July–August 2020 Volume 80, Number 4

FOUNDED 1890

RCMI

THE JOURNAL OF THE ROYAL CANADIAN MILITARY INSTITUTE

SITREP

SECOND PANDEMIC EDITION

Canada and Technological Warfare

Inside this Issue

Executive Summaries of Articles

Unpacking 'Wicked Problems' of Cyberspace: Conceptual Approaches for Novice Practitioners *by Ken Ingram*

Ken Ingram is interested in how language is used to describe the many facets of cyber, particularly in the context of military applications in the cyber domain writ large. He posits that cyber is best described as a 'wicked problem' which present "pressing and highly complex issues for policy formulation that involve many causal factors and high levels of disagreement about the nature of a problem and the best way to handle it." He describes the ways in which the CAF have attempted to address cyber threats, as well as how DND and other government departments have attempted to formulate cyber policy, while not adhering to strict doctrinal definitions which further clouds the issues. Ken then describes a series of what he terms "intersectional policies and competing priorities" in the CAF, such as recruiting cyber operators and navigating operational security challenges in the cyber domain. Further opportunities to misconceive the nature, frequency and harm from cyber-attacks are further complicated by how cyber hackers and other cyber actors are portrayed in popular media and cyber literature. He concludes by stressing the need for a well understood and commonly accepted cyber taxonomy in order to improve Canada's overall cyber capability going forward.

Automation, Autonomy, and Subsea Warfare: How the COVID-19 Pandemic Will Push Us to Accelerated Adoption, With Unintended Consequences *by Konrad Mech*

Konrad Mech's previous article for SITREP focused on dangers associated with the convergence of technologies that could enable state actors to deploy android soldiers in land-based armed conflict, including threats to military and humanitarian law. In this article, Mech transposes the same argument to the maritime domain, i.e. the potential to develop and deploy automated and autonomous maritime surface and sub-surface platforms. He provides an overview of developments in this field in Russia and China, as well as advances in technologies which increase the potential for states to deploy unmanned maritime weapons. This raises the potential for maritime conflicts between unmanned maritime systems, creating potentially devastating environmental threats due to destruction of nuclear-powered or armed vessels. COVID-19 has exacerbated all these developments in quite unexpected ways. The unplanned docking of the USS Theodore Roosevelt as a result of a mass outbreak of the virus, provided an opening for China to take advantage of the situation in the region. This raises the specter for nuclear, biological and chemical warfare to play out in the maritime domain. He concludes by stating that "I believe these imperatives will push the west to accelerate development and deployment of automated and autonomous systems to shore up identified weaknesses and vulnerabilities exposed by COVID-19. But there will be unintended consequences, because we don't know what the "unknown unknowns" are.

Canada: Droning On? *by Jeremy Wang*

Jeremy Wang wants to ensure that the CAF selects the right Remotely Piloted Aircraft (RPAs)—or drones—and for the right reasons. While Canada has built drones for other countries, we have not done so for ourselves. With allies and potential adversaries pushing ahead with aggressive drone acquisition programs, and acknowledging that drones are now considered an essential capability in modern conflicts, he lays out a logical approach to how Canada can effectively acquire drone technology. The approach he advocates is built around three inter-related phases. First, the CAF must determine if drone technology is a suitable solution to meet specifically identified capability gaps (in ISR, for example). Second, the acquisition process must ensure that potentially identified suppliers of drone technology understand in detail what problem or gap the drone technology must be able to solve. Third, the proposed solution must be tested in the most rigorous manner. Wang's solution is to identify users in the CAF who have the skills and knowledge to utilize tactical-level technology most effectively: the answer being special operations forces. He states "by leveraging the intensity and speed of CANSOFCOM's procurement cycle, each stakeholder achieves their own goals. CANSOFCOM gains new tools that enhance their capabilities, the supplier's product earns the 'spec ops' stamp of approval, and the broader CAF can leverage the early success to inform and ease their own purchases."

Machine Intelligence in Targeting: Opportunities and Risks *by Liam Robertson*

Liam Robertson believes that Machine Intelligence or 'MI' (popularly known as Artificial Intelligence) is emerging as one of the most disruptive technologies which has the potential to upset the global balance of power: he cites Putin who stated that "Whoever becomes the leader in this sphere will become the ruler of the world." The CAF is in the midst of trying to understand how MI can be leveraged to support military operations, including opportunities and challenges. The focus of his article is the potential to utilize MI to enhance the CAF's joint targeting capabilities including target development, improving situational awareness, and enhancing capability and options analysis. He argues that "Canada must invest in organizations, directed research and designate trial formations to gain understanding of how the integration of MI into military forces will affect future operations." He argues that while the CAF does not possess the scale to allow it to develop leading-edge technologies, "we are small and agile enough to rapidly operationalize functional concepts in order to seize relevance in key areas." One way to ensure that the CAF can remain relevant in this emerging domain is to institutionalize "the establishment of a multidisciplinary cadre of capable CAF and DRDC members possessing MI/MLA skills and capabilities." He concludes by asserting that "The sine qua non of victory will be the possession of capable Machine Intelligence. In the near term, investment in such capabilities by our rivals will only increase."

The production of SITREP is made possible in part by the generosity of the Langley Bequest, which is made in honour of Major Arthur J Langley CD and Lt (N/S) Edith F Groundwater Langley

From the Editor

While at time of writing the RCMI remains shuttered, the Province recently announced that Toronto can enter Stage 3 of the provincial re-opening, and this will allow RCMI staff to begin activating the extremely detailed plans that have been developed. It is highly likely, according to President Michael Hoare, that the ability to re-open the RCMI will require several weeks of preparation and, thus, a probable timeframe will see us in the Long Bar sometime in September. Whatever the 'new normal' conditions for service may entail, I am positive that Members and guests alike will undoubtedly celebrate this occasion.

In the meantime, the pace of new defence and security-related information and educational opportunities have proliferated online to the point that I can participate in so-called webinars, presentations and zoom meetings on an almost a daily basis should I so choose (which I do not…). That said, to give you an idea of which organizations and what sorts of topics are being discussed, the following list is illustrative.

The Conference of Defence Associations (CDAI), of which the RCMI is a long-time member, offered webinars on the security issues surrounding 5G and the Huawei controversy, as well as Quantum Supremacy and Its Many States of National Insecurity. One of our own, Dr. Howard Coombs, is producing an online weekly newsletter for the CDAI entitled *CDA Institute Aerogram* which incorporates a wealth of information gleaned from a wide variety of sources and organizations.

The Brute Krulak Center for Innovation and Creativity, a sub-set of the Marine Corps University, produced online presentations addressing Iran's Maritime Strategies and Tactics, and the New Firing Table (a detailed overview of how offensive and defensive cyber operations actually work). An upcoming presentation will discuss gender inclusion versus integration in the military.

The John Hopkins University of Medicine (which maintains the COVID-19 global scoreboard, which is now all but required consultation on a quotidian basis) provides extensive access to pandemic-related articles, data and events which are constantly updated. An extremely interesting expert discussion entitled Crisis, Security and COVID-19 can be found *here* .

