational-assessment methodology to assess CAF's effectiveness compared to coalition partners during both operations. Indicators typically used to evaluate performance and effectiveness of achieving desired end states and objectives within each OE are useful; however, they are normally classified (i.e., weapon effectiveness). The operational assessment will, instead, focus on evaluating CAF's performance and effectiveness to the coalition within each operation. Although targeting effectiveness on each OE is not being evaluated, it is important to consider each OE and its effects on the targeting process. The OE of each operation will be considered; this will be followed by the targeting capabilities applied with respect to the joint air tasking cycle (discussed in Figure 2), and finally, the article will focus on Royal Canadian Air Force (RCAF) combat capabilities. Although not specific to targeting, these three areas will provide context to the MOP and MOE for comparative analysis.

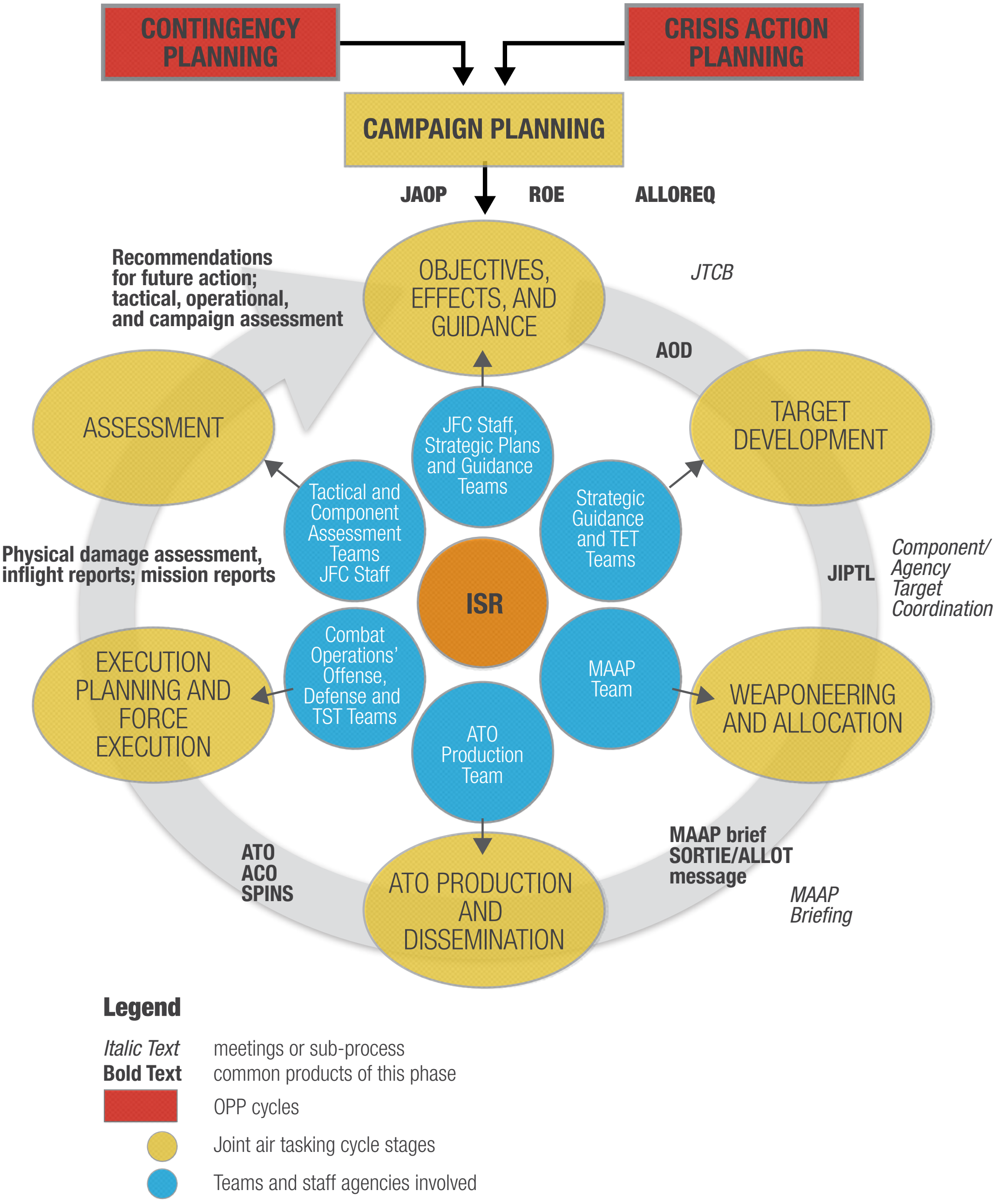

CONTINGENCY PLANNING
CRISIS ACTION PLANNING
CAMPAIGN PLANNING
JAOP
ROE
ALLOREQ
Recommendations for future action; tactical, operational, and campaign assessment
OBJECTIVES, EFFECTS, AND GUIDANCE
JTCB
AOD
ASSESSMENT
JFC Staff, Strategic Plans and Guidance Teams
TARGET DEVELOPMENT
Tactical and Component Assessment Teams JFC Staff
Strategic Guidance and TET Teams
Physical damage assessment, inflight reports; mission reports
ISR
JIPTL
Component/ Agency Target Coordination
EXECUTION PLANNING AND FORCE EXECUTION
Combat Operations' Offense, Defense and TST Teams
MAAP Team
WEAPONEERING AND ALLOCATION
ATO Production Team
ATO
ACO
SPINS
MAAP brief
SORTIE/ALLOT message
MAAP Briefing
ATO PRODUCTION AND DISSEMINATION
Legend
Italic Text meetings or sub-process
Bold Text common products of this phase
🟥 OPP cycles
● Joint air tasking cycle stages
● Teams and staff agencies involved

Figure 2. Joint air tasking cycle[13]

The joint air tasking cycle, depicted in Figure 2, provides a framework for the efficient and effective employment of air capabilities.[14] Although this cycle is specific to the combined air operations centre (CAOC) functions in the planning, coordination and execution of air operations, the joint targeting cycle stages are incorporated into the joint air tasking cycle. Op MOBILE and Op IMPACT both used the joint air tasking cycle, with air operations being directed by the CAOC.

Targeting is command led and intelligence supported. As depicted in Figure 2, intelligence, surveillance and reconnaissance (ISR) is centrally located within the joint air tasking cycle; this is representative of its role in supporting all stages of this cycle. The second stage, target development, consists of vetting; validation; target-list development; and nomination for prioritization, synchronization and action. The third stage of this cycle is executed by the master air attack plan team and target effects team. Capabilities analysis occurs during this stage, and resources are allocated to targets. Weaponeering and collateral damage estimates (CDEs) are conducted to various levels of refinement within these two stages. The execution stage of this cycle, conducted by the combat operations division, incorporates both the deliberate and dynamic targeting in addition to ongoing combat operations.[15]

The red card holder (RCH) of each country within the coalition makes targeting decisions on behalf of their country within the CAOC. The RCH is responsible for ensuring their nation's caveats and rules of engagement (ROE) are adhered to within the coalition.[16] The roles, authorities and responsibilities of an RCH are nation specific and are an important area that will be considered in this article.

OP MOBILE

In February 2011, the Arab Spring movement spread to Libya, resulting in civil unrest when violence escalated between protestors and pro-Gaddafi security forces. Alarmed by the deteriorating situation, the international community responded by adopting United Nations Security Council resolution 1973 on 17 March 2011, calling for states to establish a "no-fly zone" and to "take all necessary measures … to protect civilians and civilian population areas."[17] Two days later, the United States (US) initiated OOD.

On very short notice, seven CF188s from 425 Squadron in Bagotville and two CC150T aircraft from 437 Squadron in Trenton deployed to Trapani, Italy. On 21 March, CF188s conducted their first combat missions in support of OOD, the first since 1999 during Op ALLIED FORCE in Kosovo. OOD transitioned to OUP when the North Atlantic Treaty Organization (NATO) took control two weeks later under the command of Canadian Lieutenant-General (LGen) Charles Bouchard.[18]

Operating Environment

Libya is twice as big as Afghanistan and 160 times larger than Kosovo, presenting several challenges. The operating environment was partially contested and dynamic. The limited ground force / special operations forces (SOF) integration with the air force and lack of ISR provided many challenges to the targeting process. When the mission transitioned to NATO, the CAOC was not prepared, and effectiveness suffered from inadequate targeting expertise and support.

It was clear from the beginning that the initial Libya campaign would require US command and control as well as its unique strike capabilities. Planning for the Kosovo campaign took 15 months, while OOD was planned in a matter of weeks. United States Africa Command (AFRICOM) ran the campaign through the 603rd Air and Space Operations Center (AOC) in Ramstein. Within the first 24 hours, 22 of the 24 fixed surface-to-air missile (SAM) sites had been destroyed by cruise missiles and stealth aircraft.[19] The remaining threat to coalition air operations was a small number of tactical SAMs as well as a large number of man-portable SAMs and anti-aircraft artillery. Although mitigated by US suppression-of-enemy-air-defence support,[20] the contested environment meant that fighter aircraft had to operate at higher altitudes, limiting their effectiveness of finding and identifying targets, both visually and with targeting pods.[21]

The situation on the ground was very dynamic. The lack of detailed ground integration drove the requirement for more ISR assets. Although some coalition partners employed military advisors and liaisons with the anti-Gaddafi opposition forces, the deliberate target development process was hampered. Combined with the necessity to minimize collateral damage, the coalition had to employ more dynamic targeting in the form of strike coordination and armed reconnaissance (SCAR) missions.[22] Strike authority was delegated to the pilots whenever practicable.

> The discipline of OUP aircrew was commendable … .
>
> … Using a restricted fire line aided aircrews in knowing where within the ROE they could engage without CFAC [combined force air component] approval. Conversely, the CFAC had to approve targets on the restricted side of the restricted fire line. Whether aircrews or CFAC approved, due to the fluidity of the battlespace, limited ISR assets, and the strategic nature of every bomb, leadership and aircrews exhaustively weighed each engagement decision.[23]

The process of finding targets became more difficult, as Gaddafi forces traded their readily identifiable military equipment and tanks for those similar to the opposition forces. The rebels began marking the tops of their vehicles with an “N” to avoid misidentification; however, Gaddafi forces soon replicated this technique.[24] The opposition forces not only tried to adapt their strategies and movements to NATO’s air campaign but also directly influenced its targeting process. According to a RAND report:

> What is not widely known is that oppositionists across the country formed a complex network of spotters, informants, forward observers, and battle damage assessors. Anyone with a cell phone, Google Earth, Skype, Twitter, or email was in a position to report—and all of these conduits were used to pass coordinates, pictures, and other data. As the war progressed, the quality of the reporting improved. According to one Misratan observer, “First it was the general area, then GPS [global positioning system], and then Google Earth. I personally never reported anything unless I had someone put eyes on the target.” The problem that mission planners faced, therefore, was not a shortage of targeting information, but a flood of it. The challenge was vetting the sources, corroborating the data with other collection platforms, transforming it into intelligence, and then determining what was actionable.[25]

LGen Bouchard characterized the transition of OOD to the NATO structure as a “Hail Mary pass” because of the rapid response required (just three weeks of planning) and scepticism about the chances for the success of such an undertaking.[26] The transition of the operation to NATO proved to be anything but smooth, “exposing fissures in the alliance and gaps in capabilities.”[27] The CAOC in Poggio Renatico, Italy, lacked adequate infrastructure and computer architecture to support the necessary staff and operations. Personnel assigned to the CAOC had little experience, training or qualifications in CAOC functions and required major augmentation, especially in targeting.[28]

Initially, all targeting was envisioned to be supported from Turkey; however, this concept was abandoned after a few days when it was realized that two locations were unworkable.[29] Intelligence sharing and target development struggled as the NATO CAOC "lacked a functional ISR division,"[30] and "at the core of this limitation is the fact that few countries had the national capability to collect intelligence, analyse it, share it on classified architecture, and then develop the high-fidelity targeting materials necessary for an aerial campaign where collateral damage is a concern."[31] The solutions to the problems presented to operational planners required a divestment of targeting responsibilities to the pilots, thereby increasing operational efficacy and responsiveness.

CAF Targeting Capabilities

The speed of the Libyan crisis and deployment of RCAF assets put tremendous pressure on Canadian Expeditionary Force Command (CEFCOM), the predecessor to Canadian Joint Operations Command (CJOC). Heavily occupied by years of land-centric operations in Afghanistan, there was little experience and expertise in air operations.[32] Although effects-based operations, predominantly an air-force concept, had gained much momentum and acceptance jointly following Kosovo, there was a lack of targeting capability and expertise within CAF.[33] Despite the limited targeting capabilities, procedures, training and command support, competent commanders and aircrew were able to make correct decisions and operate effectively because they were enabled by higher headquarters and given appropriate authorities.

The cadre of fighter pilots sent to the CAOC to perform RCH duties had received no prior training in targeting or CDE methodology. Targeting decisions were recorded by a log, and deliberate pre-planned target packages consisted of imagery and a sheet with three sections for notes (intelligence, legal advisor [LEGAD] and operations). CEFCOM's initial lack of familiarity with the air operation resulted in limiting the authority of the Canadian RCHs. Colonel Gagne, one of the first deployed RCHs, described the deployment as "very challenging and highly rewarding" and credited direct communication with CEFCOM leadership as critical to building trust and confidence as the operation proceeded.[34] CF188 pilot performance also built confidence as the operation progressed as "public reports of CF-18s not dropping weapons due to collateral damage concerns confirmed that, in spite of low experience levels, Canadian aircrew were exercising a high degree of discretion and professionalism in a very sensitive operation."[35]

Intelligence and communication support to the RCHs in Poggio was very limited. A robust intelligence team was deployed to Trapani with level-three systems; however, the detachment was unable to contribute to the targeting process. Eventually near the end of the operation, the badly needed communications and intelligence support was established in Poggio to aid in targeting.[36]

On a number of occasions, the RCHs attempted to get strike approval for targets that exceeded their delegated authority, with limited success. RCHs soon realized that calling back to Canada was not always feasible for dynamic situations. Eventually CEFCOM delegated more authorities to the deployed RCHs, which increased their flexibility and effectiveness. One other distracting factor for the RCHs was the implementation of the air task force (ATF) concept. Initially, the RCH was dual-hatted as the ATF commander; however, midway through the operation, a separate ATF commander was deployed to the CAOC.[37]

The pace of operations was very high. Colonel Kenny, the RCH near the end of the operation, stated that "it was unusual for a day to go by without a strike." He also stated that even if they could effectively communicate with Canada, that CEFCOM "would have been significantly challenged to keep up with the pace of that operation." It was obvious that CEFCOM was satisfied with the state of operations or potentially distracted by Afghanistan, as Colonel Kenney stated that "sometimes we were wondering if they were even paying attention," and in retrospect, he "felt that some additional oversight would have been nice."[38]

RCAF Air Power Capabilities

RCAF air power employed by professional aircrews proved very effective despite having some capability deficiencies (weapons and CP140 capabilities). The CF188 had undergone a major modernization since last used in combat during the Kosovo campaign, with the most important and applicable upgrade being the Snipper XR targeting pod. Delays in acquiring the GBU-49 (GPS and laser-guided weapon) in time for the operation resulted in the RCAF very quickly acquiring and fielding the GPS-guided GBU-31 and GBU-38 joint direct attack munitions (JDAMs) in time for the end of the operation.

Although the CF188 performed superbly, the lack of low-collateral-damage and direct-attack munitions limited its effectiveness against certain targets. There was limited success employing laser-guided bombs against tanks, and the potential for collateral damage precluded striking other targets. The lack of the BRU-55 bomb rack limited the CF188 to one precision-guided munition (PGM) per weapon station.[39]

The Block II CP140 was equipped with the electro-optical/infrared MX-20 and a deployable mission support centre, which proved effective. However, without a beyond line of sight (BLOS) capability, data could not be shared in real time.[40] The Block II variant also lacked a self-defence suite that restricted employment to "wet feet" until the environment became more permissive.

The CP140 contributed critically required ISR and transitioned to the new role of SCAR. The successful accomplishment of this new skill, aided with embedded joint terminal attack controllers (JTACs), is a testament to the crew's professionalism and flexibility; however, the lack of self-protection, digitally aided close air support (CAS) equipment, Link 16 and target-marking capability degraded SCAR effectiveness.[41]

Measures of Performance and Effectiveness

CAF's performance in Op MOBILE was exceptional, given the limitations and restraints on the operating environment as well as targeting and air power capabilities. Canada was one of six countries that agreed to conduct offensive strikes, and RCAF CF188s flew 944 sorties over 3,882 hours and expended 696 PGMs, accounting for approximately 10 per cent (%) of all strikes (OUP total was 9,646 sorties and 7,642 munitions).[42]

As illustrated in Table 1, the coalition achieved on average a weapon per sortie (wpn/sortie) rate of 0.79. The RCAF achieved a rate of 0.74 wpn/sortie or 5.6 flight hours per weapon expended (hrs/wpn). Despite not having low-collateral-damage weapons or JDAMs, the RCAF achieved similar effectiveness rates as other countries with these capabilities such as Belgium (0.76 wpn/sortie, 5.5 hrs/wpn) and Denmark (0.72 wpn/sortie, 5.1 hr/wpn).[43] As a result of Op MOBILE, several lessons were identified specific to targeting, primarily the requirement to institutionalize the capability in terms of doctrine, training and command support.[44]

	Operation MOBILE	**Operation IMPACT**
Operating Environment	· partially contested and dynamic environment · limited ground-force/SOF integration with the air force · insufficient ISR and air-to-air refuelling (AAR) assets · limited expertise and support in NATO's newly adopted CDE methodology · CAOC very limited in capabilities and support	· permissive and fairly static environment · ground forces providing intelligence · sufficient ISR assets · robust CAOC capabilities, support and targeting expertise
CAF Targeting Capabilities	· CEFCOM's primary mission focus is Afghanistan · non-existent targeting capabilities, procedures and training · very limited secure communications and command support	· CJOC's primary mission · limited targeting capabilities and training · targeting directives · some secure communications and command support capabilities
RCAF Air Power Capabilities	· CF188 modernization with robust capabilities · Laser-guided bomb (LGBs) are only PGM · No inertial-aided munition (IAM), fast-moving target (FMT), direct fire air-to-surface missile (ASM), low-collateral-damage weapon (wpn) capabilities · Limited 1 PGM per wpn station · CP140 has MX-20 electro-optical/infrared (EO/IR) and L-11 · No APS-508 imaging radar, ALQ-507 ESM, L-16 BLOS, directional infrared countermeasures (DIRCM) [self-protection] · Laser tracking device (LTD) / IR marker	· CF188 enhanced self-protection · EPW II and JDAM · BRU-55 doubles CF188's carrying capacity of some PGMs · No FMT, direct fire ASM, low-collateral-damage wpn capabilities · CP140 modernization adds many capabilities and interim beyond line of sight (iBLOS) · Bk IV – BLOS, WGS, Link 16, DIRCM (self-protection) · LTD / IR marker
MOP	**Strike Missions** · **OOD/OUP** flew 9,646 sorties, expended 7,642 munitions · **RCAF** flew 944 sorties, 3,882 hours, expended 696 munitions · RCAF accounted for approximately 10% of all strikes · 660 of 944 strikes were dynamic (70%)	**Strike Missions** (30 Oct 14 to 15 Feb 16) · **OIR** flew 28,283 sorties, expended 36,769 munitions · **Target types:** 31% fighting positions, 30% other, 26% buildings, 5% oil infrastructure, 5% staging areas · **RCAF** flew 1,378 sorties, 5,512 hours, expended 606 munitions · RCAF accounted for approximately 2% of all strikes · **Target types:** 71% fighting positions, 8% buildings, 8% staging areas, 8% other, 6% vehicles
MOE	· **OOD/OUP** 0.79 wpn/sortie · **RCAF** 0.74 wpn/sortie, 5.6 hrs/wpn · **Belgium** 0.76 wpn/sortie, 5.5 hrs/wpn · **Denmark** 0.72 wpn/sortie, 5.1 hrs/wpn · **Norway** 0.96 wpn/sortie, 5.3 hrs/wpn	· **OIR** 1.3 wpn/sortie · **RCAF** 0.44 wpn/sortie, 9.1 hrs/wpn · **Australia** 0.74 wpn/sortie, 10.3 hrs/wpn, 7.6 hrs/wpn corrected for 468 nm [867 kilometres] distance from Al Minhad Air Base to Al Jaber (2 hours transit/sortie further than the RCAF)
Targeting Lessons Identified	· callback to CEFCOM for targeting approval not feasible · ATF construct was not fully implemented and distracted RCH · lack of RCH training · LGB buddy-lase procedures with other assets · JDAM and BRU-55	

Table 1. Comparison between Op MOBILE and Op IMPACT[45]

OP IMPACT

In 2014, the Islamic State of Iraq and the Levant's (ISIL's)[46] rapid advance across Iraq and Syria and the ineffectiveness of Iraqi Security Forces (ISF) in stopping them caught the international community off guard. ISIL's brutal actions of converting or killing non-Sunni populations in its goal of establishing an Islamic caliphate have displaced millions in the region and threatened regional and international security. On 7 August 2014, President Barack Obama authorized targeted military intervention in Iraq to halt the advance of and degrade ISIL.

Op IMPACT initially included the deployment of six CF188s and two CP140 aircraft to support the US-led coalition by conducting air strikes in Iraq and Syria from 30 October 2014 to 15 February 2016.[47] Unlike Op MOBILE, the deployment of CAF assets into theatre was well paced and deliberate. The RCAF ATF construct was more mature, and the ATF commander was separated from the targeting process, as learned following the Libya operation.[48]

Operating Environment

During the period that CAF was conducting air strikes, the operating environment for air operations in Iraq and Syria can be characterized as permissive and fairly static in terms of ground operations. Coalition joint fires and ISF/Peshmerga security force integration was well established, and there was an abundance of ISR assets. Air operations were controlled via United States Air Forces Central Command (USAFCENT) in Shaw Air Force Base, South Carolina, and the 609th AOC in Al Udeid Air Base, Qatar. USAFCENT had robust targeting capabilities, an ISR division and command support.[49]

In terms of air threat to coalition operations, ISIL's capabilities were limited.[50] Although Syrian pro-government forces had an established air defence system, they employed it passively, never attempting to interfere with coalition operations. On 30 September 2015, Russian forces deployed to Syria to support Bashar al-Assad's government. The US chose not to cooperate with Russian forces but, rather, deconflicted from them and established a memorandum of understanding.[51]

The coalition was successful in initially stopping ISIL's advance across Iraq in Syria, allowing ISF and Peshmerga security forces time to regroup and build capacity. By the end of Op IMPACT, the Peshmerga had made advances towards the ISIL-held city of Mosul and ISF had made gains in Ramadi and south west Iraq.[52] Coalition advisors, including CAF special operating forces aiding Peshmerga forces in Erbil, improved coalition understanding of the ground situation and coordination of joint fires.[53]

From the commencement of operations until the end of 2015, the coalition conducted 11,648 ISR sorties in comparison to 27,704 strike sorties.[54] These ISR assets were effectively controlled and coordinated by a robust and capable CAOC in Al Udeid with support from USAFCENT in Shaw Air Force Base. The large number of ISR assets allowed the coalition to develop targets and support ground operations much more effectively than was possible with the limited ISR and ground integration during OUP.

CAF Targeting Capabilities

In the years following Op MOBILE, CAF had made concerted efforts to institutionalize targeting by establishing a strategic working group and J3 targeting cell within CJOC. Progress in developing a strategic targeting directive (STD) and targeting training was fairly complete prior to Op IMPACT; however, they continued to evolve during the operation.[55]

Although CAF has ceased its kinetic air mission in Iraq, OIR is an ongoing operation, thus limiting the level of detail that can be discussed. Therefore, targeting will be discussed doctrinally with the understanding that operations will deviate and adapt to the requirement of the OE. In an air operation, all joint fires are approved by the target engagement authority (TEA) and coordinated with ground forces via JTACs and tactical control air parties within fires cells of ground units.[56] In OIR, joint fires are coordinated with ISF as well as tribal and Peshmerga forces by embedding specially trained advisors. "U.S. advisors have been embedded in various Iraqi headquarters in an effort to identify requirements for air support and pass them to the Combined Air Operations Center in Qatar, which is overseeing the air campaign."[57]

For non-US aircraft, the additional strike-approval step of RCH approval is required for all strikes (deliberate, dynamic or CAS). Although the coalition uses the RCH term, CAF has opted to use the TEA term within CAF targeting policy. Each CAF TEA team is comprised of a TEA, who is supported by a LEGAD and an intelligence officer.[58]

The Canadian TEA teams that deployed initially to Op IMPACT received limited training with CJOC staff, subject matter experts and former RCHs. Although there were growing pains with the newly drafted targeting directives, the TEA teams were more prepared than their counterparts in Op MOBILE. Similarly to Op MOBILE, the TEA's targeting authorities were initially limited. During the course of the deployment, it became obvious to the TEA teams that the imposed limitations were unfavourable to their effective execution; they lobbied on several occasions for clarification of targeting directives and ROE and requested changes to targeting authorities, as their understanding of the operation developed. Along with the targeting directives came an extensive target-reporting system absent from Op MOBILE. Although necessary for accountability, there was duplication of information between coalition targeting packages, the target summary sheet completed by the TEA and separate LEGAD reporting. CJOC staff had more targeting expertise than during Op MOBILE; however, it had limited organic air operations and fighter expertise.[59]

The lesson from Op MOBILE in separating the ATF commander and TEA was implemented; however, the ATF and joint task force (JTF) commanders were not located in the CAOC. This resulted in the two TEAs, a lieutenant-colonel and major, being the most senior CAF Op IMPACT representatives within the CAOC. Visa difficulties, working space and sustainment of senior officers were reasons cited for not placing a higher-ranked officer in the CAOC. Consideration should, thus, be made for future air operations, as significant high-level discussions about coalition air operations are conducted in the CAOC.[60]

As with Op MOBILE, each TEA described the challenges in getting approval when the target or ROE did not fall within their authority, especially dynamically. This resulted in passing on several targets or waiting until the situation became desperate enough that the strike could be conducted under self-defence. A cursory look at the types of targets CAF struck compared to the coalition (see Figure 3) shows that most strikes were against targets associated with combat engagement and CAS where self-defence situations would be likely.[61]

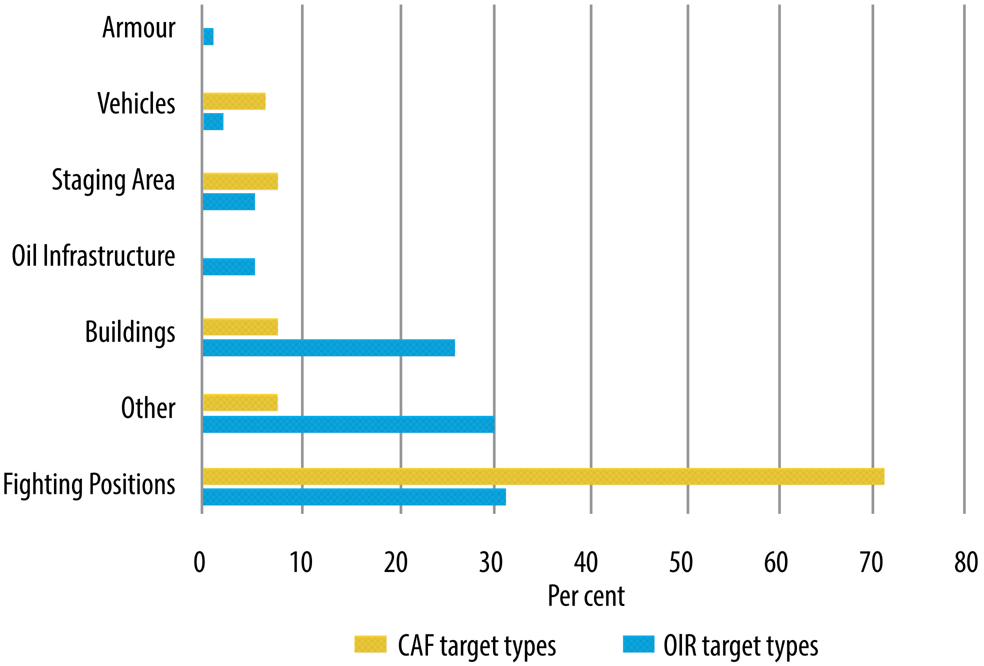


Figure 3. RCAF vs OIR target types, 30 October 2014 to 17 March 2016[62]

During Op MOBILE, each RCH interviewed described infrequent occasions when the LEGAD and RCH disagreed on the validity of a target, and the RCH made an operational decision based on their best judgement under the authority delegated as a military commander.[63] Without going into specifics, the freedom of an Op IMPACT TEA to make a military decision outside of the consensus of the entire TEA team was limited, resulting in a policy of decision making by committee.[64]

On the few occasions where the TEA could consult CJOC for strike approval, it was questionable what added benefit, in terms of decision-making support, was gained. The CJOC team's unfamiliarity with the current ground situation, complicated and changing targeting directives as well as complex air weapons effects and CDE methodology often led to long discussions, with the TEA explaining complex factors in layman's terms. It would be disingenuous to criticize the intentions or professionalism of the CJOC staff; nonetheless, they did not have access to all of the expertise, resources and information nascent within the COAC.[65] LGen Bouchard sums this up well, "Commanders must be given appropriate levels of responsibility to make decisions … if you don't have confidence in them, you did not train them effectively … stop trying to run an operation with a 5,000 mile [8,047 kilometre] screwdriver from Ottawa."[66]

RCAF Air Power Capabilities

Since Op MOBILE, the CF188 had improved capabilities in both self-protection and weapons with the introduction of the GBU-49 and BRU-55 bomb rack. Despite lacking a direct-fire capability and low-collateral-damage weapons, the CF188 was well suited for the operation and more capable in terms of weapon payload, guidance and fusing options, allowing flexibility against a greater range of targets. The Block III CP140 modernization was a more extensive improvement in ISR capabilities, adding an interim-BLOS capability that allowed ISR integration with the CAOC.[67]

Measures of Performance and Effectiveness

It would be expected that CAF performance and effectiveness would improve or, at a minimum, be on par with the coalition, given the contrast in limitations and restraints in the OE, targeting capabilities and air power capabilities from Op MOBILE to Op IMPACT; however, that was not the case. The CF188 flew 1,378 sorties, 5,512 hours and expended 606 munitions accounting for approximately 2% of all strikes (OIR total was 28,283 sorties and 36,769 munitions).[68]

The coalition achieved a 1.3 wpn/sortie. The RCAF's rates of 0.44 wpn/sortie and 9.1 hrs/wpn were significantly less and half as effective as they were during Op MOBILE. Direct comparison of these generic statistics with the coalition is problematic because some capabilities are not comparable. For instance, unmanned air vehicles (UAVs) with long loiter time and low-collateral-damage weapons have more employment opportunities; as well, approximately seven B-1B bombers are capable of delivering the same amount of ordnance that was employed by the RCAF during the entire operation.[69] However, examining the Royal Australian Air Force (RAAF) statistics is worthwhile for comparison. Matched with very similar capabilities and targeting directives as the RCAF, the RAAF achieved a 0.74 wpn/sortie rate and 10.3 hrs/wpn or 7.6 hrs/wpn corrected for 468 nautical miles (nm) [867 kilometre] distance from Al Minhad Air Base to Al Jaber (2 hours transit/sortie further than the RCAF).[70] It is fully acknowledged that a greater detail of analysis for this discrepancy may offer other explanations; however, the most obvious seems to be targeting authority.

EFFECTIVENESS OF AIR POWER TARGETING AND EMPLOYMENT

> *Talent and genius operate outside the rules, and theory conflicts with practice.*[71]
>
> – Carl von Clausewitz

Targeting must be command-led by competent leaders empowered with the appropriate levels of authority and responsibility to be effective. Air power must be given an appropriate level of flexibility in tactical execution to take full advantage of its capabilities. These two factors are the primary reasons why CAF was less effective targeting with air power during Op IMPACT and can first be illustrated using the Pigeau and McCann Competency, Authority and Responsibility (CAR) Model of Command. The model's Balanced Command Envelope shows that during the later stages of Op MOBILE, targeting policies placed the RCHs and aircrew inside balanced command, while policies during Op IMPACT placed the TEAs in the region of ineffectual command and overall effectiveness suffered.

The competency dimension of Pigeau and McCann's CAR model can be adapted to evaluate the RCH or TEA's ability to make competent decisions based on their working environment and available resources.[72] The competencies of the RCHs and TEAs are similar in terms of experience and knowledge of fighter operations; however, the TEAs deployed during Op IMPACT had an advantage in additional training and access to more resources, including intelligence and targeting support from the robust and capable CAOC. Highly integrated with friendly ground forces and having an abundance of ISR assets ensured the TEAs in Op IMPACT were well positioned to make competent decisions.

Pigeau and McCann describe authority as command's domain of influence: the degree to which a commander is empowered to act.[73] TEAs in Op IMPACT did not have as much authority as the RCHs in Op MOBILE or many of the other RCHs of the coalition in Iraq. There are two arguments made by CJOC Chief of Joint Targeting and Effects for this reason: The first being that the authority level was commensurate with appropriate risk against collateral damage and civilian casualties (CIVCAS). The second, Op MOBILE was commanded by a Canadian commander, and as such, his authority in directing targeting was deemed appropriate, therefore air power could take more of an execution mindset.[74]

OOD/OUP "designed a 'zero CIVCAS' framework that translated into the highest level of protection of civilians, property, and civilian infrastructure"[75] and was the first air operation to use 100% PGM.[76] Conversely, USAFCENT Commander, Lieutenant General Charles Brown, has stated that OIR is the "most precise air campaign in history."[77] An interim OIR report from the Washington Institute dated 13 January 2015 speaks to the importance of restraint on the cohesion of the coalition:

> The manner in which the campaign has been conducted has also been important. Coalition air operations have been carried out with an extremely high degree of precision and restraint. Thus far, reliable claims of civilian casualties—approximately fifty each in Iraq and Syria—are very low considering the number of weapons delivered. … This restraint has likely decreased the damage inflicted on ISIS [Islamic State of Iraq and Syria], but it has also paid huge dividends in assembling a broad coalition … .[78]

The importance of CIVCAS and collateral-damage avoidance was equal for both operations, and all targeting decisions made in OIR have this in mind. It would not be in the best interest of the US to put a coalition member in a possible CIVCAS situation, as it would threaten the coalition's cohesion. Implementing restrictive CAF targeting policies to mitigate risk against a zero CIVCAS framework is unnecessarily restrictive and impacts effectiveness as shown by the poor wpn/sortie ratio. The very low number of CIVCAS occasions by a coalition that employed 60 times more ordnance speaks to the effectiveness of the existing framework. CIVCAS can never be fully mitigated in an operation like OIR, and it is impossible to measure how many instances of CIVCAS were avoided by more restrictions. However, weapon employment rates and credibility are the casualties of caveats. Further, restricting strike authority until ground forces are put in a dangerous situation where self-defence ROE must be employed is bad policy. Ultimately, these restrictions actually had the intended effect and damaged coalition cohesion.

The suggestion that LGen Bouchard was making decisions for Canadian targeting is flawed because he was acting as the NATO Commander, thus making deliberate targeting decisions for the theatre. It may have been convenient that he was Canadian; however, he was not located in the CAOC, hence the reason CAF deployed RCHs to execute air power targeting. In discussions with the author, LGen Bouchard described his role in approving all deliberate targets and allowing the CFAC to execute air power strikes and dynamic targeting stating: "I refused to have a Predator feed in my headquarters because that was not my job, I had a large map and thought about the bigger picture … anything that could affect the coalition … the cohesion of the coalition was our centre of gravity."[79] LGen Bouchard also described his actions in stopping unnecessary target filtering by other agencies such as the CFAC or airborne warning and control system against targets he approved; however, he acknowledged that each nation should "have the right to refuse targets."[80]

The CAR model divides responsibility into two parts: extrinsic and intrinsic. Extrinsic responsibility is associated with personal and legal authority and is the degree to which an individual feels accountable up and down the chain of command, while intrinsic responsibility, simply stated, is a function of resolve and motivation.[81] RCHs and TEAs both had an extraordinary level of responsibility authorizing air strikes on behalf of the government of Canada.

The Pigeau and McCann CAR model (see Figure 4) can be expressed in three-dimensional space to represent the region of balanced command. The red star represents the region of command RCHs achieved near the end of Op MOBILE. It shows that they had the appropriate amount of authority and responsibility commensurate with their high level of competency. The white star represents the command assessment of the TEAs during Op IMPACT. It shows that the lower level of authority put them in the region of command that Pigeau and McCann describe as ineffectual command.