Lastly, I would be remiss if I did not mention the incredible wealth of information that may be accessed once a person signs up for the weekly World Economic Forum's *Strategic Intelligence* service. Some of the recent offerings from the service included The Digital Transformation of Business; the Great Re-Set; Precision Medicine; Blockchain and, of course, COVID-19. Why men-

Royal Canadian Military Institute
Founded 1890

Viceregal Patrons

Her Excellency the Right Honourable Julie Payette
Governor General of Canada

The Honourable Elizabeth Dowdeswell, OC, OOnt
Lieutenant Governor of Ontario

Vice Patrons

General Jonathan Vance, CMM, MSC, CD
Chief of Defence Staff

His Worship John Tory
Mayor of Toronto

Officers & Directors

LCdr/Dr. Michael J. Hoare, CD (Ret'd)—President and Executive Director
Capt Rodney W. J. Seyffert, CD (Ret'd)—Vice President
LCol Michael J. K. Clarry, CD (Ret'd)—Vice President
Mr. Robert C. Kay, JD—Director
Mrs. Julie A. Lindhout, MA—Director
Mr. James H. Lutz, MA—Director / Secretary
Ms Michele Walkau, MEd—Director
Mr. Jay M. Yakabowich—Director

Past President

HCol Gilbert W. Taylor

Honoraries

HLGen Richard Rohmer, OC, CMM, DFC, O.Ont, KStJ, CD, OL, Legion d'Honneur, QC
Honorary Vice President

Dr. J. L. Granatstein, OC, FRSC
Honorary Historian

Mr. Arthur Manvell
Honorary Librarian

LCol J. Roy Weir, CD, ADC, QC (Ret'd)
Honorary Solicitor

Ms Gertrude Steiger Kearns, CM
Honorary War Artist

Maj Gillian Federico, CD (Ret'd)
LCdr The Rev J. David Mulholland (Ret'd)
HLCol The Rev Mark L. Sargent, CD
Honorary Chaplains

General Manager

Mr. Garett Wright

Controller

Ms. Elena Trouba

Director, Defence and Security Studies Programme, Editor, Sitrep

Maj/Dr Daniel D. Eustace, CD (Ret'd)

An Official Publication of the Royal Canadian Military Institute

426 University Avenue,
Toronto, Ontario, M5G 1S9
Tel: 416-597-0286/1-800-585-1072 Fax: 416-597-6919

Website: *www.rcmi.org*

Editorial E-Mail: *daneustace1@gmail.com*

tion this in the context of a defence and security publication? For the simple reason that there is no complex topic or issue on the global table that does not impact on some aspect of national security.

This brings us to the current edition of SITREP. Once again, we have provided Executive Summaries for your initial "speed-read" of the publication which, no doubt will be followed by a more leisurely and in-depth review of the enclosed material. While the potential to offer any number of focus areas was possible (particularly given the aforementioned overview), many of the challenges faced by the Canadian Armed Forces (CAF) are centred on technological developments and issues. Each of the four articles in this edition address some aspect of military technology that deserve further analysis and elucidation. These include the CAF acquisition of unmanned aerial vehicles (UAVs or drones); the growing threats posed by the deployment of automated and autonomous maritime surface and sub-surface platforms; the opportunities and risks generated via the introduction of Machine Intelligence into CAF operations, and the confusion and lack of precision in CAF cyber operations due to a superficial level of understanding of cyber terminology. While these subjects in no way encompass the full range of technological challenges faced by the CAF, they all do illustrate the incredibly complex environment in which the CAF is operating now, and will in the future.

As a final point, one of the more interesting threads that I have discerned via my participation in several of the webinars, presentations and discussions previously mentioned, is the unexpected ways that the pandemic is generating new challenges, risks and opportunities, many of which reside in the technological realm. To the extent that a technology may be developed or selected as an alternative to a human-based solution or approach (which may be unavailable or considered too risky in a pandemic environment), this may become the default solution in areas never previously considered or imagined. If Moore's Law (which posits that the number of transistors double on a chip every two years) holds true going forward, then the growth potential for technologies such as 5G, artificial intelligence, quantum computing and autonomous machines to drastically alter the defence and security environment is very real. Given Canada's debt and deficit levels as a result of its pandemic economic response, does the CAF have any real hope of achieving parity or maintaining pace in this new, and very dangerous, competition for global technological supremacy?

Maj Daniel D. Eustace, CD, PhD (Ret'd)
Director, Defence and Security Studies Programme

Unpacking 'Wicked Problems' of Cyberspace: Conceptual Approaches for Novice Practitioners

by Ken Ingram

Introduction

Regardless of training or vocation, every cybersecurity professional faces the difficulty of first conceptualizing cyberspace and subsequently articulating it to others. A dearth of discourse within DND/CAF specifically examines this phenomenon and it's a dilemma because the language we use matters—especially in policy, yet extendable to advisors, diplomats, and the decisions made not only by senior leaders, but also everyday computer users.

Borrowed metaphors such as 'viruses' and 'infections' are often employed when describing cyber-related threats. Others, such as 'trojans', draw from particular histories of warfare. We are routinely warned about future dangers by references to the past. Culturally specific conflicts such as 'cyber Pearl Harbor', 'cyber 9/11', or 'cyber Armageddon' saturate much of the contemporary literature. Perhaps most menacing, however, is the use of 'cyber' as a subject, adverb, adjective, and noun; paradoxically communicating everything and nothing. Additional terms, such as 'cyber attack' and 'hack', colloquially define any unwelcomed incident affecting a computer, peripheral device, or data. These examples have become normative in everyday language and require astute attention.

This paper examines some of the most common language, imagery, and other non-technical factors associated with cyberspace—including intersectional policies and competing priorities. These factors are critical aspects of cybersecurity yet they are often ignored, eclipsed, or rendered invisible by other facets of the warfighting domain. This approach reveals underlying problems. If unaddressed, they will continue to impede progress towards addressing 'wicked problems' of cyberspace.

Wicked Problems Of Cyberspace

'Wicked problems' are an important concept in public policy and are highly relevant to cyberspace—particularly from the perspective of national security. Since the term emerged in the late 1960s (its origin is discussed in detail elsewhere), 'wicked problems' present "pressing and highly complex issues for policy formulation that involve many causal factors and high levels of disagreement about the nature of a problem and the best way to handle it." As Bateman (2011) notes, the term 'wicked' is not to imply something is evil. Rather, it describes "a problem that is highly resistant to resolution." Other examples of 'wicked problems' include the nature of poverty, maritime security, health inequalities, and (I contend) politics of the English language. These problems, whether analogous or highly relevant to cyberspace, entangle fundamental differences between stakeholders whereby effective solutions require changes to both mindset and behaviour. Most recently, efforts are underway to eliminate the word 'cyber' as jargon and replace 'cybersecurity' with the term 'digital security'.

Pressing, Highly Complex Issues

There is no shortage of major media headlines, alerts, and other sources of disclosure to demonstrate overwhelming evidence that our data and computer networks are vulnerable. Cyber-espionage was cited as a means for "the greatest transfer of wealth in history" nearly a decade ago and remains rampant. Other malicious activities—with disproportionate severity—apparently seek to degrade, deny, disrupt, or destroy critical infrastructure or influence democratic elections. A sense of urgency is palpable from news cycles, senior officials, cybersecurity professionals, advocacy groups, and alleged victims.

Ken Ingram *is a Section Head within Canadian Forces Intelligence Command (CFINTCOM) who possesses roughly a decade of specialization in computer network intelligence. A recent M.A. graduate of Columbia University in NYC, he is also a Lieutenant-Commander in the Naval Reserve and serves part-time as Executive Officer of HMCS Carleton.*

This paper was written by a student attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. It has been published here for the first time with the kind permission of CFC and DND. The citations and bibliography which are contained in the original paper have been removed for ease of publishing; interested readers may obtain an original copy of the paper from the Editor.

The views expressed are those of the author and do not necessarily reflect the views of the Institute or its members.

Underlying political, administrative, and policy elements are almost certainly present although they progress at a comparatively glacial pace (and are thus far less appealing to most audiences) compared to the more sensational aspects of cyber-related threats. Many of the complex issues we face concerning cyberspace are in fact, not new. Previous candidates of the Canadian Forces College (CFC) Joint Command and Staff Programme (JCSP) have examined more than a dozen cyber-related topics. Each paper illuminate a dimension of cyberspace from a particular DND/CAF lens, offering valuable insight regarding deterrence, procurement, decentralized military functions, capability gaps, broad capability development proposals, environment-specific requirements such as within the Royal Canadian Navy, integration of the Primary Reserve within force generation and force employment models, joint offensive cyber operations with the CAF and Canada's national cryptologic agency, and a need for clear strategic direction including a blueprint for hiring talent, amongst others. These papers, including the most recent ones, also demonstrate that Canadian defence policy continues to adjust as some cited entities no longer exist and terminology remain in flux.