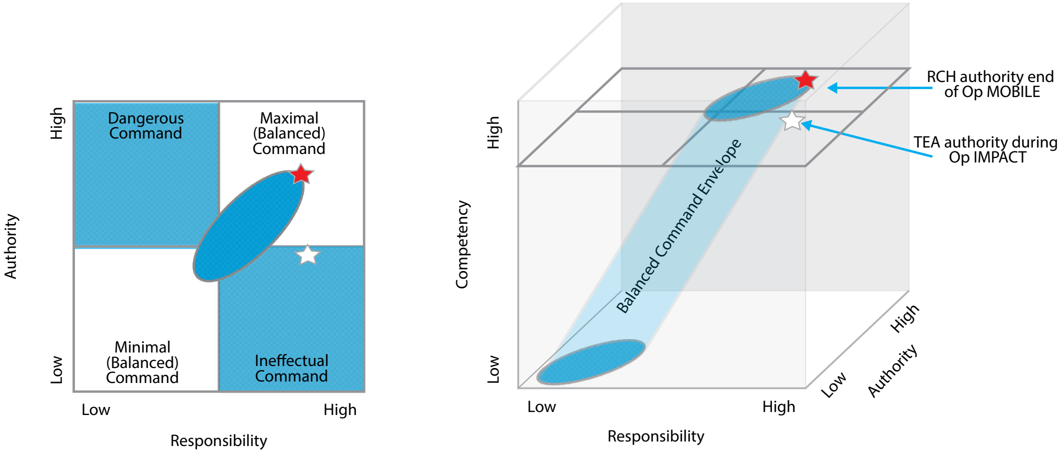

Authority
High
Low
Dangerous Command
Maximal (Balanced) Command
Minimal (Balanced) Command
Ineffectual Command
Low
High
Responsibility
Competency
High
Low
Balanced Command Envelope
RCH authority end of Op MOBILE
TEA authority during Op IMPACT
Low
High
Responsibility
Low
High
Authority

Figure 4. CAR representation of RCH and TEA during Op MOBILE and Op IMPACT[82]

The second reason why targeting effectiveness impaired combat execution was because a targeting process rather than a doctrinal joint fire support (JFS) construct was used to conduct CAS by non-US nations. This presents a difficult problem, as there are a number of good reasons why this was appropriate for the OE; however, it is important to understand the consequences of this construct in future air operations or if the OE changes. First, the context of what is meant by targeting and its role in supporting joint fires will be discussed. Targeting in its simplest form is a *selection process*. US doctrine defines joint targeting as "a fundamental task of the fires function"[83]; its purpose is to:

> integrate and synchronize fires into joint operations. Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. Targeting also supports the process of linking the desired effects of fires to actions and tasks at the joint force component level.[84]

Although intrinsically linked to joint fires, targeting is a separate task that enables joint fires by selecting targets and matching capabilities to achieve desired effects. Targeting doctrine conveniently categorizes targeting as deliberate or dynamic based on time and necessity to act; however, excluded from this process—but in the spectrum of necessity to act with force—is combat engagement[85] and self-defence. An effective joint fires and JFS system is intrinsic to joint combat operations.[86]

CAS, the predominant mission during OIR, was executed as dynamic targeting for coalition aircraft. The RCHs or TEAs would receive a brief by a fires team under the authority of a US TEA to strike a target and authorize a strike if it met national caveats. However, CAS is not found on the joint targeting cycle in Figure 1 because it is combat engagement and part of the JFS system in order to support the ground commander's intent. OIR is unique because the OE is permissive and static, communications with the CAOC and fires cell is very effective and, most importantly, there are no coalition troops in harm's way. It would not be appropriate from a risk-mitigation point of view to delegate CAF CAS strike approval to the cockpit given these factors; however, this would be different under other circumstances. The key takeaway is that CAS is not normally part of targeting, and future planners and commanders should understand that deviating from doctrine will affect tactical execution and effectiveness.

CONCLUSION

Operational assessment of targeting with air power during Op MOBILE and Op IMPACT has demonstrated how important targeting policies and doctrine are to effectively achieve desired effects. Lessons in targeting during Op MOBILE resulted in significant efforts to develop targeting capabilities. Although originating from the well-intentioned desire to adopt a linear, accountable and systematic decision-making process to manage risk, the unintended result established during Op IMPACT was a restrictive system encumbered by a bureaucratic process that promoted ineffectual command as described by the Pigeau and McCann Balanced Command Envelope. Executing CAS via a dynamic targeting process rather than as combat engagement within the JFS doctrine introduces inefficiencies; however, depending on the OE, it may be appropriate. These policies had ripple effects down to tactical execution of air power and directly impacted combat effectiveness in achieving desired effects.

Excess caveats in a mitigated framework unnecessarily degrade effectiveness and credibility, resulting in an uneven distribution of risk among the coalition and ground forces. Targeting must be command-led by competent leaders empowered with the appropriate level of authority and responsibility to be effective. Air power must be given an appropriate level of flexibility in tactical execution to take full advantage of its capabilities, provided that the OE is properly evaluated in terms of risk versus effectiveness. Strategic planners and leaders must understand that imposing restrictions on targeting or attempting to make targeting decisions from the national capital is ineffective in mitigating risk and ultimately results in decreased combat effectiveness with the undesired second-order effect of damaging credibility and coalition cohesion.

Lieutenant-Colonel Jared "Skitzo" Penney is a CF188 pilot with a Master of Defence Studies from the Royal Military College of Canada and considerable fighter experience. He has completed four operational fighter tours, including an exchange with the United States Marine Corps before heading the Air-Land Integration Cell in Kingston. He has combat experience in Iraq from August 2008 to December 2008, Libya from March 2011 to May 2011 and Qatar from October 2014 to April 2015. Having graduated from the Joint Command and Staff Programme, he took command of 3 Wing Operations in Bagotville, Quebec, in 2016.

ABBREVIATIONS

ACO	airspace control order
ALLOREQ	allocation request
AOC	Air and Space Operations Center
AOD	air operations directive
ASM	air-to-surface missile
ATF	air task force
ATO	air tasking order
BLOS	beyond line of sight capability to transmit mission data (including full motion video)
CAF	Canadian Armed Forces
CAOC	combined air operations centre
CAR	Competency, Authority and Responsibility
CAS	close air support
CD	Canadian Forces Decoration
CDE	collateral damage estimate
CEFCOM	Canada Expeditionary Force Command
CFAC	combined force air component
CFJP	Canadian Forces Joint Publication
CIVCAS	civilian casualties
CJOC	Canadian Joint Operations Command
CMM	Commander of the Order of Military Merit
DIRCM	directional infrared countermeasures
DND	Department of National Defence
EPW II	Enhanced Paveway II, GBU-49 is a dual-mode PGM both laser and GPS guided
ESM	electronic support measures (radar warning system / signals intelligence [SIGINT])
FMT	fast-moving target
GPS	global positioning system
hrs/wpn	flight hours per weapon expended
IAM	inertial-aided munition (i.e., GBU-38)
IR	infrared
ISF	Iraqi Security Forces
ISIL	Islamic State of Iraq and the Levant
ISR	intelligence, surveillance and reconnaissance
JAOP	joint air operation plan
JDAM	joint direct attack munition (IAM with GPS guidance i.e., GBU-38)
JDN	Joint Doctrine Note
JFC	joint force commander
JFS	joint fire support

JIPTL	joint integrated prioritized target list
JTAC	joint terminal attack controller
JP	Joint Publication
JTCB	joint targeting coordination board
LEGAD	legal advisor
LGB	laser-guided bomb (i.e., GBU-12)
LGen	lieutenant-general
LTD	laser tracking device
MAPP	master air attack plan
MOE	measure of effectiveness
MOP	measure of performance
MSC	Meritorious Service Cross
MSM	Meritorious Service Medal
NATO	North Atlantic Treaty Organization
nm	nautical mile
OC	Officer of the Order of Canada
OE	operational environment
OIR	Operation INHERENT RESOLVE
OOD	Operation ODYSSEY DAWN
Op	operation
OPP	operations planning process
OUP	Operation UNIFIED PROTECTOR
PGM	precision-guided munition
RAAF	Royal Australian Air Force
RCAF	Royal Canadian Air Force
RCH	red card holder
ROE	rules of engagement
SAM	surface-to-air missile
SCAR	strike coordination and armed reconnaissance
SOF	special operations forces
SORTIE/ALLOT	sortie allotment
SPINS	special instructions
TEA	target engagement authority
TET	targeting effect team
TST	time-sensitive target
US	United States
USAFCENT	United States Air Forces Central Command
WGS	World Geodetic System (reference coordinate system)
wpn	weapon
wpn/sortie	weapon per sortie

NOTES

[1] "The Chief of the Defence Staff Announces Canadian Armed Forces General and Flag Officer Senior Appointments, Promotions, and Retirements," Canada, Department of National Defence (DND), accessed August 11, 2016, http://news.gc.ca/web/article-en.do?nid=1028409.

[2] **Deliberate targeting** is conducted against targets identified and located during the planning phase of operations and is intended to be prosecuted on either a scheduled or on-call basis. This method best ensures that the desired effects will contribute directly to strategic objectives, while avoiding or minimizing collateral damage. **Dynamic targeting** is conducted against either known or unknown targets of opportunity that have not been located during the planning phase of operations. These targets may be unplanned and/or unanticipated. Dynamic targeting is also a planned process but uses an expedited version of deliberate targeting procedures to execute time-sensitive targets and other targets that need to be prosecuted quickly, due to their potentially fleeting nature, or critical importance. From Canada, DND, B-GJ-005-309/FP-001, Canadian Forces Joint Publication (CFJP) 3-9, *Targeting* (Ottawa: DND, 12 December 2014), 1-6.

[3] The *Defence Terminology Bank* record 5514 defines targeting as "the process of selecting and prioritizing targets and matching the appropriate response to them, taking into account operational requirements and capabilities."

[4] Ross Pigeau and Carol McCann, "Re-conceptualizing Command and Control," Canadian Military Journal 3, no. 1 (Spring 2002): 61.

[5] US, Joint Chiefs of Staff, Joint Publication (JP) 3-60, *Joint Targeting* (Washington, DC: Joint Chiefs of Staff, 2013), II-2.

[6] Ibid., II-4.

[7] Adapted from Canada, DND, CFJP 3-9, *Targeting*, 4-16.

[8] US, Joint Chiefs of Staff, Joint Doctrine Note (JDN) 1-15, *Operation Assessment* (Washington, DC: Joint Chiefs of Staff, 15 January 2015), A-7.

[9] Ibid., A-5.

[10] Ibid., A-4.

[11] US, Joint Chiefs of Staff, JP 3-60, *Joint Targeting*, C-7.

[12] US, Joint Chiefs of Staff, JDN 1-15, *Operation Assessment*, A-4.

[13] Source: US, Joint Chiefs of Staff, JP 3-60, *Joint Targeting*, C-3.

[14] US, Joint Chiefs of Staff, JP 3-60, *Joint Targeting*, B-5.

[15] Ibid., B-5-7.

16. This is based on the author's experience as the CAF RCH and TEA during Op IMPACT from October 2015 to April 2016.

17. Patricia A. Weitsman, "Operations Odyssey Dawn and Unified Protector," in *Waging War: Alliances, Coalitions, and Institutions of Interstate Violence* (Stanford: Stanford University Press, 2014), 164–65.

18. On Canada's contribution to OUP, see Richard O. Mayne, "The Canadian Experience: Operation Mobile," in *Precision and Purpose: Airpower in the Libyan Civil War*, ed. Karl P. Mueller (Santa Monica, CA: RAND Corporation, 2015).

19. Elizabeth Quintana, "A War from the Air," in *Short War, Long Shadow: The Political and Military Legacies of the 2011 Libya Campaign*, ed. Adrian Johnson and Saqeb Mueen (Royal United Services Institute, 16 Mar 2012), 31, 33.

20. SA-6 Gainful, SA-8 Gecko, SA-9 Gaskin and the French Crotale were still present. Source: Christina Goulter, "The British Experience: Operation Ellamy," in Mueller, *Precision and Purpose*, 160.

21. Based on the author's experience flying combat missions in Libya from March to May 2011.

22. Jason R. Greenleaf, "The Air War in Libya," *Air and Space Power Journal* 27, no. 2 (March–April 2013): 32.

23. Todd R. Phinney, "Reflections on Operation *Unified Protector*," *Joint Force Quarterly* 73 (April 2014): 90.

24. "The Hidden Story of Airpower in Libya (and What It Means for Syria)," Frederic Wehrey, *Foreign Policy*, accessed August 11, 2016, http://foreignpolicy.com/2013/02/11/the-hidden-story-of-airpower-in-libya-and-what-it-means-for-syria/.

25. Frederic Wehrey, "The Libyan Experience," in Mueller, *Precision and Purpose*, 61.

26. Deborah C. Kidwell, "The U.S. Experience: Operational," in Mueller, *Precision and Purpose*, 136.

27. Greenleaf, "Air War in Libya," 37.

28. Ibid., 39–40.

29. Colonel Normand Gagne, CD, telephone conversation with author 18 April 2016.

30. Phinney, "Reflections on Operation *Unified Protector*," 89.

31. Ibid., 88.

32. Gagne telephone conversation with author; and Colonel Eric Kenny, MSM, CD, telephone conversation with author 11 April 2016.

33. Michael Clark, "The Making of Britain's Libya Strategy," in Johnson and Mueen, *Short War, Long Shadow*, 25.

[34] Gagne telephone conversation with author.

[35] Darcy E. Molstad, "CF-18s in Combat from Iraq to Libya: The Strategic Dividend of Fighters" (directed research project, Canadian Forces College, 2011), 73. It will also be published as Darcy E. Molstad, "CF-18s in Combat from Iraq to Libya: The Strategic Dividend of Fighters" in *The Curtis Papers: Canadian Aerospace and Joint Studies*, vol. 2 (Trenton, ON: DND, forthcoming).

[36] 1630-1 (Comd TF LIB), 7 November 2011, End of Tour Report, Task Force Libeccio.

[37] Gagne telephone conversation with author; and Kenny telephone conversation with author.

[38] Kenny telephone conversation with author.

[39] CF188s were most often configured with three external tanks, leaving two weapon stations free (based on author's experience in Op MOBILE).

[40] Daniel Arsenault and Josh Christianson, "Punching Above Its Weight: The CP140 Aurora Experience within Task Force Libeccio and Operation MOBILE," *Royal Canadian Air Force Journal* 1, no. 3 (Summer 2012): 29–30.

[41] Alan Lockerby, "SCAR-C Over Libya: To War in an Aurora," *Canadian Military Journal* 12, no. 3 (Summer 2012): 66.

[42] 1630-1 (Comd TF LIB), 7 November 2011, End of Tour Report, Task Force Libeccio, 1; and Karl P. Muller, "Examining the Air Campaign in Libya," in Mueller, *Precision and Purpose*, 4.

[43] Christian F. Anrig, "The Belgian, Danish, Dutch, and Norwegian Experiences," in Mueller, *Precision and Purpose*, 301.

[44] 1630-1 (Comd TF LIB), 7 November 2011, End of Tour Report, Task Force Libeccio.

[45] Sources: ibid.; Muller, "Examining the Air Campaign in Libya"; "Operation IMPACT – Air Task Force-Iraq Airstrikes," Canada, DND, accessed August 11, 2016, http://www.forces.gc.ca/en/operations-abroad-current/op-IMPACT-airstrikes.page; "Operation INHERENT RESOLVE: Targeted Operations against ISIL Terrorists," US, Department of Defense, accessed August 11, 2016, http://www.defense.gov/News/Special-Reports/0814_Inherent-Resolve; and "Air Task Group (ATG)," Australia, Department of Defence, accessed August 11, 2016, http://www.defence.gov.au/Operations/Okra/atg.asp.

[46] ISIL is also known as the Islamic State of Iraq and Syria (ISIS), the Islamic State (IS), and Daesh.

[47] "Operation IMPACT – Air Task Force-Iraq Airstrikes."

[48] Lieutenant-Colonel William Radiff, CD, telephone conversation with author 11 April 2016.

[49] "Ground to Air: The Unseen Link," US, United States Air Forces Central Command, accessed August 11, 2016, http://www.afcent.af.mil/News/ArticleDisplay/tabid/4779/Article/749596/ground-to-air-the-unseen-link.aspx.

50. Based on author's experience as Canadian TEA during Op IMPACT from October 2015 to April 2016.

51. "Department of Defense Press Briefing by Col. Warren via Teleconference from Baghdad, Iraq," US, Department of Defense, accessed August 11, 2016, http://www.defense.gov/News/News-Transcripts/Transcript-View/Article/632421/department-of-defense-press-briefing-by-col-warren-via-teleconference-from-bagh.

52. Interactive maps are available at Livuamap, accessed August 11, 2016, https://isis.liveuamap.com/ and "This Animated Map of ISIS Expansion in Syria, Iraq and Beyond Is Unsettling,"Tyler Rogoway, Foxtrot Alpha, accessed August 11, 2016, http://foxtrotalpha.jalopnik.com/this-animated-map-of-isis-expansion-in-syria-iraq-and-1756464711.

53. "Operation IMPACT," Canada, DND, accessed August 11, 2016, http://www.forces.gc.ca/en/operations-abroad-current/op-IMPACT.page.

54. "Combined Forces Air Component Commander 2011–2016 Airpower Statistics," US, United States Air Forces Central Command, accessed August 11, 2016, http://www.defense.gov/Portals/1/features/2014/0814_iraq/docs/March_2016_Airpower_Summary.pdf.

55. Based on author's experience as Officer Commanding Air-Land Integration Cell 2012–2015 and Canadian TEA during Op IMPACT from October 2015 to April 2016.

56. US, Joint Chiefs of Staff, JP 3-09, *Joint Fire Support* (Washington, DC: Joint Chiefs of Staff, 2014), I-3 and I-4.

57. "Operation Inherent Resolve: An Interim Assessment," Scott A. Vickery, The Washington Institute, accessed August 11, 2016, http://www.washingtoninstitute.org/policy-analysis/view/operation-inherent-resolve-an-interim-assessment.

58. Based on author's experience as Canadian TEA during Op IMPACT from October 2015 to April 2016; and "Exclusive: Inside Canada's Bombing Bureaucracy," Terry Milewski, CBCNews, accessed August 11, 2016, http://www.cbc.ca/news/politics/cf18-bombing-forms-milewski-1.3476675.

59. Radiff telephone conversation with author.

60. Gagne telephone conversation with author; Kenny telephone conversation with author; and Lieutenant-Colonel Sean Doell, CD, telephone conversation with author 11 April 2016.

61. Based on author's experience as Canadian TEA during Op IMPACT from October 2015 to April 2016.

62. Source: "Operation IMPACT – Air Task Force-Iraq Airstrikes"; and "Operation INHERENT RESOLVE."

63. Gagne telephone conversation with author; Kenny telephone conversation with author; and Lieutenant-Colonel Jeffery Lebouthiller, CD, telephone conversation with author 15 April 2016.

[64] Based on author's experience as Canadian TEA during Op IMPACT from October 2015 to April 2016.

[65] Radiff telephone conversation with author; Lieutenant-Colonel Jean-Paul Peart, CD, telephone conversation with author 14 April 2016; and author's experience as TEA during Op IMPACT from October 2015 to April 2016.

[66] Lieutenant-General Charles Bouchard, OC, CMM, MSC, CD, telephone conversation with author 10 June 2016.

[67] 2000-0 (A2), 19 January 2016, 1 Canadian Air Division Intelligence, Surveillance and Reconnaissance (ISR) Directive – Spiral One.

[68] "Operation IMPACT – Air Task Force-Iraq Airstrikes"; and "Operation INHERENT RESOLVE."

[69] "B-1B Lancer," US, United States Air Force, accessed August 11, 2016, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104500/b-1b-lancer.aspx.

[70] "Air Task Group (ATG)."

[71] Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret, introduction and notes by Beatrice Heuser (Oxford: Oxford University Press, 2008), 89.

[72] Ross Pigeau and Carol McCann, "Re-conceptualizing Command and Control," 57–58.

[73] Ibid., 58–59.

[74] Lieutenant-Colonel Jay MacKeen, MSM, CD, telephone conversation with author 9 May 2016.

[75] Gregory Alegi, "The Italian Experience: Pivotal and Underestimated," in Mueller, *Precision and Purpose*, 219.

[76] Muller, "Examining the Air Campaign in Libya," 4.

[77] "General: Airpower Key to ISIL Fight; Strikes to Continue," US, United States Air Forces Central Command, accessed August 11, 2016, http://www.afcent.af.mil/News/ArticleDisplay/tabid/4779/Article/658205/general-airpower-key-to-isil-fight-strikes-to-continue.aspx.

[78] "Operation Inherent Resolve: An Interim Assessment."

[79] Bouchard telephone conversation with author.

[80] Ibid.

[81] Pigeau and McCann, "Re-conceptualizing Command and Control," 58–59.

[82] Adapted from ibid.

[83] US, Joint Chiefs of Staff, JP 3-60, *Joint Targeting*, vii.

84. Ibid.

85. Combat engagement occurs during the close battle, where combat with the adversary is actual, imminent or likely. Planned targets should be engaged using deliberate or dynamic targeting procedures wherever possible; however, during combat engagement, targets will appear inside of the relevant planning cycles and will need to be prosecuted when there is no time for either a deliberate or formally expedited targeting process to take place. In these cases, targeting during combat engagement follows a simplified methodology, taking into account ROE and the law of armed conflict. Source: Canada, DND, CFJP 3-9, *Targeting*, 1-9.

86. Joint fires can be both lethal and non-lethal. JFS implies the use of joint fires to support manoeuvre elements. The effective integration of joint fires relies on a robust system that uses interoperable network architecture, standard operating procedures and extensive joint training.

CYBER WARFARE SCHOOLS OF THOUGHT:

BRIDGING THE EPISTEMOLOGICAL/ONTOLOGICAL DIVIDE, PART 2

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

Editor's note: Part 1 of this article examined the Conservative school of thought and introduced the Revolutionary Materialist school of thought in the summer 2016 issue of the Royal Canadian Air Force Journal. *Part 2 completes the review of the Revolutionary Materialist school of thought and then turns to the Liberal Materialist school of thought.*

A NEW ERA OF WARFARE

In order to emphasize the revolutionary nature of an era, Revolutionaries tend to propose new categories of emerging warfare and associated conceptual language. Wayne Hall discusses "Knowledge War," which he describes as "an intense competition for valuable information and knowledge that both sides need for making better decisions faster than the adversary."[1] In this, there is an obvious linkage between this concept and the thinking of Colonel John Boyd and his Observe, Orient, Decide and Act (OODA) Loop.[2] The goal of knowledge warfare is to find and "sustain decision dominance, which leads to an overall advantage in decision making and results in a triumph of will by one side or the other."[3] Hall argues that technology produces three specific features which enable the generation of knowledge warfare. First, the inter-relations between social, economic, and political systems create a "world tapestry of systems."[4] This tapestry enables second- and third-order effects to be created by pulling on the threads of this tapestry, even from a distance. Second, "truth" has increasingly become a relative variable, rather than an absolute one. As such, this opens up many paths to consider what constitutes the "proper" course of action. While this certainly raises the spectre of anarchy and relativism, it also frees individual decision makers from "dogmatic thinking," opening up new paths for creative problem solving. Finally, technology unites these two aspects together and reflexively speeds up the process as it advances in capability. "Victory in future conflicts will go to the side whose leaders make the best use of knowledge to make the most effective and, in some cases, quickest decisions."[5] Thus, knowledge leads to better decisions, resulting in rapid actions generating political effects, which in turn influence the will of the enemy to continue engaging in conflict.[6]

Irrespective of whether they discuss novel forms of warfare that will emerge in this new era, Revolutionaries tend to emphasize the opportunities for manoeuvre that emerge with cyber warfare. Winn Schwartau argues that cyber offers "subtlety" in achieving strategic goals, a better way to reach them without the chaos and bloodshed of kinetic operations.[7] The goals of "information warriors" are to steal information in order to turn it against their opponents; to modify information in order to instill fear or embarrass them; to destroy information outright to deny its use; and, only finally, to destroy information infrastructure, so as to put the method for transmitting information out of commission.[8] Hall echoes this emphasis on manoeuvre in his writings as well. Information warfare is linked to asymmetric warfare in its emphasis on affecting and influencing behaviour as opposed to movement and control of terrain and the destruction of objects on that terrain.[9] Hall cites Sun Tzu, a theorist of revolutionary concepts, arguing that the real terrain of battle lies in the minds of humans and manoeuvre involves the manipulation of knowledge and the psyches of human beings as central to this modality of warfare.[10] Influenced by Sun Tzu's writings on offensive strategy, "those skilled in war subdue the enemy's army without battle,"[11] Jeffrey Carr offers a definition for cyber warfare that captures its indirect nature along with the sophistication of Sun Tzu inspired strategy: "Cyber Warfare is the art and science of fighting without fighting, of defeating an opponent without spilling their blood."[12]

John Arquilla and David Ronfeldt are two of the most prominent Revolutionary writers in the canon. Since their seminal piece *Cyberwar is Coming!*[13] they have published numerous works examining the impact of modern information technology (IT) on contemporary conflict.[14]

Both were among the first to use the term *cyberwar* as a conceptual tool as well as developing a civil-oriented term, *netwar* to describe non-military use of information weaponry. Both concepts attempt to create similar conditions: interference in "what a target population knows or thinks it knows about itself and the world around it."[15] Netwar is aimed at elite and public opinions and works through the use of propaganda, subversion, deception and interference with the media. Cyberwar, on the other hand, while similar in nature, focuses solely on military use of these vectors to alter "the 'balance of information and knowledge' in one's favour, especially if the balance of forces is not."[16] Both concepts seek to take advantages of the technological affordances of IT to lower the entry costs of these activities: as less capital and labour is necessary to initiate this type of activity, smaller, less well-resourced, decentralized and agile groups are able to take on larger, centralized and static institutions.[17] Arquilla and Ronfeldt share ideas similar to Hall's Knowledge War, in that they argue that actors involved in netwar aim to "confound people's fundamental beliefs about the nature of their culture, society, and government, partly to foment fear, but mainly to disorient people and unhinge their perceptions."[18] Thus, "Epistemological War" structurally challenges an organization by raising fundamental questions as to whose responsibility it is to respond and what missions are necessary to undertake: "When roles and missions of defenders are not easily defined, both deterrence and defence become problematic."[19]

Following from their netwar concept, Arquilla and Ronfeldt discuss the spread of social conflict onto the Internet and how cyberwar manoeuvre also takes place in terms of the actors who are introduced to this new battlespace. Small communities of interest now have the ability to confront states more aggressively.[20] Netwar enables non-state actors, non-governmental organizations, other militant social activists and even states pursuing limited objectives with limited means to attack policy problems.[21] The recent activities of Anonymous[22] (which has targeted states, corporations and other interest groups) provide an obvious example of this effect, however, so do the Tea Party and Occupy Wall Street movements in the United States (US) as well as certain aspects of the Arab Spring.[23] However, illegitimate actors may also participate and may ultimately form the principal drivers for this form of activity. Carr notes that "cyber-crime is the lab where malicious payloads and exploits used in cyber warfare are developed, tested and refined."[24] All this points to a more fluid operational environment where the lowered entry costs to strategic competition between social groups lends agency to groups that have traditionally had more limited opportunities to participate. In effect, the growth of strategic capability on the part of these new actors has increased the manoeuvre space available to these groups and further complicated the military operating environment for more traditional strategic actors.

Arquilla and Ronfeldt are firmly in the Revolutionary camp with these concepts. They argue that both cyberwar and netwar are waypoints towards a new post-industrial era because the age of attrition is coming to an end and that military forces may not even need to be engaged in order to achieve victory.[25] Arquilla and Ronfeldt state:

> The emergence of Netwar [and cyberwar for that matter] implies a need to rethink strategy and doctrine, since traditional notions of war as a sequential process based on massing, maneuvering and fighting will likely prove inadequate to cope with a non-linear landscape of conflict in which societal and military elements are closely intermingled.[26]

Greg Rattray introduces the concept of strategic information warfare (SIW), which describes "efforts to defeat opponents through attacks on centers of gravity without fighting fielded military forces."[27] Similar to Arquilla and Ronfeldt's netwar, SIW targets the opponent's will to fight as well as their ability to carry on normal economic routines and command fielded forces.[28]

The Revolutionary perspective on this emerging cyber environment is also of a particular character. Revolutionaries tend to be deterministic in their outlook on the impact of technology on the strategic environment.[29] For Schwartau, the technological environment of IT is the source of cyberwar. Networks' ability to defy borders, their utility in the spread of information (enabling all to weigh their local circumstances against conditions elsewhere), the clean and bloodless nature of cyberwar and the low risks of action versus the high payoffs for success, all motivate consideration of it as a strategic vector for influencing others. Because, in general, high technology is poorly understood, yet still highly relied upon, fear of the unknown means that cyber events will generate a significant amount of fear. Last, Schwartau concludes that cyberwar will take place simply because it can. In other words, technology is an anarchic free force that will sweep all before it.[30]

Richard Clarke focuses on the actual design of the Internet as a causative factor in the appearance of cyberwar. Noting that the Internet was designed to share information, not for security, Clarke notes that features such as the Domain Name System, the Internet's addressing system, is easily spoofed, as is the routing system, the Border Gateway Protocol. Internet reliance on open and unencrypted software allows any with the will to reprogram and interfere with the system; indeed, its decentralized design with a lack of centralized control measures is often the excuse for facilitating systematic anarchy which facilitates bad behaviour.[31] The same technological features also create a first-strike incentive for those considering cyberwar attacks. A cyberwar attack to an offensively minded group offers several advantages: speed of attack, anonymity, the difficulty to deter such attacks as well as the continued secrecy with which cyber events are treated by governments and corporations. Given such overwhelmingly positive incentives to conduct cyberwar strikes, cyber-capable groups are left without any need to reflect on the possible repercussions of such an act.[32]

Arquilla and Ronfeldt also discuss technology in a deterministic fashion. IT disrupts and erodes hierarchies, by diffusing and redistributing power, crossing borders, expanding spatial and temporal horizons as well as opening closed systems. Arquilla and Ronfeldt state: "The information revolution favors the growth of such networks by making it possible for diverse, dispersed actors to communicate, consult, coordinate, and operate together across greater distances and on the basis of more and better information than ever before."[33] These conditions allow "swarming" actions to occur, when dispersed nodes converge on a target or issue area from multiple directions in a sustained pulse of activity. Nodes coalesce rapidly and stealthily; once the task is completed, they disengage and re-disperse, and then ready themselves for the next pulse. This is viewed as being considerably different from typical mass and manoeuvre of conventional military operations.[34] As they put it:

> The information revolution favors and strengthens network forms of organization, while making life difficult for hierarchical forms. The rise of network forms of organization … is one of the single most important effects of the information revolution for all realms: political, economic, social, and military. It means that power is migrating to small, nonstate actors who can organize into sprawling networks more readily than can traditionally hierarchical nation-state actors. It means that conflicts will increasingly be waged by "networks," rather than by "hierarchies." It means that whoever masters the network form stands to gain major advantages in the new epoch.[35]

Along with opening up strategic agency at the organizational and operational levels, technology also blurs conventional concepts for structuring cognitive understanding of the battlespace. Thus, offence and defence are blurred to the extent where it becomes "difficult to distinguish between attacking and defending actions."[36] Similar sorts of problems can be seen in the difficulty of determining who is undertaking the action and what their motivations for it are. Thus, simple "hacking"[37] becomes conflated with cybercrime and ultimately with cyberwar itself, as the only thing that distinguishes these activities from one another is the motivation which lies behind it. This in turn complicates the ability of the state to respond to these actions. Arquilla and Ronfeldt argue:

> [nation-state] sovereignty and authority are usually exercised through bureaucracies in which issues and problems can be sliced up and specific offices can be charged with taking care of specific problems. In netwar, things are rarely so clear. A protagonist is likely to operate in the cracks and gray areas of a society, striking where lines of authority crisscross and the operational paradigms of politicians, officials, soldiers, police officers, and related actors get fuzzy and clash.[38]

CYBER VULNERABILITIES WITH INTEGRATED MILITARY HARDWARE

Science-fiction writers and Revolutionaries are fascinated with the vulnerabilities that come with a society that is completely dependent on the information and services that support their basic existence. Less advanced adversaries need not look to direct military confrontation, as indirect approaches can negate the technological advantages of superior military capabilities that are dependent on technology to be effective at war.[39] Furthermore, globalization of electronics manufacturing has opened the door to foreign interests to embed covert code or leave the hardware open to external commands/influence by adversarial groups or nations.[40] The majority of the electronic component fabrication occurs outside continental North America, leaving the US [and Canadian] defence industry significantly vulnerable to cyberattacks.[41]

Revolutionaries draw on visionary scenarios to articulate the impact of cyber vulnerabilities by considering futuristic "most dangerous" courses of action that lead to defeat of a force. One science-fiction scenario that captures the essence of potential cyber vulnerabilities involves the Borg from the television series *Star Trek: The Next Generation*. Despite the advantages posed by the interconnected nature of the Borg society, their highly integrated being becomes their greatest point of vulnerability. In the episode "The Best of Both Worlds: Part 2," the crew of the *Enterprise* was able to defeat the more powerful Borg adversary by hacking into an unprotected portion of the Borg network and injecting a command that put all the Borg personnel to sleep. The Revolutionary lesson from this scenario is that legitimate system commands may be leveraged by hackers to neutralize a highly sophisticated weapon platform.

As mentioned in the introduction, the potential cyber vulnerability specific to the F-35 fighter aircraft lies in the Autonomic Logistics Information System (ALIS) and its control over aircraft functions.[42] The concerns/fears of defence officials relates to the potential that adversaries will find a way to compromise/exploit the F-35's ALIS and ground the plane or take control away from the pilot to operate the fighter aircraft. A Revolutionist scenario that envisioned similar cyber vulnerabilities in fighter aircraft occurred during the first episode of the 2003 *Battlestar Galactica* miniseries. In the episode, Cylon forces leverage an electronic jamming exploit during their assault to completely neutralize all the computer systems aboard their adversary's seventh-generation Viper fighter spacecraft. In this scenario, the antiquated and lower-tech military platforms operating with closed computer systems such as the Mark 2 Viper were immune from the cyber "kill switch"[43] vulnerability. Such Revolutionist scenarios highlight the potential for concern when employing sophisticated military hardware such as the fifth-generation F-35.

To the members of the Conservative school, referencing science fiction to highlight the concept of a military cyber kill switch does not instill confidence that the concept has any merit. On the other hand, Revolutionaries are able to contemplate possible future outcomes in military affairs without mental restrictions. Conservatives may have doubted the possibility of a military cyber kill switch until the details of the 2007 Israeli Operation ORCHARD were made public.[44] During Operation ORCHARD, the Israeli Air Force performed air strikes on a suspected nuclear reactor in Syria without alerting the Syrians to their location or triggering any air-defence capabilities. The cyber significance of this operation relates to the Israeli Defence Forces' ability to completely suppress the Syrian air defences through cyber and not kinetic techniques. The Israeli Defence Forces employed airborne network-attack technology to take control of the Syrian defence network and subsequently activate a secret kill switch that neutralized the system. The existence of a cyber kill switch for networked military capabilities is no longer the domain of Revolutionary visionaries but a cold hard threat for Conservatives to consider and Liberal Materialists to manage. The cyber kill switch is yet another example of a technological concept that was forecasted by revolutionary science fiction several years before becoming reality in the public domain.

CONCLUSIONS

This chapter considered Revolutionary Materialist perspectives within the cyber warfare schools of thought schema. Revolutionary Materialists are forward-looking visionaries that consider possible future outcomes to better understand the implications of technological changes on society. The Revolutionary approach considers the "most dangerous" trend of technological changes to better develop strategies and responses. While this approach raises the spectre of anarchy and relativism, it also frees individual decision makers from "dogmatic thinking," opening up new paths for creative problem solving. It is the basic belief of Revolutionaries that cyber technology has profoundly altered the praxis if not the nature of warfare. Influenced by luminary writers such as Authur C. Clarke and Marshall McLuhan, Revolutionaries employ technologically influenced scenarios to articulate the complex concepts in relatable terms. Revolutionaries "prepare people to accept the future without pain and to encourage a flexibility of mind."[45]

> TO REVOLUTIONARIES, CYBERSPACE IS THE "NEW HIGH GROUND" FROM WHICH TO EXERT STRATEGIC POWER.

The most materialists of the schools of thought schema, Revolutionaries focus on the affordances offered by cyber capabilities and the impact of technology on humanity. In terms of cyber warfare, Revolutionaries are manoeuvrist warfare advocates emphasizing the advantages of adopting irregular approaches to attacking adversaries' critical vulnerabilities. To Revolutionaries, cyberspace is the "new high ground" from which to exert strategic power. This new high ground also erodes classical hierarchies of control and offers strategic power to non-traditional non-state ideologically inspired groups with cyber exploitation skills. The most dangerous outcomes facing society are cyber-skilled state and non-state actors launching paralysing electronic Pearl Harbors (EPHs) or kill-switch exploitations on key capabilities.

With implications of humanity becoming fully integrated with technology to enhance humankind, the highly technologic agency of the Revolutionary school professes profound changes to the conduct of warfare. Current discussions of cybernetic implants and lethal autonomous weapons offer a certain degree of credibility to the visionary epistemological approach to understanding the implications on humanity. Interestingly, bold Revolutionary visions eventually turn out to be humorously "conservative" as the products of invention and discovery become common place in society.

In the next chapter, this paper explores the fundamental characteristics of the Liberal Materialist school of thought. Liberal Materialists represent the middle ground perspective on the school of thought spectrum. Liberal Materialists also focus on materialism but counterbalance that focus with a Conservative framework of human agency to control the effects of cyber warfare through the power of social institutions. This paper explores how Liberal Materialists leverage pragmatic thought to balance historical and futuristic perspectives to more effectively deal with managing humanity's technologically based social issues and the implications on the praxis of warfare.

CHAPTER 4 – THE LIBERAL MATERIALIST SCHOOL OF THOUGHT

> *Liberalism is trust of the people tempered by prudence. Conservatism is distrust of the people tempered by fear.*[46]
>
> – William E. Gladstone

In many ways, the Liberal Materialist school of thought has been the least visible of the major divisions of reflection on cyber warfare. Liberals have published few manifestos on the issue of cyber warfare and generally have not attracted similar levels of attention.[47] This is because this school of thought is the most expansive of the three, in that it devotes itself to the question of how IT is shaping our society, as opposed to strictly confining itself to the issue of cyber warfare.[48] As such, the Liberal school is hidden within broader studies of Internet governance, privacy and the exploration of the social impact of computing technologies. Nevertheless, within these areas, specific consideration of cyber warfare is often present within these studies given the overlap of issue areas.

Like the Revolutionaries, Liberals share a thread of materialism in their thinking in that their writings emphasize how the technological context is opening up both opportunities and new dangers for individuals, organizations and states. However, Liberal writing lacks the sensationalism and scenarios found in the Revolutionary literature. As their name suggests, Liberals emphasize the agency that accompanies the growth of IT. This agency accrues to everything that IT touches, and so while individuals can take advantage of this, so too can states, non-governmental organizations and even other forms of technology. However, Liberals have little faith that this evolution in technology necessarily points towards classic "liberal"[49] ends or results. Indeed, many argue that without effective state intervention, the results might be decidedly poor for society. Others point to new forms of policy engagement between the state and other actors in mediating these new opportunities. As such, Liberals share with the Revolutionaries that technology is changing society; however, their approach is more evolutionary than revolutionary. There is still space for the state to act in this novel environment, and not all institutions are to be swept away.