While beyond the scope of this paper, other 'wicked problems' presented by cyberspace that warrant further consideration include the widespread inadequacy of contemporary computer literacy skills; insider threats and also 'unintentional insiders'—those who elevate risk due to their own cognitive bias, routines, and behaviour that prioritizes trust and convenience rather than best practices and common sense. Research demonstrates that scaring people about cyber-related threats doesn't improve cybersecurity and often has the opposite intended effect. Shifting away from predominantly human factors, disruptions to defence-related logistics support and tainted supply chains, including fake parts or 'digital backdoors', pose risks to mission assurance, force projection, and force sustainment. At this very moment, cyber-espionage activity is probably harvesting proprietary information from cleared defence contractors who are preparing sophisticated multibillion-dollar platforms of the future (in essence, 'systems of systems'). A technological 'arms race' also exists between nations as they compete for raw materials, semiconductors, telecommunications equipment and bulk data.

By no means are these examples mutually exclusive. When considering the enormity of the problem, surmised by Major-General Loos as a domain "increasingly more complex, congested and contested", we must also acknowledge the speed of technological advancements—their inclusion within our homes and workplaces whether afloat, on land or in the air—far outpacing policy formulation and implementation.

At first glance, these complex problems appear to align with the type of 'wicked problems' defined by Roberts (2000) whereby "stakeholders agree on the nature of the problem, but not on the solutions". Looking to a global perspective, however, further conflates the nature, urgency, and complexity of these issues. There are profound opposing perspectives about what cyberspace is and what it represents. Russia and China do not use the word 'cyber' and opt for terms such as 'informationalization' and 'digital confrontation'. These differences are not merely linguistic. They present profound ideological disparities whereby 'access to the internet and free expression' (primarily Western constructs) clashes with deeply held convictions that cast information as a threat to be highly regulated, censored, and controlled. Questions about intellectual property, state sovereignty, privacy and human rights are also part of the discourse.

Ongoing Limitations of Policy Formulation

The *Canada First Defence Strategy* (2008) was a milestone for introducing the word 'cyber' into the lexicon of Canadian defence papers although it appears only once in the document. It's lengthier 2017 successor, *Strong, Secure, Engaged* (*SSE*), mentions 'cyber' a total of 87 times using 24 different variations—all of which are undefined. The variation is noteworthy because each term conceivably conveys a different meaning and interpretation within DND/CAF, Government of Canada (GoC), and abroad including allies and potential adversaries. While the prevalence of cyber-related words in the 113-page document

is unprecedented for a Canadian defence paper, *SSE* articulates very little meaning for the public or the majority of the Defence Team when it comes to cyberspace.

Graphic illustration for cyber-related words, terms, and concepts in SSE.
Size of font is relative to the number of times a term appears (displayed as a number).
Those without a number appear in the document only once.

Canada's first national Cyber Security Strategy (also known as a first-generation policy) took a few years to formulate before it was release in 2010 by Public Safety Canada. The document defines cyberspace as:

> **Cyberspace** is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship.

It briefly describes a three-pillar stratgy without addressing the specifics of *how* progress will be made, *who* is responsible, or *what* the mandates are. It may be concluded that the document's main premise, like other first-generation policies by other like-minded countries at the time, was to characterize 'cyber' as something new and something different (a characterization since contested or abandoned). It also established the sentiment that government should be organized to face cyber-related threats and prioritized federal funding.

In our current *National Cyber Security Strategy*, the definition for cyberspace was amended to note "more than 3 billion people" (*vice* 1.7b) in 2018. While not explicit, this change suggests that cyberspace is contingent on the number of people with access to it rather than the majority of the world's population who are excluded. The document also notes other cyber security action plans that will supplement the strategy and it will align with other GoC cyber-related initiatives, including "the Canadian military's use of cyber" (this is the only reference to DND/CAF in the entire document). Objectives are set, but not priorities.

The following alternative definition of cyberspace, proposed in 2016 at the Joint Terminology Panel, does not mention humans and characterizes it as "[t]he element of the operational environment that consists of interdependent networks of information technology structures—including the Internet, telecommunications networks, computer systems, embedded processors and controllers—as well as the software and data that reside within them."

While not intended to be an exhaustive examination of national or governmental policies, this brief examination aligns with the observation that "wicked problems lack agreement on both a definition and a solution"—even at the national level—yet "any fruitful attempt to tackle a wicked problem will of necessity be multisectoral".

Intersectional Policies and Competing Priorities

In early 2018, the Royal Canadian Navy announced it was lifting the 'draconian' policy of prohibiting Wi-Fi coverage in warships so that sailors could achieve a better work-life balance and communicate with their families back home. At around the same time yet unrelated, the U.S. military was unexpectedly forced to re-examine its security policies after the location of bases, routes, and perimeters were disclosed as part of a larger data set of approximately 13 trillion GPS points from users of a mobile personal fitness tracker. These examples offer a small glimpse of intersectional policies and competing priorities (i.e. fitness, morale, recruiting and retention) that the CAF must manage moving forward as technology—and expectations—change.

Cyber Operator, a relatively new military occupation in the CAF that was created in 2017, is specifically noted in *Strong, Secure Engaged* "to attract Canada's best and brightest talent and significantly increasing the number of military personnel dedicated to cyber functions." The Defence Women's Advisory Organization, created to encourage diversity in the CAF by addressing and overcoming barriers that women face, met in Ottawa during January 2019 when the Deputy Vice Chief of the Defence Staff, Major-General Frances Allen, discussed her previous experience as Director General Cyberspace and Joint Force Cyber Component Commander. The *Defence Story* notes "the rapidly growing cyber workforce has exciting opportunities for women with an interest in any aspect of the cyber field" with specific examples such as planning, policy, law, and human resources. Of the 99 Cyber Operator positions in total, 76 are presently filled although the vast majority of them (73) were drawn from in-service selection programs (personnel already in the CAF) while only three were Direct Entry (recruited from outside the military). The profile of "Canada's first female Cyber Operator" appeared in a Canadian military magazine as of November 2019 - and to its credit - noted she holds an arts degree whereby technical and creative skills allow her bring the whole picture together. She is presently one of only two Cyber Operators who identify as female. With the objective of increasing representation of women in the CAF towards the goal of 25 percent, progress within the Cyber Operator trade—albeit one microcosm amongst roughly 90 occupations —is not promising.

Visualizing 'Cyber'

When attempting to visualize cyberspace or cybersecurity, human factors are usually the first to be omitted. While more technical aspects such as hardware, software, and packets of information are inherent to the field, humans remain the primary actors and stakeholders as they are inevitably behind most keyboards and interfaces despite varying levels of automation.

Yet media, private vendors, and television shows continue to portray 'hackers' wearing hoodies, masks, or black balaclavas. These depictions perpetuate a particular fantasy that is deeply engrained within lay culture when in reality, these accessories are unnecessary (if not uncomfortable, unless made of merino wool perhaps). Images may also miscommunicate using gendered, xenophobic, or erroneous attribution (i.e. not all 'hackers' are malicious—some are 'ethical hackers'). While official government documents may not use these images, their prevalence elsewhere undoubtedly influences readers' perceptions when en-

countering words like "hacker' (present in official material) and absence of plausible alternatives.

Examples of 'hackers' drawn from news and stock photography webpages.