LIBERAL ISSUES

The Liberal school shares a heavy materialist focus, like the Revolutionary school. This materialism, however, is tempered by very typical liberal emphasis on issues of freedom, individuality and institutional development. Among Liberals, however, there is little confidence that IT's effect on society will be anything but liberal. As such, there is an equally liberal emphasis on activism and engagement in order to shape technological developments in open-minded and humane directions.

Technology has a critical role in shaping society, according to the Liberal school. Significant changes in how society generally, and international society specifically, is organized stem from the global nature of contemporary digital communication technology. Because these technologies and the companies that provide communication services cross international jurisdiction, efforts to impose controls on them are inherently costly and complex. This is magnified by the growing scale of the communication facilitated by this rapidly evolving technology and the distribution of decision making beyond that of political units. All of this has required new institutions such as ICANN (Internet Corporation for Assigned Names and Numbers) and the IETF (Internet Engineering Task Force) in order to manage the constellations of technologies, service providers, civic society groups and states.[50]

As many writers point out, in function, many of these developments are nothing new.[51] What may be new in these developments is the reflexive change they cause in the interactions between technological advance and human affairs. Digital communications are eminently flexible in their tendency to be repurposed and re-appropriated by communities of interest outside the original design parameters. These successes build upon one another in a manner which ultimately directs the technology into areas not originally anticipated by the designer. As Dan Kuehl remarks, "It is the inseparable linkage of the technology, the human users, and the impact of the interconnectivity in the modern world that differentiates these kinds of information networks from earlier ones—such as the Pony Express of the 1860s—and that hints at cyberspace's future impact."[52] This interaction has produced clashes between the new capabilities offered by technology and the interests of states, in particular. Mueller breaks these conflicts into four areas: intellectual property protection, cyber security, content regulation (concerning pornography, especially that related to pedophilia) and critical Internet resources (the technical security of those resources). These issues raise clear questions of cross-border jurisdiction and governance capacity. As Mueller remarks:

> There is a family resemblance across each of these domains observable in the acute conflict between the capabilities of open global networking and the problem of maintaining boundaries and control. This conflict can only be resolved through changes in the existing institutions governing communication and information.[53]

Many of the challenges posed by digital communications technology, however, have little to do with conflict between states and emerging non-state institutions. Some of the most creative vectors within cyberspace arise from criminal activity, which Ronald Deibert and Rafal Rohozinski remind us is also a form of liberation, often seeking to transcend local limitations stemming from poverty or political inequality.[54] In both cases, however, the interest of the Liberal school of thought is to "uphold the Internet as a forum of free expression and access to information … ."[55] The objectives of this project are "shared agenda of communications security and privacy, freedom of expression, equal access, the protection of an open public domain of knowledge, and the preservation of cultural diversity."[56]

MATERIALISM IN THE LIBERAL SCHOOL

While the goals of the Liberal school are essentially humane in nature, human activity is not necessarily the only or even the most important influence on the behaviour of this medium. As Deibert and Rohozinski note, the physical structure of cyberspace "shape[s] and limit[s] notions of security and risk … the technical character of cyberspace itself is a restrictive factor that shapes the realm of the possible in ways that discourse alone cannot explain."[57] The spread of computers into most aspects of contemporary life has a technological basis which Manuel Castells refers to as "informationalism."[58] Castells argues that informationalism forms the technological basis on which all of the possibilities of the information age are built, composed of the effects of the falling cost and rising power of microprocessors (Moore's Law), the combinatorial effect of networking (Metcalfe's Law) as well as the essential mutability of digital information which allows it to be effortlessly combined in new ways to produce new applications, services and information.[59] Dorothy Denning observes that the consequence of computers in every aspect of our lives is the increasing accessibility of information. The significance of this access cannot be accurately determined given the mutability of that information. However, Denning argues that these increased opportunities to access and manipulate information cannot lead to anything other than an equally increasing opportunity to conduct information warfare.[60] Kuehl argues that the technological basis of cyberspace is changing how one creates information content, how one shares that content and, ultimately, how humans will interact with one another in the future.[61] Finally, Deibert, Rohozinski and Masashi Crete-Nishihata point out that the technological basis of cyberspace will shape the character of conflict that takes place within that domain.[62] Thus, there is a clear prerogative to control the physical infrastructure in order to effectively control the information that flows over its sinews; there will be considerable importance at both the strategic and tactical levels for denying information to opponents. The distributed nature of the medium will incite both outsourcing and "privateering" as well as globalizing any conflict. Finally, the complex nature of the medium will both create and magnify unanticipated outcomes that stem from cyber conflict.[63]

Given the cross-cutting nature of issues arising from the governance of the Internet, it will not only be a resource for those in conflict, but also a contested space itself.[64] Mueller's four issue areas listed above (intellectual property protection, cyber security, content regulation and critical Internet resources) are all ones over the scope of freedom versus the need to regulate content, behaviour and access. However, Deibert and Rohozinski caution against simplifying all conflict over the Internet to a simple binary of liberation versus control. As they note, both liberation and control are socially constructed ideas, the meaning of which varies considerably depending on the political and social context in which they are discussed. Furthermore, not only are the social forces very dynamic, the technological context in which they are deployed is itself constantly changing from moment to moment, making "any portrayal of technology that highlights a single overarching characteristic biases towards either liberation or control seem fanciful."[65]

As such, while the Liberal school points to the critical role of technology in shaping this medium, it is equally insistent that there are no technical fixes to be had in resolving these problems. There are technical problems inherent in the distributed nature of digital technologies and those who deploy and control them, and the Internet's inherent mutable and multifunctional nature makes it innately creative to the whims of those who use it. On top of these fundamental issues, there is the equally intrinsic problem of human conflict in general. Just as the problem of crime has historically resisted "solution" irrespective of the nature of political organization, one should not expect that the extension of traditional human conflict to cyberspace will be any more resolvable than it has been in physical space.[66] At its heart, cyberspace and its security is a multifaceted social problem built on a strong technological foundation.

AGENCY, HUMAN OR OTHERWISE, IN CYBERSPACE

The limitations of a strict materialist approach to cyberspace are evident when one considers that conflict within cyberspace is not about the technology itself, but how it is used by political actors. Kuehl links cyber warfare to earlier forms of conflict by contrasting naval and air warfare with it. Kuehl states:

> A materially based view is clearly inappropriate because the issue is not controlling electrons or electromagnetic forces, but rather influencing the use of cyberspace in the same way that air or naval superiority is not about controlling molecules of air or water but rather controlling how the physical domain is used. It is a measure of effect of impact on human affairs and processes.[67]

Deibert and Rohozinski also compare cyberspace to other military domains, but add that while the technological context constrains human use of it, unlike sea, air, land and space, cyberspace is dependent upon human intervention in order to keep it functioning. As such, the actions of human agency affect its very constitution.[68] However, elsewhere they argue that "communication technologies are neither empty vessels to be filled with products of human intent, nor forces unto themselves imbued with some kind of irresistible agency." Rather, they are the manifestation of dynamic and evolving social forces, which when introduced, reflexively shape and direct the manner in which they will be used, but are also subject to the forces of contingency, innovation and repurposing.[69] In sum, human society, individual creativity, commercial interests and technological affordances all combine together in a complex mix of influences and social dynamics to produce cyberspace. As Carl H. Builder puts it, "not all may seek or elect to exploit the emerging abundance of information, but it is there for the taking, and the power it conveys depends only on the creativity, imagination, and boldness of the individual."[70] Thus, power is there to those who are able to create and use it but it is "a tangled web of rival public and private authorities, civic associations, criminal networks and underground economies"[71] as well as contingencies arising from repurposed technologies and commercial decisions that become political.[72]

DISTRIBUTION OF POWER

Notably then, the Liberal school places particular emphasis on the distribution of power that is being caused by digital technologies. This distributive feature is located in a variety of sources. The very nature of the contemporary communication sector facilitates much of this distributive element. For Mueller, it is located in the increasingly privatized nature of Internet governance, which is a structural response to the limitations of governments to provide for it. Four aspects dominate this march of privatization. The scale of the Internet means that no one person or body can possess complete knowledge of the overall system. Thus, local network operators are best positioned to manage the volume of activity. The rapid advance of technology makes it difficult for the rationalized bureaucracies of modern states to keep pace in terms of both human and capital resources. Again, those with specialized technological know-how are best positioned to provide advice on implementing technologies and management policies. Further, the same rationalized jurisdictions of government bureaucracies makes them poor actors in a policy arena where the issues cross all manner of jurisdictional and policy boundaries. Finally, governments are bound by codes of conduct which private actors are not, thus making them perfect proxies to accomplish what governments otherwise cannot.[73]

Another effect of the increasing computerization of contemporary society is the growth in pure data that is being stored by all manner of applications. This is easily seen in the commonality of gigabyte-sized storage devices and the arrival of terabyte-sized ones in increasing numbers. This challenge demands increasing sophistication in information processing.[74] Studies conducted by Martin Hilbert at the University of Southern California's Annenberg School for Communications and Journalism calculated in 2007 there existed over 300 exabytes[75] of stored data, of which 7 per cent of the data was non-digital (paper, books, photographic prints, etc.)[76] Hilbert further estimates that stored information worldwide in 2013 to be approximately 1200 exabytes with less than 2 per cent of that figure to be non-digital. "The amount of stored information grows four times faster than the world economy, while the processing power of computers grows nine times faster."[77]

"THE AMOUNT OF STORED INFORMATION GROWS FOUR TIMES FASTER THAN THE WORLD ECONOMY, WHILE THE PROCESSING POWER OF COMPUTERS GROWS NINE TIMES FASTER."

Military organizations are also not averse to the challenges presented by big data and the sheer volume of data and information that must be effectively filtered and analysed when conducting modern-day operations. In 2008, the Canadian Forces *Concept of Fusion* paper remarked:

> In order to conduct effective military operations, commanders and respective staffs continually need to understand and accurately predict changes in their battle-space. This means military decision makers need to be able to perceive their environment or battle-space, comprehend their environment, and make projections about the changes that will take place in their environment in order to achieve Situation Awareness (SA). The fundamental challenge facing military decision makers is the selective absorption of pertinent information from numerous and complex sources to efficiently achieve comprehensive SA.[78]

The Canadian Armed Forces (CAF) concept of "fusion" proposed the creation of an automated service by which volumes of "various sources and types of information can be combined to enable commanders and staffs to generate a more informed, coherent 'view' of operational activities that supports their decision-making process."[79] The sought algorithm/service to enable information fusion would employ predictive techniques for big data to propose which sources of information were pertinent for commanders and staffs to develop more profound knowledge and understanding of a particular situation as it unfolds. The "dark side" of such a service relates to the human confidence placed in the sophisticated automated/artificial "intelligence" to determine what information is pertinent to military operations. The dark tendency would be for commanders and staffs to not develop a profound knowledge of the situation but rather rely explicitly on computer-based advice to make potentially lethal decisions. Liberal Materialists must concern themselves with the regulation of automated influence in the development of military advice to ensure that lethal force is not applied solely on the basis of automated mathematical "probabilistic cause."[80]

Scott Knight is another member of the Liberal Materialist school who advises on cyber issues as they relate to military activities. In one of his works, "War by Computer: Canadian Cyber Forces in 2025," Knight acknowledges the need for policy and capabilities in the rapidly evolving cyber domain to protect citizens and military forces from their dependence on information technologies.[81] Knight argues that managing and protecting against cyber threats from an institutional perspective requires more capability than just purchasing the latest commercial security solution. Cyber defences will require a targeted strategy of defence that includes a militarized cadre of skilled cyber forces.[82] Knight admits that commercial intrusion-detection systems and antivirus software are adequate for defending against adversaries employing broad-based attack techniques (indiscriminately attacking everyone) but does little against those adversaries who are specifically targeting the institution. Knight states:

> The most dangerous kinds of adversaries are those who are targeting us specifically. By definition these adversaries are willing to expend the resources, and take the risks, involved in gaining access to our information systems. These are foreign intelligence services, military adversaries, and others, and are our most dangerous opponents.[83]

A solid member of the Liberal Materialist camp, Knight is concerned about institutionally defending against dangerous cyber adversaries that possess the funding, manpower and access to commercial products to develop techniques and capabilities that will defeat standard commercial off-the-shelf perimeter defences.[84] In addition to developing exploits to counter institutional server-side perimeter defences that protect against external attacks, adversaries are also investigating alternate attack vectors such as client-side exploits. The client-side approach attempts to exploit more vulnerable software resident inside the institutional protective perimeter by introducing malicious code at a client computer. Previously, it was felt that if classified computers or command networks were air gapped and isolated from other networks or the Internet they were safe from attack. Client-side attack vectors employ various forms of exploits that can be introduced with removable media across air-gapped systems. Knight introduces the concept of "information flows" as the transfer of information (bidirectional or unidirectional) from one system to another by way of removable media, data diodes, etc.[85] Once an adversary can identify an information flow, it can be exploited as a system vulnerability. Air-gapped classified computers and command networks are no longer safe from malicious codes that exploit an information flow, thus defeating the protection of stand-alone isolation.[86]

In terms of a client-side attack of a network connected to the Internet, the malicious code can be introduced through some benign method such as USB stick, email attachment or a compromised web page. Once the code has been deployed on the unsuspecting system, it will attempt to covertly communicate back to an adversarial individual or group through an information flow. The malicious communication or "covert channel"[87] will attempt to hide within the regular activity of the system or network to avoid detection by system security capabilities. Knight explains that covert channels can establish a back-door communication path with an attacker that can defeat traditional outward-facing firewall and perimeter defences.[88]

Knight also highlights that critical mission systems onboard warships, aircraft and air-defence systems are just as vulnerable to cyberattack.[89] The "credential stealing" virus infection of US Predator and Reaper drone fleets is but one example of a weapon system falling victim to an adversarial cyberattack.[90] There are growing concerns as to the increased vulnerability of sophisticated US weapons systems in light of the known losses of designs for advanced systems to Chinese-sponsored espionage.[91] Publicly, the Pentagon remains confident in its warfighting capabilities despite the compromises of key weapons programmes such as the Patriot missile system as well as the F-22 and F-35 fighter aircraft. "Suggestions that cyber intrusions have somehow led to the erosion of our capabilities or technological edge are incorrect."[92] Nevertheless, "highly connected" warfare strategies that increase the cyber integration of military capabilities also increase the exposure of these capabilities to cyberattack and exploitation.[93]

In addition to state-sponsored cyber warfare, many Liberal writers share similar concerns with the Revolutionaries Arquilla and Ronfeldt with respect to non-state actors. Like their concept of netwar, Liberals discuss how non-state actors, both civil and otherwise, are emerging based on the distributive properties of digital technology. Civic networks were the earliest of adopters for social technologies, in terms of both producing communities of interest and practice as well as in generating financial support. These civic networks are complemented by so-called "dark nets" made up of militant groups, extremists, criminal organizations and terrorists. Deibert and Rohozinski divide these up into armed social movements (Al Qaeda, Hezbollah and Chechen guerrilla organizations) and transnational criminal organizations.[94] The new organizational arrangements prompted by these developments themselves raise novel political issues and governance problems that generate institutional change at the transnational level. The challenges arising from cyberspace involve highly scalable and difficult to trace actions and distributed actors that exceed the ability of the state to control them. This has prompted new organizational arrangements that are beginning to reconstitute relationships between business, government and civil society. However, these new arrangements are themselves problematic in terms of governance and politics. Mueller argues that society is not seeing a reassertion of the state, but rather its gradual adaptation to these new circumstances.[95] Yet, new forms of organization will only enable new forms of collaboration and will not provide actual answers to the questions raised by this new distribution of power: who decides how power is to be authoritatively distributed, what rights accrue to which actors and how is conflict to be resolved? While the state's power has been eroded by digital technology, its role in settling these issues remains paramount.

THE ROLE OF THE STATE

The Liberal Materialist school of thought views the role of the state as the foundation for managing and controlling cyber capabilities in order to protect society from ongoing cyber threats. Liberal Materialists recognize the paradox created by the permeation of cyber technology into the functioning and sustainment of society. On one hand, cyber capabilities offer society effective and efficient opportunities for goods and services as well as opportunities for sharing ideas and information. On the other hand, cyber capabilities offer governments, militaries as well as state-based and non-state actors a powerful new means to exert strategic force that is challenging to defend against, if not impossible to deter.[96] US National Security Strategy also acknowledges the paradoxical situation stating: "The very technologies that empower us to lead and create also empower those who would disrupt and destroy."[97] In the eyes of the Liberal school, the state is responsible for formulating a national cyber strategy and exerting cyber power "to support the attainment of larger objectives … across the elements of national power—political, diplomatic, informational, military and economic."[98] The development of a national cyber strategy requires the state to effectively balance its ends, ways and means to adequately address national cyber-defence and cyber-security threats.[99]

In terms of balancing the ends, ways and means of national strategy, the state must consider national goals that impact domestic as well as international perceptions with respect to the contribution to cyber peace and security.[100] For example, Canadian cyber strategy is comprised of three primary objectives: "securing government systems, partnering to secure vital cyber systems outside the federal Government [and] helping Canadians to be secure online."[101] The role of Department of National Defence and CAF as a derivative of the national cyber strategy is to protect defence infrastructure, identify threats and possible responses as well as maintain cyber-defence relationships with allied militaries.[102] Deibert views Canada's cyber strategy to be rather "thin" in terms of national commitment and overall detail.[103] Deibert argues that governments need to be more aware and active in countering the social forces currently undermining the openness of cyberspace with "assertions of state power, interstate competition, espionage, crime and warfare."[104] As a means to combat the forces that threaten cyberspace (cyber warfare), governments may leverage capabilities and services to conduct state-sponsored surveillance, censorship and information warfare.[105]

Some Liberal Materialists argue national cyber strategy should include both elements of preemption and deterrence.[106] In an article published in the *Washington Post*, Mike McConnell makes the case that, depending on the threat facing the US, it should be able to employ both preemption and deterrence to defend its interests.[107] Following in McConnell's train of thought, other Liberal Materialists believe that "the laws of armed conflict can be widened to embrace Cyber Warfare in order to allow the US to respond with the use of force against aggressive assaults on its computer and IT infrastructure."[108] Classifying a cyberattack as an act of war allows the state to use both cyber- and kinetic-response capabilities as coercive means of deterrence. The US's 2015 "National Security Strategy" leaves the door open to all available state response capabilities stating: "On cybersecurity, we will take necessary actions to protect our businesses and defend our networks against cyber-theft of trade secrets for commercial gain whether by private actors or the Chinese government."[109] The Liberal Materialist school, being the middle ground between Conservatives and Revolutionaries, employs elements of both schools to manage cyber-warfare issues. In the case of military responses to cyberattacks, Liberal Materialists acknowledge cyber activities have political and ontological significance and look to established Conservative frameworks of control to manage behaviour and deter inappropriate activity. In the case of national cyber-defence strategy, strategic-thinking Liberal Materialists are investigating aspects of *jus ad bellum* or "the rules that regulate the use of armed force by states in their international relations."[110] Chapter VII to the Charter of the United Nations deals with actions with respect to threats to the peace, breaches of the peace and acts of aggression. Article 51 states:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.[111]

But invoking *jus ad bellum* in response to malicious cyber activity is problematic due to well-known challenges of action attribution and actor identification.[112] There exists a legal obligation to identify the perpetrator of a cyber-incident as well as verify it did not occur accidentally.[113] Therefore, the major issue with justifying action based on cyberattack self-defence is the proof linking aggressor with action.[114]

ONE COLLABORATIVE STEP TOWARDS SECURITY AND CIVILITY WOULD ENTAIL THE CREATION OF AN INTERNATIONAL CYBERSPACE TREATY AS AN EXTENSION OF THE LAW OF ARMED CONFLICT.