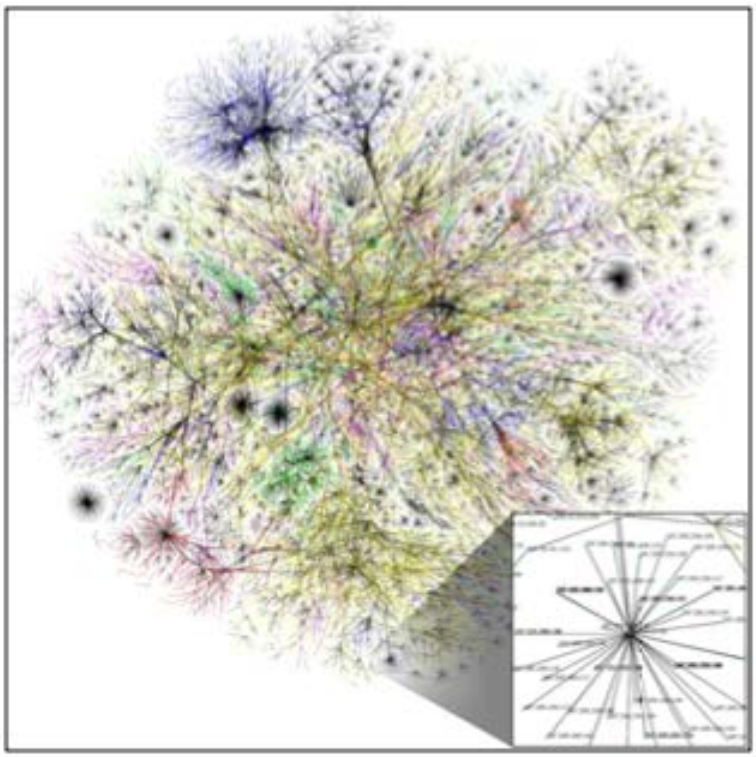
Technical vs Human Factors

In 2003, the Opte Project sought to create a static visualization for a portion of the internet—including routes and nodes—using multiple sources and tools. Human factors, however, are often excluded from these depictions.

Limitations of 'Cyber' Threat Maps

Private companies such as FireEye, Kaspersky, and Norse (among others) offer threat maps to visualize activity in cyberspace. While each of these services vary, they typically have a similar aesthetic: an overlay of bright colours representing transnational activity against a dark digital backdrop of Earth.

Cyberspace is often conceptualized as 'borderless' yet divisions at the political, corporate, private, and individual-level exist in the form of national firewalls, state-funded censorship, or other forms of circuits and switches. Threat maps offer little value because they are devoid of context. Some offensive cyber operations, for example, leverage Command and Control (C2) infrastructure that forms a network of interconnected yet geographically dispersed endpoints. Such operations rely on multiple stages yet threat maps depict unidirectional activity that also conveys no information about the intent of the offensive cyber activity, significance of the compromise (if any), or meaningful measures (whether success or failure).



An illustrated portion of the internet (left) compared to use of mobile devices at home (top right) and workplace. Sources (respectively): The Opte Project, Engadget, Carlo Allegri *(Reuters).*

Norse Live Attack Map. Source: *Newsweek*.

Why Most Activity is Not an 'Attack'

Likely one of the strongest words in the English language, 'attack' often accompanies the word cyber; however, the majority of cyber-related incidents (including cyber-espionage and precursors such as reconnaissance, scanning, probing) are not considered attacks. Much progress remains to be seen for establishing 'norms' about the way states behave in cyberspace and how older laws, conventions, and norms such as the Law of Armed Conflict (LOAC) apply.

A website re-direct that impacted a CAF recruiting website (forces.ca) in 2016 offers a useful example. Visitors were automatically forwarded to a Chinese state-run website, according to media reporting that claimed the recruiting website was 'hacked'. An initial examination revealed that the recruiting website was hosted externally by a service provider in the public sector. The Public Safety Minister, acknowledging the event as "a serious matter", also noted the importance of not jumping to conclusions.

Nomenclature and Taxonomy

Playful, yet often unfamiliar, words characterize threats in cyberspace such as phishing, malware (malicious software), ransomware, zero-days, Stuxnet, NotPetya, and WannaCry. Naming conventions for malware exist and classify it according to families and potential threats. Not too long ago, Public Safety in Ottawa maintained a giant database for malware analysis aptly named BeAVER (BEhavioural Analysis using Virtualization and Experimental Research). The imagination inevitably conjures images of the Containment Unit in *Ghostbusters* yet this Canadian example demonstrates that there is room for creativity in cyberspace. Laymen, however well-intentioned, distill all unwelcome or inconvenient events as "hacks" or "attacks". The use of these mental shortcuts is widespread. It is perhaps most akin to exasperated entomologists who overhear other people using the word 'bugs'.

Conclusion

This paper serves as a mechanism to explore language, imagery, and other non-technical factors associated with cyberspace. It reveals significant problems with the way we conceptualize and articulate the warfighting domain. These factors are as ubiquitous as

cyberspace yet similarly obscure. The terms and metaphors commonly encountered, while sometimes playful, are not universal. They are frequently derived from specific historical and cultural contexts that are prone to romanticizing, politicizing, and misinterpreting.

Our increasingly interconnected world, while fostering innovation and unprecedented access to information, reveals a deepening reliance—if not dependence—on global telecommunications infrastructure for commerce, governance, and critical services. As society and militaries integrate technology, many of the challenges that plague cyberspace are not new. Yet our ability to describe nuanced threats remains relatively rudimental and inarticulate. These realities pose significant problems, particularly when faced with intersectional policies across government departments and agencies, between nation states, and competing priorities within the DND/CAF or GoC. The analysis, drawn from primary and secondary sources, also exemplifies how we face no greater 'wicked problem' than that of cyberspace. Despite its complexity, however, ample opportunity exists for improvement and collaborative solutions.

Automation, Autonomy, and Subsea Warfare: How the Pandemic will push us to accelerated adoption, with unintended consequences?

by Konrad Mech

Last year, I wrote an article titled *Android vs Human Soldier: What Near-Future Warfare Will Look Like*. As a former officer in the Royal Canadian Artillery who works in the technical space, I became concerned with the rapid convergence of technologies that may enable state actors to deploy android combat units in the near future. I compared the features of a notional android soldier with a human soldier, and posited some uncomfortable outcomes including maltreatment of prisoners of war, indiscriminate collateral injury or killing of non-combatants, and summary execution of targeted leadership. A respected senior commander from the Canadian Army and a military lawyer provided input on military and international humanitarian law. I believe that many similar issues must be confronted in the maritime space.

Warfare is ugly. It is much worse when state actors violate established norms by performing atrocities against military members and the civic populace at large. During WWI, Germany outraged the world in 1915 by sinking the ocean liner *RMS Lusitania*, killing 1,198 non-combatants. The German high command restricted submarine warfare until 1917, when they adopted unrestricted submarine warfare, allowing attacks against tankers and merchant vessels, including neutral vessels, without warning. This action was a significant factor in the United States decision to enter the war against Germany. Unrestricted submarine warfare occurred again in three theatres during the Second World War: during the Battle of the Atlantic (Germany against the western allies); in the Baltic (Russia and Germany against each other), and in the Pacific Theatre (Japan against USA). Today's and tomorrow's new technologies, unchecked and unregulated, could embolden some powers to engage in similar behavior in future conflicts.

While the world has been blessed with an absence of major conflict since the end of the Second World War, we are faced with the ascendancy and rapid militarization of the Peoples' Liberation Army Navy (PLAN) in China, and a resurgent Russia. Russia is already very active in the Arctic, and China has stated it has polar interests. China is asserting territorial dominance in the South China Sea, including provocative maneuvers against other navies, and has focused on asserting naval dominance as far as Hawaii in the Pacific. The PLAN also seized a USN sea glider in disputed waters in the South China Sea. With the accelerating development of intelligent mines and torpedoes, swarm drones, hypersonic missiles, subsurface sensors, weapons guidance technology, inertial navigation, and

Major Konrad Mech, P.Eng. (ret'd) *works in the Maritime industry. He has previously written for SITREP.*

The views expressed are those of the author and do not necessarily reflect the views of the Institute or its members.

a strong focus on automation and autonomy, it's a good time to devote serious thought to these issues.