In response to Liberal Materialists concerns about the unmanageable characteristics and architecture of the Internet, some senior US government officials have proposed constructing a more secure and protected enclave within the "supposed lawless Wild West of the Internet."[115] Others suggest, however, that the Internet should be re-engineered to ensure geolocation and attribution are inherent in the Internet's architecture as a means of deterrence.[116] Unfortunately, the idea of redesigning the Internet and starting afresh is an extremely costly proposal that does not guarantee success in achieving specific security goals.[117] Furthermore, there are mounting concerns with the political leadership militarizing cyberspace and seeking to create their own "cyber Manhattan Project to build weapons" instead of pursuing collaborative security through alliances and partnerships to resolve international and interrelated cyber issues.[118]

One collaborative step towards security and civility would entail the creation of an international cyberspace treaty as an extension of the Law of Armed Conflict. The likelihood of misinterpreted actions potentially leading to conflict is increased in the absence of any international agreements establishing the standards of cyber conduct and what constitutes armed attack in cyberspace.[119] Such a treaty would also pave the way for a universal application of constabulary functions by police forces to control nefarious activity.[120]

Alison Lawlor Russell, in her book *Cyber Blockades*, extends the traditional Law of Armed Conflict relating to physical blockades to a state-sponsored activity in cyberspace. Based on the alleged Russian cyberattacks on Estonia in 2007[121] and on Georgia in 2008,[122] Russell explores the implications of state-sponsored applications of cyber force as a means of national power to "shut down, close off, or otherwise render cyberspace useless for an entire country."[123] Traditionally regarded as acts of war, blockades in cyberspace represent an expedient, low-cost method to punish an adversary through denial of services connected to the Internet. In addition, depending on the context of application, cyber blockades may not always represent an act of war due to the passive nature of the act.[124] Interfering with state sovereignty and the freedom of action within its own territory, cyber blockades represent a potentially strong coercive measure short of war. Nevertheless, cyber blockades at present are a significant challenge for Liberal Materialists to manage in the absence of an international cyber treaty or codification into international law.

Finally, the role of the state from the perspective of Liberal Materialists involves commitment and resources to respond to growing cyber-defence and cyber-security issues. Governments need to invest in not only technology but also human capital.[125] Misha Glenny argues a similar point in her book *DarkMarket: How Hackers Became the New Mafia*: "Computers and networks will never be safe if they are not protected by advanced hackers."[126] Knight makes the same case for the CAF of the future by calling for the creation and development of highly educated cadre of skilled cyber forces to complement existing automated defences.[127] Investment in developing human cyber expertise is also a tenent of the US military's cyber strategy to establish the organizational and training framework to generate and employ cyber forces in an active and layered capacity.[128] Unfortunately, Liberal Materialists must contend with the challenges of competing national imperatives in order to secure the required resources for an effective cyber-defence strategy.

CONCLUSIONS

This chapter considered Liberal Materialist perspectives within the cyber warfare schools of thought schema. The most expansive of the three schools of thought, Liberal Materialists are devoted to managing and controlling how IT is shaping our society. The issues relating to cyber warfare are just a derivative of the broader social scope concerning the Liberal Materialist school. Liberals fully accept that technology is changing society, but view technological changes as more evolutionary than revolutionary in nature. Liberals have little faith in IT's impact on society and believe that technology must be governed if humanity is to positively evolve with technologic discoveries and advances. In terms of cyber, Liberals attempt to balance the desire for net neutrality with required controls to ensure appropriate use and conduct. Liberals approach the impact of cyber activities on society with guarded prudence instead of succumbing to the Conservative fears of the unknown.

To shape the character of conflict in cyberspace, Liberals must not only control the physical infrastructure supporting cyber but also consider potential actions that could deny an adversary access to information or deny freedom of action with the domain. Cyber warfare represents a wicked problem for Liberals to solve, as the globalizing nature of cyber invites a host of additional non-traditional actors to aggravate and amplify unanticipated strategic outcomes. Technology is a critical factor in shaping cyberspace, but resolving the problem of protection, control and governance is a social challenge. Governments and states are bound by international law while non-state or private actors act with little worry of prosecution. With issues of attribution and identification plaguing cyberspace, private actors make perfect proxies for state-sanctioned cyber warfare.

Warfare strategies that increase the cyber integration of military capabilities also increase the exposure of these capabilities to cyberattack and exploitation. Liberals must be prudent and practical in their approach of ensuring that traditional warfare means that have been enhanced with highly integrated cyber capabilities are not compromised in time of need. Knowing that air-gapped, classified command-and-control systems are vulnerable to client-side attacks despite commercial security products, Liberal strategies must include the investment of human capital to develop and leverage the necessary skills to ensure governments can adequately protect citizens and their interests in time of conflict.

Liberal Materialists view the state as the foundational element in protecting society from cyberspace threats. Liberals must contend with the paradoxical nature of cyber capabilities on society. Governments need to adopt a Liberal Materialist approach in order to more effectively balance the ends, ways and means of national power to adequately address cyber-security threats on behalf of its citizens. Given the effects of globalization and the interconnected nature of cyber on international relations, Liberal Materialists must influence states and governments to collaborate internationally to enhance the existing framework of international law, including the Law of Armed Conflict, to include cyber activities. Cyber warfare need not be conducted in the shadows but should be officially recognized as a means of national power that can be managed and controlled.

In the next and final chapter, this paper explores the key points extracted from the application of the cyber warfare schools of thought schema on the survey of available literature and considers how an institution may approach bridging the epistemological/ontological divide. In addition, this chapter articulates some thoughts and recommendations for CAF leadership facing the challenges of operating forces integrated with the cyber environment in the execution of defence activities and the need for epistemological normalization to effectively bridge the divide.

CHAPTER 5 – CONCLUSION

At the close of this discussion of the different cyber warfare schools of thought, the essential questions that began this inquiry remain unanswered: What is to be done? What course of action should militaries and governments follow? Has the proposed cyber warfare schools of thought schema bridged the epistemological/ontological divide? Completing a survey of cyber literature and subsequently categorizing the different points of view, it becomes obvious that there is a basic lack of agreement on the nature of the threat posed by IT to the security of states, organizations and individuals. Each school has its own tensions and contradictions in addressing the social problem of technologic influence. Approaching the social problem with dissimilar cognitive lenses, the different schools interpret the social problem uniquely and subsequently derive distinctive social explanations for each of the unique problems. In essence, there is an epistemological divide which prevents a fundamental assessment on the ontological meaning of cyber events for considering long-term security issues.

Revolutionaries often pose the most dangerous apocalyptic scenarios or herald occurrences of technology-led Revolutions in Military Affairs (RMAs) that easily catch the attention of politicians, journalists and worrywarts of every description. However, the absence of an EPH as yet; the failure of extant information attacks to pose any sort of wider threat aside from nuisance value; and the difficulty in measuring the effect of compromised information due to subversion, espionage and sabotage all suggest the problematic nature of some of this school's predictions. In his book *Strategy for Chaos*, Colin S. Gray also takes a dim view of agents professing such revolutionary promotion, remarking "RMA advocacy literature can be linked to monkeys making chess moves and parrots repeating clever phrases. The monkeys and parrots may well perform accurately, but they will not understand the meaning of what they are doing."[129] Furthermore, the assumption of widespread social chaos seems ahistorical in nature and may be reflective of broader philosophical assumptions and biases unrelated to the issue of warfare. In the experience of the Second World War, the use of air power failed to achieve the results that were predicted of it by earlier air power theorists such as Giulio Douhet. In the case of both Britain and Germany, the populations did not protest, riot or demand a cessation of hostilities in the face of aerial bombardment. While the use of nuclear weapons seems to have confirmed the predictions of air power theorists, there was considerable debate within the Japanese leadership on whether to surrender based on imperial strategic considerations and not due to the atomic bomb's influence on Japanese society. The recent events in Japan following the tsunami and nuclear meltdowns at Fukushima in 2011 did not result in widespread panic. Furthermore, the power outages associated with the ice storm in 1998 and the North American blackout during the summer of 2003 did not lead to widespread chaos, despite the length of time both events took to be resolved. Nor do Revolutionaries provide any psychological or social theory to justify their assumption that the effects of an EPH or Digital 9/11 would lead to the widespread social chaos that their scenarios describe. All of these suggest problems with the most dangerous assumptions made by Revolutionaries.

TOUTING THE ADVANTAGES OF OFFENSIVE OVER DEFENSIVE CYBER-WARFARE CAPABILITIES, SPECIAL INTERESTS ADVANCING CYBER WARFARE AGENDAS NOW REPRESENT A NEW CYBER MILITARY-INDUSTRIAL COMPLEX.

The Liberal school of thought seems more pragmatic and eminently more reasonable. It describes conditions which are clearly visible in everyday life in terms of its assessment of technological change. The disruptive effects of compromised cyber capabilities on industries such as Sony Studios in 2014 are easily visible, even to those not familiar with academic debates. Nevertheless, Liberals must contend with several securitization actors that play on society's fears of the unknown and attempt to prejudice the pragmatic threat assessments of the Liberal school. Special interest groups such as lobbyists and corporations are often accused of leveraging their influence for commercial gain. Lobbyists and corporations that promote unnecessary defence spending and place corporate gains ahead of public welfare are commonly referred to as a military-industrial complex. Touting the advantages of offensive over defensive cyber-warfare capabilities, special interests advancing cyber warfare agendas now represent a new cyber military-industrial complex. Feasting on a climate of fear and insecurity of the unknown cyber threat, the cyber military-industrial complex has been increasingly successful at proliferating tools and services and creating the conditions for a new arms race. Cyber-weapon escalation in the form of a cyber arms race self-generates additional threats that primarily serve the financial interests of the cyber military-industrial complex. Still, the Liberal school lacks precision in addressing cyber threats as well as the special interests of the cyber military-industrial complex. Furthermore, the fundamental debate over its core imperative (liberal freedom versus state control) limits the Liberal school's utility in terms of understanding the changes affecting warfare and the reassessment of traditional military praxis.

While many of the objections raised against the materialist schools of thought would seem to imply the relative correctness of the Conservative position, it may underestimate the threat posed by cyber warfare. Consistent with the dangers of Black Swan Theory and Hume's Induction Problem, by focusing on the constancy of warfare, it may miss the outlier changes that might ultimately lead to a shift or fundamental revolution in military affairs. An intellectual born out of the Romantic era, Clausewitz viewed war and human affairs as entities apart from scientific rules and principles. He sought to explain the impact of morale and military genius, such as Napoleon, on the practice of warfare. Clausewitz was writing against earlier military-based Enlightenment theory, which was attempting to provide a scientific basis for the conduct of warfare and characterize the praxis of 18th century warfare through the tools of geometry. Thus, while Clausewitzian thought provides the benchmark for analysing the presence of change in warfare, Clausewitz, himself, was writing of fundamentally revolutionary events and how they had changed the nature of warfare from what it had been prior to Napoleon. If society is, in fact, going through social shifts as momentous as those created by the conditions of Industrialism and the Enlightenment, then the Conservative school of thought, with its emphasis on the incremental/evolutionary rather than revolutionary value of IT, may miss the changes that are all around us.

It is important to note that the ontological issues concerning the crisis of modernity are far broader than simply the changes in the military cyber warfare environment or even of IT itself within the social conditions of "post-industrial" society. As far back as the 1960s, authors such as Marshall McLuhan were noting that important technological social shifts were underway that were likely to cause significant shifts in how society functions. One needs to understand the nature of IT and its broader social dimensions. This will permit the discussion to escape the cage in which it has been placed by the parameters of the technology-led RMA debate. Instead, one must consider the implications and social consequences given the ontological changes to the very being of society. In doing so, one calls upon the value of the out-of-the-box perspectives of the Revolutionary school to extrapolate clear guideposts and cautionary tales of a technologically determinist society. Cellular telephone culture—derived from the revolution in mobile personal communications—is but one example of society's technological determinism. The growing impatience to move information more quickly and always be connected with society is the foundation of individuals' addictions to personal communications.

A consideration of the epistemological issues confronting those who wish to use cyberspace as a new vector for state action must be dealt with before one can be secure in moving forward with this capability. The essential mutability of IT poses concrete challenges to the use of this technology to achieve political ends in the manner warfare has traditionally functioned. Strategic advantages derived from the exploitation of cyberspace have been difficult to identify. The nature of the epistemological challenges may pose as many opportunities as barriers for those who can take advantage of them. For governments and militaries such as CAF to resolve the epistemological dilemma, they must first embrace the technologic influences and changes on society's ontology. Institutions must be honest in their assessment of the social dimensions influenced by technology. For command chains, this entails an introspective look at what cyber technology means for the being of people and organizations and the ontological significance on the existing praxis of warfare. This also means accepting that the military operating environment has increased in complexity with the introduction of cyber capabilities and exploits. The debate of whether cyberspace is a unique warfighting domain or harmonized with the traditional warfighting domains remains outside the scope of this paper. Nevertheless, the acceptance that a warfighter's ontology involves interacting and employing cyber capabilities is a significant step towards bridging the epistemological/ontological divide.

The proposed cyber warfare schools of thought schema can, in fact, bridge the epistemological/ontological divide. Having accepted that society's ontology has changed, militaries such as CAF must develop a pragmatic and comprehensive cyber-warfare strategy that not only complements traditional warfighting capabilities but also addresses the threat realities of the current modern world with responses up to and including military force. From the schools of thought schema, this would entail CAF adopting a Liberal Materialist perspective in drafting such a strategy. For a traditionally conservative organization, such a shift in perspective may be difficult and require a shift in institutional culture. In educational terms, this may entail a better balance/mix of leadership backgrounds ranging from conservative defence studies (social sciences) to liberal-rooted scientific and engineering studies (applied sciences). This does not mean that all the traditional values in the Conservative school will be lost, but rather, they will be enhanced with Liberal and potentially some Revolutionary Materialist inspired insights. A consolidated and well-rounded perspective of cyber warfare derived from the school of thought schema will empower CAF to be more versatile and responsive to known and unknown cyber threats. The use of the cyber warfare schools of thought schema should not be approached from a purely quantum perspective, labeling people and organizations by discrete schools that never change. The cyber warfare schools of thought schema is a spectrum that can be leveraged and employed as the situation demands. Nevertheless, the anchor of CAF's strategy needs to be unified and clearly solidified on Liberal Materialists values if it is ever going to effectively bridge the epistemological/ontological divide.

Leveraging the proposed typology, one can conclude that cyberspace is a working space that traverses the divide between a purely technologic base of knowledge and the state of society's being. For society to effectively resolve its own social epistemological dilemma, it must find resolution in the questions relating to the meaning and significance of cyberspace. The social nature of knowledge must be tempered by the understanding of what society has become. No longer the exclusive territory of science fiction, cyberspace is a reality from which society's existence is supported. In order to dispel its fears of cyber technology, society in general must demand that its government be more transparent about the threats and the ends, ways and means of national strategy that are being used to protect everyone against misuse, abuse and anarchy.

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

ALIS	Autonomic Logistics Information System
CAF	Canadian Armed Forces
EPH	electronic Pearl Harbor
IT	information technology
RMA	Revolution in Military Affairs
SA	situation awareness
SIW	strategic information warfare
US	United States

NOTES

[1] Wayne M. Hall, *Stray Voltage: War in the Information Age* (Annapolis, MD: Naval Institute Press, 2003), 2.

[2] John R. Boyd, "The Essence of Winning and Losing" (lecture notes, 1996).

[3] Hall, *Stray Voltage*, 2.

[4] Ibid., 9.

[5] Ibid., 3.

[6] Ibid., 3–4 and 9–10.

[7] Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, Distributed by Publishers Group West, 1994), 82.

[8] Ibid., 82–85.

[9] Hall, *Stray Voltage*, 4.

[10] Ibid., 5.

[11] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA: O'Reilly Media Inc., 2011), 2.

[12] Ibid.

[13] John Arquilla and David F. Ronfeldt, "Cyberwar is Coming!," Vol. P-7791 (Santa Monica, CA: RAND Corporation, 1992).

[14] Other works by John Arquilla and David F. Ronfeldt: *The Advent of Netwar* (1996); *In Athena's Camp: Preparing for Conflict in the Information Age* (1997); *Networks and Netwars: The Future of Terror, Crime and Militancy* (2001); and *Netwar Revisited: The Fight for the Future Continues* (2002).

15. Arquilla and Ronfeldt, "Cyberwar Is Coming!," 28.

16. Ibid., 30.

17. John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica, CA: National Defense Research Institute, RAND, 1996), 5–6.

18. Ibid., 14.

19. Ibid.

20. Ibid., 5. Arquilla and Ronfeldt define netwar as an "emergent form of conflict (and crime) at societal levels, short of war in which the protagonists use network forms of organization and related doctrines, strategies and technologies attuned to the information age."

21. Ibid., vii.

22. "Some vigilantes are affiliated with loosely knit hacking organizations like Anonymous, known more for infiltrating computer networks of governments and corporations to make political statements or for the 'lulz'—the hacker term for laughs." From Rick Gladstone, "Behind a Veil of Anonymity, Online Vigilantes Battle the Islamic State," *New York Times*, March 24, 2015, accessed July 4, 2016, http://www.nytimes.com/2015/03/25/world/middleeast/behind-a-veil-of-anonymity-online-vigilantes-battle-the-islamic-state.html?ref=topics&_r=0.

23. John Pollock, "How Egyptian and Tunisian Youth Hacked the Arab Spring," *MIT Technology Review*, August 23, 2011, accessed July 4, 2016, http://www.technologyreview.com/featuredstory/425137/streetbook/.

24. Carr, *Inside Cyber Warfare*, 5.

25. Arquilla and Ronfeldt, *Cyberwar is Coming!*, 44.

26. Arquilla and Ronfeldt, *The Advent of Netwar*, vii.

27. Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001), 22.

28. Ibid., 99–100.

29. For a discussion on technological determinism, see Joelien Pretorius, "The Technological Culture of War," *Bulletin of Science, Technology & Society* (2008).

30. Schwartau, *Information Warfare*, 20–22.

31. 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), 74–82.

32. Ibid., xi.

33. Arquilla and Ronfeldt, *Cyberwar is Coming!*, 27.

34. Arquilla and Ronfeldt, *The Advent of Netwar*, 13.

35. John Arquilla and David Ronfeldt, "A New Epoch—and Spectrum—of Conflict," in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND Corporation, 1997), 5.

36. Arquilla and Ronfeldt, *The Advent of Netwar*, 13.

37. Hacking is being used in the sense that the term was originally used by programmers, as "an expert or enthusiast" who understands how a system works and how it can be manipulated to perform tasks. See Pekka Himanen, *The Hacker Ethic: A Radical Approach to the Philosophy of Business* (New York: Random House, 2009).

38. John Arquilla and David Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND Corporation, 2001), 14.

39. Schwartau, *Information Warfare*, 53.

40. Sally Adee, "The Hunt for the Kill Switch," IEEE Spectrum 45, no. 5 (May 2008): 34–39.

41. 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.

42. 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/.

43. Adee, "Hunt for the Kill Switch."

44. Erich Follath and Holger Stark, "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor," *Speigel Online*, November 2, 2009, accessed July 4, 2016, http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html; and John Leyden, "Israel Suspected of 'Hacking' Syrian Air Defences: Did Algorithms Clear Path for Air Raid?," October 4, 2007, accessed July 4, 2016, http://www.theregister.co.uk/2007/10/04/radar_hack_raid/.

45. Jerome Agel, *The Making of Kubrick's 2001* (n.p.: New American Library, 1970), 300.

46. ThinkExist.com, accessed July 4, 2016, http://thinkexist.com/quotation/liberalism_is_trust_of_the_people_tempered_by/227359.html.

47. One exception to this rule has been the explorations of Ron Deibert and his CitizenLab at the University of Toronto. They have published several studies concerning Internet censorship, privacy and hacking that have been well publicized within the international media. While studies such as Ghostnet have not been explicitly about cyberwarfare, the implications of that study raise many important issues of computer security, the role of cyber-espionage and the breach of privacy that resonate strongly within the area of cyberwarfare. See Ronald J. Deibert, *Black Code: Inside the Battle for Cyberspace* (Toronto: Signal, 2013).

48. Lawrence Lessig, "The Law of the Horse: What Cyberlaw Might Teach," *Harvard Law Review* (1999): 501–49. See also Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven, CT: Yale University Press, 2006); Manuel Castells, *The Rise of the Network Society: The Information Age: Economy, Society, and Culture*, Vol. 1 (Toronto: John Wiley & Sons, 2011); Jonathan Zittrain, *The Future of the Internet and How to Stop It* (New Haven, CT: Yale University Press, 2008); and Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (Toronto: Knopf, 2011).

49. Liberal as a derivative of liberalism: The belief in the value of social and political change in order to achieve progress. From "Liberalism," Merriam-Webster, accessed July 4, 2016, http://www.merriam-webster.com/dictionary/liberalism.

50. Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: MIT Press, 2010), 5. See also Milton Mueller and Brenden Kuerbis, "Towards Global Internet Governance: How to End US Control of ICANN without Sacrificing Stability, Freedom or Accountability" (paper, TPRC 42: The 42nd Research Conference on Communication, Information and Internet Policy, August 27, 2014).

51. Vincent Mosco, *The Digital Sublime: Myth, Power, and Cyberspace* (Cambridge, MA: The MIT Press, 2004), 1. See also Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (Toronto: Knopf, 2011), 37; and James Gleick, "Cyber-Neologoliferation," *The New York Times Magazine* (November 5, 2006), 6.

52. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security* (Washington, DC: National Defense University Press, 2009),

53. Mueller, *Networks and States*, 6.

54. Ronald Deibert and Rafal Rohozinski, "Liberation vs. Control: The Future of Cyberspace," *Journal of Democracy* 21, no. 4 (2010): 48.

55. Ronald J. Deibert and Rafal Rohozinski, "Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet," in *Access Denied: The Practice and Policy of Global Internet Filtering*, ed. Ronald J. Deibert et al. (Cambridge, MA: MIT Press, 2008), 127.

56. Ibid., 127–28.

57. Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4, no. 1 (2010): 18. See also Martin C. Libicki, "Global Networks and Security: How Dark Is the Dark Side?" in *The Global Century: Globalization and National Security* (Washington, DC: National Defense University Press, 2001): 816; and Lawrence Lessig, "Code is Law," in *Code* (New York: Basic Books, 2006).

58. Manuel Castells, *The Network Society: A Cross-Cultural Perspective* (Northampton, MA: Edward Elgar Publishing, Inc., 1996), 7.

59. Ibid.

60. Dorothy E. Denning, *Information Warfare and Security* (Reading, MA: Addison-Wesley, 1999), 15.

61. Kuehl, "From Cyberspace to Cyberpower," 32–33.

62. Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War," *Security Dialogue* 43, no. 1 (2012): 4.

63. Ibid., 5–6.

64. Mueller, *Networks and States*, 12.

65. Deibert and Rohozinski, "Liberation vs. Control," 44.

66. Mueller, *Networks and States*, 162–63.

67. Kuehl, "From Cyberspace to Cyberpower," 37.

68. Deibert, Rohozinski, and Crete-Nishihata, "Cyclones in Cyberspace," 2.

69. Deibert and Rohozinski, "Liberation vs. Control," 44.

70. John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, Vol. MR-880 (Santa Monica, CA: RAND, 1997), 95.

71. Deibert and Rohozinski, "Liberation vs. Control," 46.

72. Ibid., 45.

73. Mueller, *Networks and States*, 211. See also Deibert and Rohozinski, "Risking Security," 16.

74. Robert Latham and Saskia Sassen, *Digital Formations: IT and New Architectures in the Global Realm* (Princeton, NJ: Princeton University Press, 2009), 13.

75. One exabyte is 1x10^{18} bytes or 1 billion gigabytes.

76. Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution that Will Transform How We Live, Work and Think* (Montreal: Houghton Mifflin Harcourt, 2013), 20.

77. Ibid.

78. Paul Martin, Jim Hutton, and Loren Klimchuck, *CF Concept of Fusion* (Department of National Defence / Canadian Forces, August 7, 2008), 1.

79. Ibid.

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

81. S. Knight, "War by Computer: Canadian Cyber Forces in 2025," in *The Canadian Forces in 2025 Prospects and Problems*, ed. J. L. Granatstein (n.p.: FriesenPress, 2013), 74.

82. Ibid., 75.

83. Ibid.

84. Ibid., 76.

85. Ibid., 77.

86. Geoffrey Ingersoll, "US Navy: Hackers 'Jumping the Air Gap' Would 'Disrupt the World Balance of Power,'" *Business Insider*, November 19, 2013, accessed July 4, 2016, http://www.businessinsider.com/navy-acoustic-hackers-could-halt-fleets-2013-11.

87. "Covert channels are unexpected and hidden communication paths embedded within a communication system that violates the system security policy. Covert communication occurs when a user or application deliberately manipulates and embeds information into some property of a communication system in such a way that the embedded information is not apparent to the legitimate users of the communication system. Internet based covert channels with low bit rates are enough to convey critical information such as network encryption keys or system access codes." From Paul E. C. Martin, "Covert Channels in Secure Wireless Networks" (master's thesis, Royal Military College of Canada, 2007), v.

88. Knight, "War by Computer," 77.

89. Ibid., 79.

90. 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/; and Alex Knapp, "America's Drones Have Been Infected by a Virus," *Forbes*, October 8, 2011, accessed July 4, 2016, http://www.forbes.com/sites/alexknapp/2011/10/08/americas-drones-have-been-infected-by-a-virus/.

91. "China Cyberattack: US Weapons Systems Breached," *Sky News*, May 29, 2013, accessed July 4, 2016, http://news.sky.com/story/1096826/china-cyberattack-us-weapons-systems-breached.

92. Pentagon Press Secretary George Little quoted in ibid.

93. Knight, "War by Computer," 79.

94. Deibert and Rohozinski, "Risking Security," 21–24. See also Deibert and Rohozinski, "Good for Liberty," 130.

95. Mueller, *Networks and States*, 182–83.

96. David Betz, Tim Stevens, and International Institute for Strategic Studies, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (New York: Routledge, for the International Institute for Strategic Studies, 2011), 10.

97. US, Executive Office of the President of the United States, *National Security Strategy of the United States, May 2010* (Washington, DC: US Government Printing Office, 2010), 27.

98. Betz, Stevens, and International Institute for Strategic Studies, *Cyberspace and the State*, 44.

99. Daniel Ventre, ed., *Cyber Conflict: Competing National Perspectives* (Hoboken, NJ: John Wiley & Sons, 2013), 297.

100. Ibid., 298.

101. Canada, Department of Public Safety, "Action Plan 2010–2015 for Canada's Cyber Security Strategy" (Ottawa: Canada Communication Group, 2013), 1.

102. Canada, Department of Public Safety, "Canada's Cyber Security Strategy" (Ottawa: Canada Communication Group, 2010), 10.

103. Ron Deibert, "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace," *Journal of Military and Strategic Studies* 14, no. 2 (2012): 2.

104. Ibid., 23.

105. Ibid.

106. Mike McConnell, "Mike McConnell, on How to Win the Cyber-War We're Losing," *Washington Post*, February 28, 2010, accessed July 4, 2016, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.

107. Ibid.

108. Ed Pilkington, "Washington Moves to Classify Cyber-Attacks as Acts of War," *The Guardian*, May 31, 2011, accessed July 4, 2016, http://www.theguardian.com/world/2011/may/31/washington-moves-to-classify-cyber-attacks.

109. US, Executive Office of the President of the United States, "National Security Strategy" (Washington, DC: US Government Printing Office, February 2015), 24.

110. Marco Roscini, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force," *Max Planck Yearbook of United Nations Law* 14 (2010): 88.

111. United Nations, "Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression," in *Charter of the United Nations*, accessed July 4, 2016, http://www.un.org/en/sections/un-charter/chapter-vii/index.html.

112. Roscini, "World Wide Warfare," 88.

113. Ibid., 119.

114. Ibid.

115. P. W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 167.

116. McConnell, "Mike McConnell on How to Win."

117. Singer, *Cybersecurity and Cyberwar*, 175.

118. Ibid.

119. Benjamin Mueller, "The Laws of War and Cyberspace on the Need for a Treaty Concerning Cyber Conflict," Strategic Update 14.2 (London, UK: The London School of Economics and Political Science, June 2014), 16.

120. Singer, *Cybersecurity and Cyberwar*, 185–93.

121. Alison Lawlor Russell, *Cyber Blockades* (Washington, DC: Georgetown University Press, 2014), 75–78.

122. Ibid., 103.

123. Ibid., 5.

124. Ibid., 145.

125. William J. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* (September/October 2010): 5.

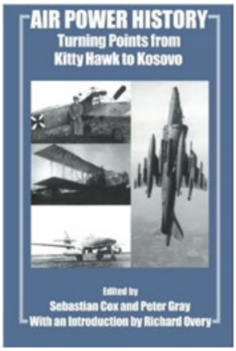
126. Misha Glenny, *DarkMarket: How Hackers Became the New Mafia* (n.p.: Random House, 2012), 271.

127. Knight, "War by Computer," 74.

128. Lynn, "Defending a New Domain," 6.

129. Colin S. Gray, *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History*, Vol. 2 (Portland, OR: Frank Cass, 2002), 280.

BOOK REVIEWS


AIR POWER HISTORY
Turning Points from Kitty Hawk to Kosovo
Edited by
Sebastian Cox and Peter Gray
With an Introduction by Richard Overy

AIR POWER HISTORY: TURNING POINTS FROM KITTY HAWK TO KOSOVO

COMD RCAF'S READING LIST

Edited by Sebastian Cox and Peter Gray

Portland, OR: Frank Cass Publishers, 2005
362 pages
ISBN 978-1-13531-598-6

Review by **Lieutenant-Colonel Pux Barnes, CD, MA**

When the selection process began for a series of books to be considered for the Commander Royal Canadian Air Force's Reading List 2016, the staff of the Canadian Forces Aerospace Warfare Centre (CFAWC) was faced with a considerable task. The current body of knowledge is rich with histories detailing the rapid rise of air power as well as its many successes and failures. While the reading list is flush with books that cover specific conflicts and phases of air power's past, one book stands out as a guide that helps the reader to see how the key events of the first century of flight have shaped today's air forces. *Air Power in History: Turning Points from Kitty Hawk to Kosovo*, edited by Sebastian Cox and Peter Gray, offers both the casual and informed reader a balanced chronology of air power in a way that shuns the common "myths, fables and legends"[1] all too often associated with the story of flight. Where this book succeeds is in its honest approach in presenting the turbulent experience of air power during the 20th century's conflicts; it sheds light on the occasions where air power both delivered and did not deliver on its promises and expectations—and indeed where it learned and matured.

The book is a compilation of 17 papers presented at a historical conference held at the Royal Air Force Museum at Hendon, United Kingdom, in 2001. The theme of the book mirrors that of the conference by attempting "to examine the events and experiences, from the First World War to Kosovo, which have shaped present-day thinking on the use of air power and the evolution of modern doctrine."[2] Seen as a whole, the papers form a well-researched and sober historical record of air power's experience. When considered individually, each paper provides analysis that helps the reader appreciate the relevance of each turning point from the earliest days of the First World War to the North Atlantic Treaty Organization's (NATO's) Operation ALLIED FORCE in 1999.

The book, an engaging study of both the well-known and the oft-neglected events of air power's roles in modern conflict, should rightfully have a place on the shelves of any library or on the desk of any student of air power.

The book is divided into four parts covering (1) the First World War and interwar years, (2) the Second World War, (3) the First Gulf War in 1991 and (4) regional conflicts. The editors offer between three and seven papers per part on various aspects of conflict, and each paper paints a vivid picture of how the people and technology associated with air power made a lasting impact on modern combat and how warfare was conducted at the beginning of the current century.

Part 1 deals with the period of 1914–1939 and includes papers such as "Learning in Real Time: The Development and Implementation of Air Power in the First World War" by Dr. Tami Biddle, a military historian and professor at Duke University, and "The Royal Naval Air Service: A Very Modern Service" by Dr. Christina Goulter, senior lecturer at King's College London. Both of these studies provide ample analysis of the lessons that air power was learning for the first time, as it was forced to adapt quickly to rapidly evolving technology and battlefield demands. Biddle observes that although the airplane had long been anticipated in the popular literature of the day, "there was no consensus on the role that aeroplanes would play in the coming war,"[3] and focuses her study on the various roles air power assumed, from artillery spotting to bombing.

The interwar period resulted in a broad schism that saw significantly differing opinions of what air power was best suited for. Seen on par with tanks, air power was widely viewed by army generals such as Pershing, Foch and Haig merely as *valuable support* to the established military of infantry, artillery and the navy. Meanwhile, as James Corum writes in "The *Luftwaffe* and Lessons Learned in the Spanish Civil War," the lightning-fast pace of German air power innovation to include strategic bombing, mass airlift of troops and the forerunner of blitzkrieg's close air support came of age and would eventually take the Allies by surprise a short time later in 1939. Despite valuable experience gained at both the tactical and operational levels during the Spanish Civil War, Corum reminds us that German leadership seemed to forget these lessons learned once the Second World War began. They failed to capitalize on the value of strategic bombing; for example, during the Battle of Britain, when they switched from targeting Royal Air Force airfields and radar installations in the summer of 1940 to bomb London, it "was another of the grand strategic mistakes of the Second World War."[4]

In Part 2, there is no trouble agreeing with the general assertion that the Second World War was a major turning point for air power. Seven articles are offered, ranging from naval, desert, strategic bombing, logistics and army perspectives, all supporting the idea that air power made profound advancements in technology and application. In "Maritime Air Power and the Second World War: Britain, the USA and Japan," Professor John Buckley from the University of Wolverhampton provides strong evidence that together with the backing of American industrial might, air power was the key ingredient in the long-term success of the United States Navy in the Pacific and the eventual defeat of Japan. Dr. Brad Gladman, then of the University of Calgary and currently of CFAWC, ably convinces of the great strides made by British and American Allies in applying tactical air power during the North African campaign, permitting the gathering of strategic intelligence and successfully directing power at key targets. His article, "Tactical Air Doctrine in North Africa, 1940–43," argues that much was learned about "the necessity of controlling tactical air power at an appropriate command level, one that had access to all available intelligence"[5] in order to employ air power and strike in a timely way to achieve a desired strategic effect. This turning point is the genesis of much of the body of our modern air power doctrine, including the widely accepted first tenet of air power: centralized control and decentralized execution.

Parts 3 and 4 of the book focus on papers that present arguments on Vietnam, the 1991 Gulf War and the 1999 air war over the former Yugoslavia as key turning points. This part of the book will be instantly more familiar to readers, as it covers conflicts that many have direct memory of or indeed participated in. John Andreas Olson writes in "The 1991 Bombing of Baghdad: Air Power Theory vs Iraqi Realities" that the strategic bombing campaign alone accomplished pivotal success by inducing "strategic paralysis" in the Iraq national leadership, ultimately leading to defeat. Dr. Sebastian Richie of the Royal Air Force's Air Historical Branch takes the book to its conclusion with a detailed study of the final turning point, the NATO air campaign known as Operation ALLIED FORCE, with his paper "Air Power Victorious? Britain and NATO Strategy during the Kosovo Conflict." He provides convincing analysis that this war was a pattern for future conflicts where air power is relied upon (perhaps too often) to be instrumental in coercing a peace and answers a number of key questions such as: why did NATO favour an air campaign over a land campaign, what were the goals of the campaign, what problems were experienced and how these problems were overcome?

Ultimately, the reader will have to decide if the arguments and analysis put forth in this book are convincing or indeed warrant the vaunted hallmark of turning points in the relatively short century of air power history. There can be no denying that the reader will gain much insight into and appreciation of the overall effect of air power in war when seen from the perspective of lessons learned and how they became the doctrinal foundations of modern air power's utility.

Lieutenant-Colonel Pux Barnes is an Aerospace Control officer in the Royal Canadian Air Force who flew as a mission crew commander on the airborne warning and control system (AWACS) aircraft during tours with NATO and the United States Air Force. He participated in numerous operations, including NATO Stabilization Force (1997–1999), Operational ALLIED FORCE (1999), NATO Kosovo Force (1999–2001), Operation NOBLE EAGLE (2005–2009), Operation ENDURING FREEDOM (2007–2008) and Operation IRAQI FREEDOM (2008). He is currently the Air Warfare Education Branch Head at CFAWC.

Abbreviations

CFAWC	Canadian Forces Aerospace Warfare Centre
NATO	North Atlantic Treaty Organization

Notes

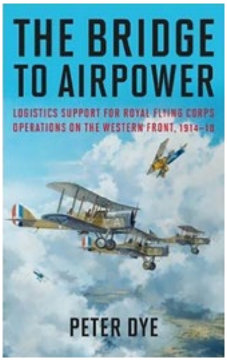
1. Sebastian Cox and Peter Gray, "Editor's Preface," in *Air Power History: Turning Points from Kitty Hawk to Kosovo*, ed. Sebastian Cox and Peter Gray (Portland, OR: Frank Cass, 2005), vii.

2. Ibid.

3. Tami Biddle, "Learning in Real Time: The Development and Implementation of Air Power in the First World War," in Cox and Gray, *Air Power History*, 3.

4. James S. Corum, "The *Luftwaffe* and Lessons learned in the Spanish Civil War," in Cox and Gray, *Air Power History*, 86.

5. Brad Gladman, "The Development of Tactical Air Doctrine in North Africa, 1940–43," in Cox and Gray, *Air Power History*, 203.