In today's subsea world, the seabed hosts fixed sensor arrays listening for acoustic signals, feeling for magnetic anomalies, and measuring changes in ocean chemistry. Navies are increasingly deploying gliders and unmanned vehicles as remote sensing platforms for intelligence, reconnaissance and sentinel functions. Sensitive sensors are utilized for target location, target identification, target tracking, attack and defense/counter-attack. Battery technology is ever more sophisticated, extending mission durations. Subsea vehicles can stay submerged in 'persistent' mode, recharging their batteries at subsea docking stations and transferring collected data via acoustic modems. Inter-operational assets like submarines, sensor networks and surface assets secure ocean space and deny mobility. Trade journalists are writing pieces such as *The World's Deadliest Torpedoes* and *The Future of Drone Warfare: The Rise of Maritime Drones*. It is clear that advanced computing power, increasing battery efficiency, underwater communications technologies that enable neural networks of surface and subsea robots, and other technical advances, are converging rapidly in potent new systems. This convergence creates potential for collateral harm to non-combatants and those 'hors de combat' (prisoners of war, those surrendering), as well as significant environmental damage and degradation - unintended (or worse, intended!) outcomes in cases where human oversight and intervention are not designed into the system.

Unintended collateral consequences to innocent parties—killing them due to automation - is already a reality. Ukrainian International Airlines Flight 752 was downed by the Iranian Islamic Revolutionary Guard when a Russian surface-to-air missile system, the SA-15 Gauntlet, was set to "weapons free". Highly automated, the time from target (mis) identification to launch was less than 10 seconds. A Wikipedia entry on Gauntlet states: "The digital computers allowed for a higher degree of automation than any previous Soviet system of its type. Target threat classification is automatic, and the system can be operated with little operator input, if desired." Obviously caused by human error, Iran announced the arrest of several people over this incident. But what of truly autonomous systems, where there is no human in the decision loop at all? What party is to be brought to justice—the system manufacturer? The software coding team? The commander who deployed the system in theatre?

Prior to the COVID-19 pandemic, militaries already faced recruiting and retention challenges. These will only get more severe as potential recruits come to understand the significant loss of personal freedom and quality of life that service entails during a pandemic. Ever since the USS Theodore Roosevelt broke orders, left patrol and docked in Guam with an infected crew, military planners have struggled with how to maintain operations while protecting the health of the crew. France's aircraft carrier *Charles de Gaulle* has had a similar outbreak of COVID-19. The Royal Canadian Navy is now sequestering entire ship complements in isolation prior to operational deployment. Shore-based crew on designated duty vessels are ordered to self isolate at home. Then, once deployed, the crew will be denied shore leave to prevent contagion. This is the definition of hardship duty, and is highly unappealing to most people.

Automation gives militaries significant benefits in terms of reduced manpower required to run complex naval systems like submarines and surface vessels. During WWII, a destroyer needed 350 crew to operate. Today, the US Navy's Littoral Combat Ship is designed to be manned by 40 personnel—10% of the complement of a similar sized warship from WWII. This reduction in manning greatly eases the challenge of manning up for a conflict, and reducing losses if a vessel is taken out during combat—an advantage that military planners will exploit. Autonomy offers the potential of reducing losses even further. Deploying vessels at and under the sea without any personnel is very attractive to military planners. However, there is a moral hazard component to this. If no humans are on board, remote operators may feel empowered to take greater risks. From the perspective of the attacker, a warship or submarine without human lives on board becomes an abstract weapon. Add autonomy to the mix and there may be a bias to increasingly violent action by

attackers using autonomous weapons rather than de-escalation to reduce loss of life.

What harms could this type of moral hazard cause? Injury and death due to indiscriminate action by autonomous weapon systems and significant harm to the environment are real outcomes. During the Battle of the Atlantic in World War Two, German U-boats sunk 6,000 ships totalling 21 million GRT - vessels with munitions sent to the bottom and fuel oil spilled in the ocean. The war caused considerable environmental damage, some lasting to this very day. Many lives were lost because convoy vessels were ordered not to stop and pick up survivors to minimize additional losses to the attacking submarines. That was then. Many modern war vessels are powered with nuclear fuel. Six nations have operational nuclear submarines. The US and France have nuclear aircraft carriers. The number of Chinese nuclear subs cannot be known with certainty. Indiscriminate action against nuclear vessels could result in badly contaminated oceans.

Compared to the maritime battles of WWI and WWII, the potential for environmental damage and degradation are significant. Thousands of undetonated drones that miss their targets, toxic fuel from inbound missiles destroyed by CIWS close in weapon systems, the millions of depleted uranium rounds fired by those CIWS, and nuclear waste from nuclear sub duels would have long-lasting effects. Bikini Atoll is still hot from nuclear testing in the 1950s. And nobody will be fighting a 'green' war—the carbon footprint would be massive.

If war is the last act in the failure of diplomacy, then how to hold bad actors to account? Outcomes of war are long-duration stalemate (WWI trench warfare), disengagement without formal end to hostilities (Korean peninsula) a negotiated peace on terms (Franco-Prussian War 1870-71), or a sound defeat of one party with unconditional surrender (Japan 1945). While losers pay the price for war crimes, victors rarely do. General Curtis LeMay was the US Air Force General responsible for the firebombing campaigns of Japanese cities in the closing days of WWII. An estimated 100,000 civilians were killed in Tokyo alone. LeMay was quoted saying "Killing Japanese didn't bother me very much at that time... I suppose if I had lost the war, I would have been tried as a war criminal."

Military personnel may empathize with this overly pragmatic viewpoint. In addition, so do many corporate executives in this domain. Many companies are actively involved in developing technologies and systems on behalf of their national governments. But today, many citizens have no personal memory or experience of war, and therefore don't think that way. Shareholders and the general public engage these companies to the extent that entire departments focus on Corporate Social Responsibility and ESG - Environmental, Social and Governance. Corporations are targeted by activist stakeholders. Google recently had a Silicon Valley staff mutiny when employees found out Google was working on artificial intelligence (AI) projects for the US military. After over 3,000 employees protested, Google withdrew from participation in next-phase AI projects. Question: what if this outcome was engineered by foreign agents to hamstring the USA in order to maintain a lead in their own nation's pursuit of AI dominance?

One thing we do know is this: there is no such thing as a power vacuum. Any opening of advantage is rapidly filled by an opportunistic foe. No sooner did the *USS Theodore Roosevelt* dock in Guam than the People's Liberation Army Navy sailed its own aircraft carrier *Liaoning* past Taiwan during the weekend of April 11–12, 2020. Many people sympathize with the carrier's dismissed Master, Captain Brett Crozier. However, the chain of events is clear: he broke orders to return to port; the carrier's supporting Carrier Strike Group suffers operational degradation, and China filled the gap. This was fully predictable. In his memo, Crozier wrote:

> "We are not at war. Sailors do not need to die. If we do not act now, we are failing to properly take care of our most trusted asset — our Sailors,"… The spread of the disease is ongoing and accelerating."…Decisive action is required. Removing the

majority of personnel from a deployed US nuclear aircraft carrier and isolating them for two weeks may seem like an extraordinary measure."…This is a necessary risk. It will enable the carrier and air wing to get back underway as quickly as possible while ensuring the health and safety of our Sailors. Keeping over 4,000 young men and women on board the TR is an unnecessary risk and breaks faith with those Sailors entrusted to our care."

But Crozier got it wrong. The whole point of power projection is to deter war. And by demonstrating how easy it is to take a Carrier Strike Group out of action, Crozier just brought Nuclear, Biological and Chemical Warfare back into play. Canada's Patrol Frigates are NBCW capable. We can easily imagine operational vessels going to sea fully buttoned up, sealed from the outside environment. And we can also see how much more resilient and robust our service personnel must be to maintain their mental health under this type of work environment.

We can now make some educated guesses about the future. Recruitment will be tougher. Keeping service members healthy will be challenging. NBCW is back in play. Enemies have become emboldened. Disinformation campaigns abound—does anyone really believe the official coronavirus infection and death figures coming out of China? And the PLAN, operating under totalitarian rule, can order vessels to sea, accepting that any loss of crew to illness is an acceptable operational cost of assuming strategic control over the seas. I believe these imperatives will push the west to accelerate development and deployment of automated and autonomous systems to shore up identified weaknesses and vulnerabilities exposed by COVID-19. But there will be unintended consequences, because we don't know what the "unknown unknowns" are.