THE BRIDGE TO AIRPOWER: LOGISTICS SUPPORT FOR ROYAL FLYING CORPS OPERATIONS ON THE WESTERN FRONT, 1914–1918

By Peter Dye

Annapolis, MD: Naval Institute Press, 2015
270 pages
ISBN 978-1-61251-839-8

Review by **Major William March, CD, MA**

Fascinating! This is not a word that I would normally use to describe a book on logistics, yet it opened my eyes to a subject that I have long known is important with respect to aerospace operations but had rarely studied. Author Peter Dye, a retired Royal Air Force Air Vice-Marshal with 35 years' experience in air-force logistics, has crafted a masterful examination of this area of military endeavour as it evolved in support of the Royal Flying Corps (RFC) during the First World War. Fundamentally, this is a story about the birth of aerospace logistics where past practices were adapted, and new processes invented, to support the first technologically driven air war.

In the introductory chapter, the author makes a strong case that aviation logistics is a neglected area of aerospace study. While acknowledging that it may not be the most exciting of subjects, Dye points out just how dependent the RFC was, and modern air forces are, on a logistical tail. By the end of the First World War, of approximately 50,000 RFC personnel in France, only 8 per cent were classed as combatants (pilots, observers, gunners, etc.) while a stunning 29,000 were deemed to be "technicians." This large "tail-to-tooth" imbalance is indicative of an organization in a constant state of growth and technological flux while experiencing an average monthly "wastage" rate (i.e., aircraft losses to all causes) of 50 per cent of its front-line strength.[1]

Throughout Chapter One, the author establishes the importance of the RFC with respect to ground combat on the Western Front. Although fighter and bomber operations were important, the major contribution to Allied victory was made by the "corps" machines spotting for the artillery and providing photographs and timely information to army commanders.

Logistic support for the RFC, described in Chapter Two, was provided by a series of large, fixed aircraft depots located well behind the lines, while smaller air parks were established at railheads at the rear of a supported army. The air parks were mobile and capable of moving with their supported land formation. Knitting everything together were air ammunition columns, which moved ordnance, equipment and consumables to the squadrons as required. Finally, there were maintainers—the riggers and fitters—servicing squadron aircraft at the airfield. Engines requiring longer than 36 hours to repair, and all recovered aircraft wrecks, were sent to the depots for repair or cannibalization. Engines, aircraft and spares proceeding to front-line squadrons were sent to the air parks for distribution.

One individual headed this massive organization for most of the war, Robert Brooke-Popham. Under his watch, the RFC established a logistic support mechanism second to none. As the size and scope of logistic responsibilities grew, Brooke-Popham supported the establishment of equipment officers (EOs), whose broad duties included transport, armament, photography, wireless and maintenance. The EOs were supported by a small army of clerks, vital cogs in a system that by the end of the war in November 1918 provided a detailed inventory of more than 3500 aircraft and 5500 engines.[2]

The production and acquisition of aero engines is dealt with in Chapter Three. Although this chapter may be glossed over by many readers, it is worth closer examination, as the author discusses how a strong aviation industry, or lack thereof, has a direct impact on air power at the front.

Chapters Four and Five offer case studies that examine the role that RFC logistics, as described in the previous chapters, played in battles of the Somme (1916), Arras (1917) and Third Ypres (otherwise known as Passchendaele, 1917). Of special interest to Canadians would be Arras, which included the assault on Vimy Ridge. Dye examines each battle, highlighting the highs, and lows, associated with logistics support for the RFC. Of note is the symbiotic relationship between aircraft production, salvage and maintenance in trying to keep pace with unanticipated losses due to enemy action, misadventure and weather. Sometimes the smallest improvement could have a major impact on operations. For example, Dye points out that changes to maintenance procedures at the squadron level (better techniques and supply) meant that monthly flying hours per maintainer rose from 1.0 to 1.2 between April and November 1917. Overall this generated approximately 4000 more flight hours per month across the RFC on the Western Front or the equivalent of five additional squadrons.[3]

Chapter Six is reserved for the last year of the war, commencing with the March 1918 German offensive and culminating with the 100 Days prior to the Armistice. Dye highlights the flexibility of the RFC's logistics system as it dealt with supporting an initial Allied retreat in the face of a determined German offensive only to be thrust into a period of rapid advancement as the Allied armies pushed the enemy back. The mobility of the air parks and air ammunition columns permitted RFC support to adapt to the operational situation. During periods where it looked as if enemy action might disrupt the supply chain, the organization shifted from a "pull" process—where a squadron requested supplies—to a "push" procedure—whereby the air parks sent several days' worth of spares and consumables to squadrons, ensuring continuity of the air-power effort.

In his concluding chapter, the author reiterates the need to examine aviation logistics and underscores that the successes enjoyed by the RFC in the field were due in no small part to its logistic organization. Although RFC practices with respect to supply and maintenance were not perfect, they were robust and adaptive enough to meet the needs of a constantly evolving air force engaged in a life or death struggle with a formidable enemy.

One minor criticism is that I would like to have seen a bit more information about recruiting and training the individuals who made the system work. I get the sense that the evolution of the human dimension of *The Bridge to Airpower* would be every bit as interesting a story as that of the logistics organization itself.

Overall, it is a well-researched and -written book that takes a complex subject and makes it accessible to readers who know very little about logistics … other than it is important. Those with an in-depth knowledge of supply-chain management, et cetera, will enjoy it for its historical perspective. I highly recommend it to members of the Royal Canadian Air Force (RCAF) as a welcome addition to their airpower studies.

Major Bill March, a maritime air combat systems officer, has spent over 39 years in uniform. He is currently a member of the Air Reserve, serving as the RCAF Historian within the Directorate of RCAF History and Heritage.

Abbreviations

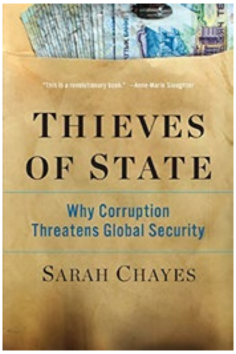
EO	equipment officer
RCAF	Royal Canadian Air Force
RFC	Royal Flying Corps

Notes

1. Peter Dye, *The Bridge to Airpower: Logistics Support for Royal Flying Corps Operations on the Western Front, 1914–1918* (Annapolis, MD: Naval Institute Press, 2015), 8–9.

2. Ibid., 46.

3. Ibid., 106.



THIEVES OF STATE: WHY CORRUPTION THREATENS GLOBAL SECURITY

By Sarah Chayes

New York: W. W. Norton & Company, 2015
262 pages
ISBN 978-0-393-23946-1

Review by **Major Chris Buckham, CD, MA**

Media and government attention, traditionally and more notably during the last 15 years, has been focused upon the economics and operational tactics of identified terrorist groups and their supporters. A phenomenal amount of military and economic resources has been brought to bear in an effort to crush these organizations. Notably missing from the dialogue, however, has been discussion of those governments whose actions have instigated, enabled and facilitated these activities. Nor does it appear that there is a clear understanding of the direct link between the corrupt practices of national leadership and an appreciation of its impact upon the ability of fringe organizations to advance their causes. Sarah Chayes's book sheds a blinding light upon the clear connection between these activities, their impact and Western governments' reluctance to acknowledge them.

Starting with a discussion of the writings of Locke, Milton, Nizam al-Mulk, Luther and Machiavelli (to name but a few), she looks at the repeated acknowledgement of the responsibility of leaders to their people: the so-called mirror-for-princes treatises. These texts emphasize the critical necessity of leadership to be accountable to the people whom they lead (and the potential impacts if the text is not followed). *Thieves of State* is not, however, a dry political analysis; Chayes draws upon her 10 years of work in Afghanistan as a reporter, an entrepreneur and a foreign-policy advisor to the United States (US) military in order to draft an accessible and eminently readable discussion of the endemic corruption of the Karzai government and the response of the US political and military establishments.

Her approach is not jaundiced but balanced and telling; Chayes effectively examines the impact that pervasive corruption has upon the ability of fringe elements to recruit and operate. The author has broken out her analysis into distinctive methods or techniques of corruption, each having in common a bottom-up flow of monies. She identifies those practising systemic corruption as Kleptocracies, further breaking them down into subcategories such as: Resource, Post-Soviet, Bureaucratic, Military-Kleptocratic Complex and Vertically Integrated Criminal Syndicates. Each type is explained in detail with examples and facts.

Additionally, Chayes discusses how populations, denied access to legitimate forms of redress due to corrupt officials and entities, are left with no option but revolt as a means of addressing their grievances. For example, Boko Haram—initially a fringe, self-sustaining community—was driven into armed rebellion by the unethical practices of the Nigerian police and bureaucracy. Their name, which means roughly Western Education is Forbidden, was derived from the fact that Nigerians know their civil service to be absolutely corrupt and also that to get a job within said civil service one has to have a Western-style university degree. Thus, irrespective of the logic of their belief, they have equated the corruption with not only the system of government but also the education needed to work within that system. It is critical to the determination of effective responses to these groups that the root causes of their formation be acknowledged and addressed as part of the solution.

Recognizing this, Chayes provides a series of practical actions that governments may take in order to influence the behaviours of corrupt regimes. These multifaceted approaches run the gamut from aid and financially based approaches to diplomatic- and business-focused tactics. Unavoidable within these methodologies is the necessity to work in tandem with other nations to ensure a common front.

While corruption is not the only element facilitating violence, it may certainly be grasped as a medium within which violent reaction among the people takes hold and flourishes. Chayes clearly illustrates that fighting fringe elements such as Al-Shabbab and Boko Haram is necessary; however, it is equally critical to recognize these organizations as indicative of a much deeper malaise: corruption. To treat the symptoms without acknowledging the actual disease will never break the cycle. This book is vital to appreciating the scope and nature of corruption, the potential impact of not addressing it and also methodologies that may be exercised to counter it.

Major Chris Buckham is an air logistics officer presently posted to the International Peace Support Training Centre in Nairobi, Kenya. He maintains a professional reading blog at www.themilitaryreviewer.blogspot.com.

POINTS OF INTEREST

UNBLINKING AND UNHERALDED: CANADA’S ISR CONTRIBUTION TO OPERATION IMPACT

BY LIEUTENANT-COLONEL BRENDAN COOK, MSM, CD

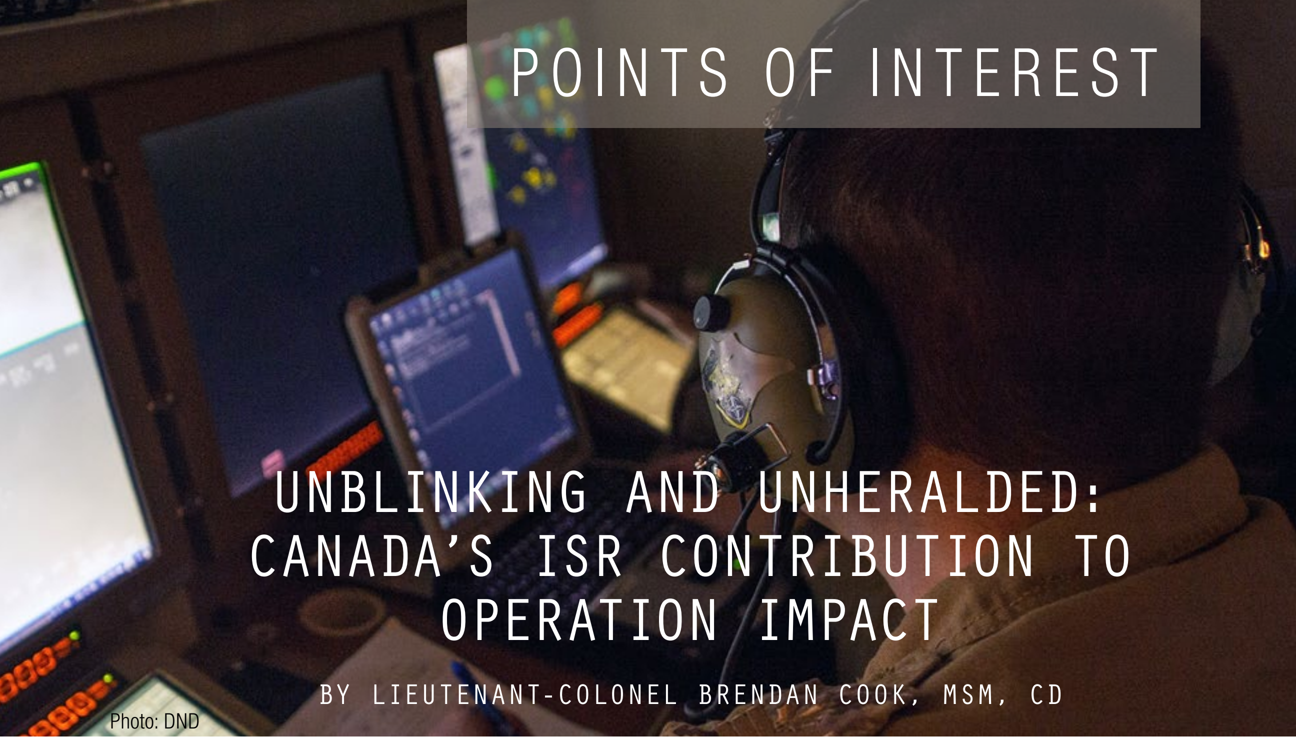


Photo: DND

A Royal Canadian Air Force member controls the radars of a CP140 Aurora during Operation IMPACT

As the Canadian contribution to the coalition fight against the Islamic State of Iraq and the Levant (ISIL) approaches its 18th month and the Canadian government embarks on a modified military mission focused on training and assisting Iraqi forces, one aspect of the mission has remained persistent, enduring and unblinking. The dedicated airmen and airwomen on the venerable CP140M continue to be a key part of the coalition’s intelligence, surveillance and reconnaissance (ISR) framework, providing the ever-watchful eye over the battlefield. More commonly known in the mainstream media as simply “spy planes,” this aspect of Canada’s contribution has been less heralded and is likely the least understood by most Canadians, yet the CP140M is a world-leading ISR capability that is much in demand by our coalition partners and of which all Canadians should be justifiably proud. It is this contribution that provides a critical link in the targeting chain, enabling successful combat operations daily. Moreover, the lessons being learned through the employment of the CP140Ms are now driving the evolution of ISR data management and operations in the Canadian Armed Forces.

The Canadian long-range patrol (LRP) contribution to Operation (Op) IMPACT consists of one LRP detachment of two modernized Block 3 CP140 Auroras (also known as CP140M) as well as approximately 75 aircrew, maintainers and support staff. It is a relatively modest tactical investment that provides huge returns for Canada and the coalition. The LRP detachment has flown over 400 combat missions, accumulated more than 3500 combat hours and executed its mission with a 96 per cent mission-success rate. Each mission has gathered valuable intelligence in support of coalition operations in the air and on the ground.

The CP140M is a fully integrated, multisensor, multimission long-endurance asset. The primary sensor used in over-land operations is the electro-optical infrared camera system, which provides both day and night capabilities. While it is also fitted with a highly advanced acoustic system for traditional antisubmarine operations and an electronic support measures (ESM) system for detecting a wide range of electronic emissions, it is the Block 3 imaging radar system (IRS) that is becoming more and more important in supporting intelligence gathering. The IRS is capable of all-weather imaging of targets, both in over-land and maritime environments, at extremely high resolution and from great distances. As a result, even on cloud-covered days, the CP140M can continue to gather intelligence over Iraq.

The radar imagery gained, while still versus live action, provides additional capabilities that standard optical systems cannot provide. For instance, the highly precise and geo-rectified images provide the ability to take detailed measurements of objects. Moreover, a comparison of the characteristics observed in the optical and radar images can provide further insights on the objects' make-up and composition. Lastly, the IRS provides the capability to generate large swaths of images known as strip maps, which enable the rapid gathering of data over a wide area for the purposes of detecting change through comparative analysis.

With these powerful sensors and its long endurance, the CP140M is routinely tasked with wide-ranging mission sets within a single sortie over Iraq. It is not uncommon for the CP140M to start a mission observing known ISIL positions in one part of Iraq only to be retasked to support dynamic targeting or troops in contact elsewhere. In this manner, the CP140M consistently demonstrates the Royal Canadian Air Force's central tents of: Agile, Integrated, Reach and Power – AIRPower.

The success of ISR operations is predicated on disciplined and well-oiled data management and analysis, in the air and on the ground. While airborne, aircrews correlate newly acquired data with pre-mission intelligence, other onboard sensors and neighbouring platforms via datalinks and secure instant-chat systems. Through this process, they triage the raw feeds, generate actionable intelligence and report it to support real-time, tactical operations or to mark and record data for more post-mission analysis. Moreover, through the use of a tactical common datalink (TCDL) and the interim beyond line of sight (iBLOS) system, aircrews are able to share real-time video with supported units on the ground or anywhere in the world via satellite links. In short, the CP140M is now more fully integrated into the coalition and Canadian ISR architecture than at any previous point in its history.

Post-mission, the ISR challenge continues in the Deployable Mission Support Centre (DMSC), a fully integrated part of the weapon system that processes, exploits and disseminates data so that the entire ISR enterprise can benefit from each and every mission to the fullest. With so much data generated by the new CP140M's capabilities, the Canadian ISR architecture has had to rapidly mature and evolve to ensure the maximum benefit is gained from existing investments. Automated data sharing and processing coupled with new expertise in analysis systems are now extending the realm of the possible.

It is both an exciting and rapidly evolving time for the Canadian LRP force. When looking at the CP140M's contributions to recent operations, those to Op IMPACT have lasted longer than Op MOBILE's and will soon be longer than Op APOLLO's. This will make Op IMPACT the longest-standing deployed mission for the LRP force in the last 20 years, at a time when the CP140M is still only at its initial operating capability.

Sustaining an operation of this duration with an LRP force that has been reduced to one third its size over the intervening decade since Op APOLLO has posed a significant challenge for the backbone of the capability, the airmen and air women as well as their families. The outstanding results being achieved in Op IMPACT are due to the tenacity and innovation of the talented and dedicated members of the LRP force, many of whom have already deployed on multiple rotations. It is they who are achieving the operational successes and driving the innovation. The foundation they are laying will ensure that the LRP force will continue to be a go-to, strategic, deployable asset for the Royal Canadian Air Force and the Canadian Armed Forces, setting the conditions for success and excellence for years to come.

Lieutenant-Colonel Brendan Cook joined the Royal Canadian Air Force in 1991. Earning his navigator wings in 1996, he was subsequently posted to 407 Maritime Patrol Squadron in Comox, British Columbia, where he served as an acoustic sensor operator. He has had postings to the Acoustic Data Analysis Centre (Pacific) in Victoria, British Columbia, the Maritime Proving and Evaluation Unit in Greenwood, Nova Scotia, as well as staff tours in Toronto and Ottawa. He previously deployed to Afghanistan in 2009 to participate in developing and testing procedures for the Heron unmanned aircraft system. He assumed command of 405 Long Range Patrol Squadron in June 2014 and subsequently deployed as the Op IMPACT ROTO 0 Long-Range Patrol Detachment Commander from October 2014 to April 2015. On completion of his command tour at 405 Squadron in 2016, Lieutenant-Colonel Cook assumed the position of Director Air Requirements 3.

Abbreviations

IRS	imaging radar system
ISIL	Islamic State of Iraq and the Levant
ISR	intelligence, surveillance and reconnaissance
LRP	long-range patrol
Op	operation

Photo: DND

A Royal Canadian Air Force CP140 Aurora aircraft awaits its next mission in Kuwait during Operation IMPACT