Canada: Droning On?

by Jeremy C. H. Wang

In 2019, the ten countries that procured the greatest number of drones spent $8 billion buying these advanced machines. Capable of tracking and neutralizing targets, and providing unprecedented battlefield awareness, Remotely Piloted Aircraft (RPAs)—colloquially known as drones—are an essential tool in modern warfare. But with some 82,000 surveillance and combat drones to be purchased around the world in the next ten years, there are 82,000 opportunities for militaries everywhere to leap forward or fall behind.

For Canada, the question of which drone to buy, and from whom, has posed challenges. In the 1990s, Canadair built military drones for use by other Western countries except, of course, Canada itself. Then, in the early 2000s, the Canadian Army (CA) unilaterally purchased drones for urgent use in Afghanistan, catching the Royal Canadian Air Force (RCAF) by surprise, and leading to questions over jurisdiction, budgets, and training that continue to this day. While the Canadian Armed Forces (CAF) has resolved many of these early issues, making effective use of the *Heron* and other systems in recent years, the rapid pace of technological evolution begs the question: how can we keep up? How will the CAF address its changing needs and sort out its internal challenges while technology continues to advance—and while allies and adversaries push ahead?

This article explores three essential questions that I believe must be *top of mind* among CAF members seeking to acquire a drone, especially a *small* drone. This is the new generation of field portable drones that offer increasingly advanced Intelligence, Surveillance, and Reconnaissance (ISR) capabilities at relatively low cost, lending themselves to shorter procurement cycles, and widespread tactical use. In my experience as an aerospace engineer, I have built, bought, operated, and consulted on small drones, primarily for industrial and government use. It is from this firsthand perspective that I offer these questions for future force generation.

Jeremy C. H. Wang *is a Canadian aerospace engineer and organizational leader experienced in start-ups. He holds a BASc in Engineering Science from the University of Toronto, and is the first Canadian to be recognized as one of Tomorrow's Aerospace Leaders in their 20's by the American Institute for Aeronautics and Astronautics..*

The views expressed are those of the author and do not necessarily reflect the views of the Institute or its members.

Do we even need a small drone?

These days, there is plenty of hype around drones. You would be forgiven to think you need one when in fact you do not. You would also be forgiven to think that drones simply replicate manned aircraft capabilities but in a smaller package. These misconceptions are the result of aggressive marketing, provocative media, and technological zeal that are commonplace in the current economic climate. For instance, the USAF UAS Flight Plan 2009-2047 report describes a future "MQ-Mc" drone capable of everything from ISR to electronic warfare to close air support with global strike and humanitarian assistance in between. Even if technically possible, does this make any sense? Is it efficient to use an aircraft capable of global strike but for close air support?

Instead, it is wiser to consider the drone as a completely new technology. The drone, like any airborne vehicle, is a tool that brings something (a payload) from point A to point B by air. Whether the drone is hand-launched or rail-launched, flies for 6 hours or 30 minutes, carries an optical instrument or explosive ordnance, it is fundamentally a transportation device. So, when defining the military need, it is best to start from first principles and consider what is the object that needs to be taken from point A to point B.

—COMBAT CAMERA/CPL DOUG FARMER

A Sperwer unmanned aerial vehicle outside Kabul, Afghanistan. The Sperwer was a target acquisition and surveillance drone deployed with Op ATHENA in Afghanistan.

Consider a hypothetical ISR scenario. An Army artillery unit regularly finds itself lacking intelligence on enemy locations in mountainous regions, such as during Canada's early ISAF missions in Kabul. If there is existing reconnaissance that satisfies that necessity, then a drone is not required. But if the available air support is ill-suited to the terrain, ground reconnaissance cannot get close enough, or allied air support is expected to be tied up, then perhaps there is a capability gap that needs to be addressed.

Still, a small drone may not be appropriate. The essential problem is acquiring, say, images of a certain resolution using an optical instrument that must be flown from some point A under friendly control to some point B overtop the mountain range. A small drone may not have the payload capacity to carry a sensor ball large enough to furnish such imagery. The drone may experience an unstable communications link across the varying terrain. The drone may be too loud when flying at altitude, causing the enemy to disperse or antagonize the drone. It may make sense to acquire a manned aircraft that simultaneously addresses other operational needs, in which case an ISR-only drone would be an expensive partial solution. However, if existing alternatives do not suffice, and a drone can be procured or developed that does fill the gap, then a small drone can be a highly effective option.

Indeed, drones are an incredibly valuable tool, and my intent is not to diminish them. But in most cases, drones are complementary, not superior, to an existing arsenal. Should the question ever become, "how can we replace X with a drone?", then extra caution is warranted. The invention of the TV did not simply usurp the radio. It physically and culturally rewired modern entertainment, changing the design of homes, making our lives more sedentary, creating new possibilities and risks. Besides, radios still occupy an important place in our cars. Any talk of replacement demands a critical evaluation of systemic operational impact.

Are we asking for a design or a solution?

Let us suppose there is a valid capability gap that calls for a small drone, and a tender must be issued. Procurement is always a tough process, not only because government accountability imposes certain rigidities on interacting with potential vendors, but because

the military must be careful to ask for a solution, not a design.

Militaries tend to define very specific requirements for drones while painting a murky picture of the operational use cases. Many requests for proposal detail the desired range, endurance, fuel compatibilities, NATO standards, payloads, weights, and so forth ad nauseum, yet lack a clear concept of operations. What does the operational theatre look like? How will intelligence be used and disseminated? How should the drone integrate with the military's organizational structure and doctrine? Why is a certain range needed, not more or less?

These nuances are hard to capture in writing, which is probably why they tend to be omitted entirely. However, information without context results in materiel acquisitions that fall short of unspoken expectations, or fail in unforeseen situations. The additional challenge with drones is that they resemble the fixed-wing aircraft and helicopters that militaries already know how to buy, when in reality, there are important differences. It takes only one oversight to produce a disaster, such as building an airframe to withstand a certain wind gust—but not the unquantifiable rough handling of equipment by soldiers in the battlefield. Manufacturers can always insist on further clarity, and this is a key trait to look for in good suppliers, but it is the buyer who grasps their own needs whether or not those needs have been articulated.

—COMBAT CAMERA/SGT DAREN KRAUS;

The CU-170 Heron UAV

So, how can we ensure context is communicated properly? First, much of military doctrine is already in the public domain. The USAF Close Air Support Manual is a Google search away. To the extent that information is already available, suppliers find it helpful to have a clear concept of operations as detailed through images, diagrams, and text that explain not only the "what" but the "how" and "why" of the drone and broader operational use case in question.

Second, for use cases involving greater operational complexity, uncertainty, or novelty, it can be helpful to adopt a rapid iterative approach. In this approach, the procuring unit details its requirements insofar as it is aware of what is needed, they select the most promising potential vendors based on an initial call for proposals, and together they conduct a series of test campaigns through which further requirements and issues come to light.

For instance, a drone may fit inside the specified transport truck on paper, but the procuring unit could be using a special variant. The drone may turn out to be easily jammable, which was assumed unacceptable but never specified in initial requirements. The soldiers themselves may loathe certain features, tossing the drone aside and reverting to old practices. Some suppliers will adapt and keep up, while others will not. At key checkpoints, the appropriate security clearances can be obtained for those vendors worth advancing further. By the end, it is clear which vendor, if any, has a promising solution. The United States Special Operations Command has made excellent use of this philosophy, with its quarterly Technical Experimentation events that invite industry partners to test their solutions with their operators. So has the Naval Postgraduate School, which, for almost 20 years, has held annual Joint Interagency Field Experimentation exercises. Rapid iteration and early outreach make the trade-off of allocating extra resources early in the procurement cycle to mitigate downstream risks.

Finally, a strong collaborative relationship is key. As militaries and manufacturers adapt to changing needs and technology, mistakes will happen. Innovation is, by definition, a risky endeavour. Communication must occur early, often, in all directions, and with transparency. Suppliers must recognize the high expectations of disruptive technology, just as the military must accept and be willing to work through the messy nonlinear process of true force generation. These norms are frequently at odds with traditional military and

corporate culture, but they are necessary for innovation. Before any problem can be solved, the problem of being a good partner and finding the right partner must be solved first.

Simply put, current drone procurement is tantamount to grocery shopping: write out the list, pass it to your family member, and hope for the best. It works for routine purchases when you know exactly what you want. But when cooking something new, design thinking is more appropriate. It helps to know the overall recipe, the occasion, the budget, who we are hosting, and some alternatives if the original ingredients are unavailable or cause allergies. And as with my partner, it helps to know she will continue to put up with me if I buy the wrong thing.

Who will advocate the hardest and fastest for the solution?

Advocacy is the process by which one group influences another to make the right decision. When deciding whether a small drone is needed, advocacy means grounding recommendations in the real needs and experiences of soldiers on the battlefield. It is company commanders going the extra mile to seek, share, and challenge perspectives, and as soon as reasonable, evaluate options and tender a solution. When designing the request for proposal and working with bidders, advocacy means acting swiftly, communicating thoroughly, testing ruthlessly, and choosing carefully to ensure the proper tools arrive in soldiers' hands. But, advocating hard and fast demands a certain pace, flexibility, and independence that is counter to conventional military culture. How does one fall in in line and challenge it simultaneously?

Although all branches of the CAF are capable of innovation, I maintain that new tactical solutions are best vetted and advocated for by the Canadian Special Operations Forces Command (CANSOFCOM). Their small but agile organization, demanding operations, strong reputation, and close relationships with other Five Eyes special operators make for quick, scrupulous purchasing decisions. Thereafter, equipment may be evaluated for use in other branches, informed by its CANSOFCOM trials. Fighter jets, frigates, main battle tanks should remain the responsibility of their respective service branches—but history shows that the acquisition of cutting-edge tactical equipment is best handled by special operators. Here are just two examples from recent Canadian Forces College papers.

During Operation Impact, CANSOFCOM operators faced a growing threat of vehicle-based improvised explosive devices (VBIED). In the span of just nine months, they researched the most suitable weapon system to destroy these devices, dispatched a team abroad to receive training, procured and shipped systems to Iraq, then trained remaining members on the system. In another scenario, the radio range for small drones was found to be severely limited due to the ground terrain, negating their ISR value. A CANSOFCOM operator improvised a solution to extend the height of the antennae, effectively doubling the communications range and restoring drone-based ISR. Most importantly, these VBIED and improvised antennae solutions remained in use by the conventional forces and host nation well after special operator presence.

How does CANSOFCOM achieve such frequent feats of innovation? Highly skilled personnel in a nimble organization which maintains a culture of creativity, trust, and decentralized task ownership. It would be impractical, certainly exhausting and chaotic, to apply this operating philosophy to the armed forces at large—for the same reasons that large corporations separate day to day operations from research labs and emerging business units.

Instead, by leveraging the intensity and speed of CANSOFCOM's procurement cycle, each stakeholder achieves their own goals. CANSOFCOM gains new tools that enhance their capabilities, the supplier's product earns the 'spec ops' stamp of approval, and the broader CAF can leverage the early success to inform and ease their own purchases. There are limitations to this approach, not the least of which is that CANSOFCOM is an inherently small unit with limited bandwidth to entertain new technologies all the time. But insofar as small drones are concerned, the approach can work, has worked, and is arguably the best way to fast-track the CAF's evaluation of disruptive tactical tools.

Final thoughts

No defence procurement system is perfect. Procurements always entail some degree of back-and-forth discussions, budgetary constraints, administrative intricacies, and fluctuating levels of support with the natural cadence of military and electoral turnover in long-term programs. Compared to the United States, where each service has its own acquisition authority, we further contend with a centralized purchasing organization led by the Department of National Defence and Public Services and Procurement Canada.

Fortunately, small drones and an increasing array of robotic, software, and low-cost tactical equipment are challenging some of these norms. Small drones are simpler and faster to purchase than their manned counterparts, but the hype surrounding them warrants a heightened sense of self awareness and caution—is a drone really the right solution? Moreover, the tendency to focus on requirements without context can lead these programs astray, as military and industry alike are still exploring the nuanced operational scenarios, opportunities, and challenges with deploying small drones. To harness the potential of small drones, we must err on the side of being more curious than confident, more critical than content.

One thing is certain. Whatever the future holds, the CAF's approach to finding and integrating new technologies must come from the bottom up. It must start with company commanders and innovation units asking the right questions and influencing up, down, and sideways to ensure the right decisions are made. It is at this level in the military hierarchy where enough authority, expertise, and political capital can yield transformational change. It is at this level where change is already happening.

Machine Intelligence in Targeting: Opportunities and Risks

by Liam Robertson

Artificial intelligence is the future, not only for Russia, but for all humankind. It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world.

—Vladimir Putin, 2017

Emerging technologies create conditions for greatly enhanced military capabilities that are potentially disruptive to existing power balances. Chief among the disruptive technologies we face today is Machine Intelligence (MI), also popularly referred to as Artificial Intelligence (AI). The high economic stakes of this technology provide irresistible incentive to compete in what amounts to be an arms race. The Canadian Armed Forces (CAF) and allied forces are investigating the immediate-term challenges and opportunities arising from the implementation of MI to support military operations. The uneven availability of effective MI will challenge our traditional decision-making frameworks and render irrelevant those national capabilities that do not keep pace.

This paper examines the near-term opportunities and challenges related to the implementation of Machine Learning Algorithms (MLA) within CAF Joint Targeting operations, arguing for an investment in specific MI capabilities. It will begin with an examination of considerations for employing MLA in support of military operations and the advantages and disadvantages influencing the transition to MI-enhanced warfare. The paper will constrain discussion to the CAF Joint Targeting capabilities emphasizing the near-term human/machine interface opportunities. Finally, recommendations will be proposed for the adaptation of the CAF to MI-enabled warfighting.

LCol Liam Robertson *is currently posted to the Director-General Cyber as CAF lead for Cyberspace Intelligence Force Development.*

This paper was written by a student attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. It has been published here for the first time with the kind permission of CFC and DND. The citations and bibliography which are contained in the original paper have been removed for ease of publishing; interested readers may obtain an original copy of the paper from the Editor.

The views expressed are those of the author and do not necessarily reflect the views of the Institute or its members.

Context

For the purposes of this discussion, the general variety of Artificial Intelligence related terms; Machine Learning, Synthetic Reasoning, Deep Learning Analytics, and Automated Reasoning Capabilities will be referred to as Machine Intelligence (MI). The narrow use of Advanced Neural Networks, Adaptive Algorithms, Machine Reasoning or Artificial Narrow Intelligence to accomplish complex but discrete tasks will referred to as Machine Learning Algorithms (MLA).

The unease created by the potential linkage of Autonomous Weapons Systems (AWS) to MI is not the subject of this paper, however a comment is warranted to preface discussion of MI applications in support of the Joint Targeting Cycle (JTC). AWS are not widely fielded at this time, yet the expansion of capabilities in related spheres of endeavour is likely to realize this capability in the near future. This has motivated eminent figures in the science and technical community to raise the spectre of a dystopian future if unrestrained development and proliferation continue. Machines are already an integral part of warfare, whether they are autonomous or not, and they could undermine global stability. Currently fielded systems permit independent operation within mission parameters, however, a "human in the loop" will not ensure complete safety. The 1988 *USS Vincennes* incident highlights that the human factor is the prime source of erroneous engagement.

Disruption

Disruptive technical advances permeate our society and rapidly find their way into our future battle-space. The private sector is leading the way in MI research and numerous MLA are available on-line without restriction contributing to a daily trickle of enhancement.

> The holy grail of Silicon Valley entrepreneurs is the disruption of entire industries—because that's where the big money is to be made. Amazon dominates book retailing; Uber decimates taxi services; Pandora replaces radio.

This disruption results in the destruction of livelihoods and shifts in economic and political power, yet the irresistible appeal of large investment returns builds an inexorable force for change.

Human Machine collaboration (sometimes referred to as a "Centaur"), envisions the augmentation of human decision-making rather than replacing it. Human military organizations may be thought of as a complex adaptive system that seeks to dominate other competing complex adaptive systems (our adversaries). The uncertainties surrounding the employment of MLA to support military decision-making make it unlikely that a tightly-coupled system concept will be accepted. Human-machine cooperation in loosely-coupled complex systems is expected to mitigate the inherent risk from common-mode failure of normal accident theory. Future military threats are likely to employ larger numbers, and coordinate their attacks more efficiently with more sophisticated maneuver and deception. Therefore, military planners and advisors are intent on holding effects delivery authority under human control:

> Saturation attacks from rockets and missiles could overwhelm human operators, a reality that has led over 30 nations to acquire air, rocket, and missile defense systems with human-supervised autonomous modes. Future advances in autonomy and swarming are likely to only exacerbate this trend.

Operational time-compression are increasing, however there is no expectation or requirement in the near-term for MI decision-support in the CAF to be directly linked to approving munitions effects.

Near-Term Opportunities

One of the primary means for CAF to contribute to current Coalition operations is by playing a role in Joint Targeting campaigns. The Canadian Joint Targeting enterprise has developed recent expertise through limited participation in coalition targeting operations in Afghanistan, Libya, Iraq and Syria. The Chief of Defence Staff (CDS) directed that the CAF establish a comprehensive Joint Targeting capability by September 2019. In the near-term, the CAF Joint Targeting enterprise can expect to exploit nascent MLA capabilities in three key areas:

1. Target Development—MLAs support the analysis of large data sets to enable Target Systems Analysis (TSA), Target Audience Analysis (TAA) and the target discovery activities.
2. Dynamic Situational Awareness—MLA agent enhances the authority pathway for Dynamic Targeting and contributes to Common Operating Picture (COP).
3. Capability/Options Analysis—MLAs rapidly and persistently assess Cyber and Information Domain conditions and propose coordinated courses of action to deliver effects.

Rather than focus solely on MI to enable battlefield automation, the CAF must also ensure that MI enables human cognition, facilitating a competitive JTC capable of delivering full-spectrum effects. Canada must invest in organizations, directed research and designate trial formations to gain understanding of how the integration of MI into military forces will affect future operations. An overview of near-term applications of MLA into the three identified areas of Joint Targeting follows.

Target Development

The detailed staff effort to consider precisely what synchronized effects are desired by a mission Commander requires intensive coordination throughout the targeting cycle. The JTC is an intelligence-enabled activity that is fed vast amounts of data requiring extensive analytical power. At the moment, human-selected areas are prioritised for examination in detail, leaving much data unexploited. Such target discovery can be more efficiently conducted with MLAs. Canada's space-based Synthetic Aperture Radar (SAR) data is under examination by Convolutional Neural Network to classify images. The resulting analysis has been demonstrated to be highly effective for naval and arctic surveillance exploitation using current sensors.

The general use of MLA as an analytical accelerator to classify and match incoming data to indicators and warnings is well understood. The emerging capability to provide conjectures of likely activity based on imagery data is of significant interest to target development organizations. Another example of that capability is the US Algorithmic Warfare Cross-Functional Team (also known as project MAVEN). This project was initiated to accelerate US DoD's integration of large Full Motion Video (FMV) data sets with MLA. The objective was to train the MLA to recognize and cue analysts to potential adversary entities. In late 2017, MAVEN deployed to support operations against the Islamic State.

Dynamic Situational Awareness

As demands for increased precision and tempo continue a cognitive bottleneck obstructs progress. The Intelligent Adaptive Interface (IAI) developments to enhance our dynamic targeting capability utilizing an agent-based algorithm. Enhanced decision-making speed with high confidence target sets derived from an extensive list of command options. The potential for this IAI to reduce the workload and human error by efficiently determining the target eligibility for engagement is encouraging. This entails no change in our rigorous target engagement authority process, but will require a cycle of training to engender the trust needed to employ an agent-based Graphic User Interface MLA on operations.

A significant key benefit is the requirement to adhere to the established ROE and LOAC in order to continue an engagement. For instance, if Positive Identification (PID) is lost or weapons setting are not consistent with mission parameters, then weapons release will be denied by the system. The value of an added objective review under combat engagement stress cannot be overstated.

Options Analysis

The leveraging of a Common Operating Picture (COP) that incorporates geographic and temporal representation of all-source intelligence with a natural language generated summary of the data is within grasp. This sort of cognitive persistence is demonstrated with Defence Research Development Canada's (DRDC) WISDOM project. WISDOM is a flexible federation of computer-based tools that support analysts and decision makers in developing their judgement or prediction about situations. It employs MLA to examine a series of related propositions and guide sensor collection. Nested within the DRDC Joint Intelligence Collection and Analysis Capability (JICAC) project, WISDOM has the immediate potential to support options analysis for operational target development. The broad scope of the JICAC project will likely prove unwieldy to the CAF, but the WISDOM architecture is scalable to support current operations. Intelligence augmentation with MLA enables all source intelligence enhancement through document analytics. WISDOM employs multiple automated reasoning tools for multisource exploitation of the massive data repositories analysts are required to sift through to move beyond keyword search and enable contextual searches.

Proposition queries to explore database and assist analysts in understanding a target system or audience. A synthesis of human developed engagement options or courses of action (COAs) contrasted with computer-generated COAs becomes possible. An MLA observes information differently than its human counterparts and is capable of identifying patterns in the data that human analysts may overlook due to the large volume and complexity of data. The potential for the further exploration of imperfect information is illustrated with the Libratus poker system which seemingly addresses a challenge in game-theoretic reasoning containing hidden information within a large state space.

> The techniques that we developed are largely domain independent and can thus be applied to other strategic imperfect-information interactions, including non-recreational applications. Owing to the ubiquity of hidden information in real-world strategic interactions, we believe the paradigm introduced in Libratus will be important for the future growth and widespread application of AI.

Such an MLA can also be employed to enhance the delivery of effects in the Information Environment (IE). State and non-state actors can leverage greater sophistication and scale in executing their Information Operations. The rapid creation of precise messages and media formats by MLA enables the delivery of rapidly adaptive synchronized non-munitions effects across all contested domains.

Preliminary studies also indicate that MLA-enabled offensive cyber operations will significantly enhance cyber effects. The addition of MLA to a cyber operation will increase

the tempo and variety of cyber effects while reducing the cost. Proliferation of specialized MLA will enable a broad swath of actors to engage in this activity. The key limitation will become access to the suitable algorithms and the requirement for skilled specialists will diminish.

Risks

MI is quintessentially dual use in nature. This ensures that discoveries that may yield commercial benefit will proliferate rapidly. Once proven and trusted, an MLA is materially more efficient than human centric processes and vastly scalable. The classic business objective of "faster, better, cheaper" is within grasp. Any attempt to constrain or ban such technologies will be fraught with difficulties. A motivated actor with the resources to purchase or steal a MI system may obtain tremendous offensive cyber-capability, potentially becoming an Advanced Persistent Threat (APT) even if that actor is relatively ignorant of the technology. The marginal cost of replicating software approaches zero, providing no constraint. MLAs like this could then be readily adapted to drive APT cyber-attack tactics, where the MLA is competing against human or non-adaptive defensive MLA.

MLA employing deep neural networks have proven to be an extremely powerful tool for object recognition, often can performing as well or better than humans in standard testing. Despite that success, some unexpected vulnerabilities persist. A class of visual objects known as "adversarial images" are capable of deceiving algorithms into identifying false images with high levels of confidence.

> This vulnerability of deep neural nets to adversarial images is a major problem. In the near term, it casts doubt on the wisdom of using the current class of visual object recognition AIs for military applications—or for that matter any high-risk applications in adversarial environments.

This subtle manipulation of imagery data (data poisoning) or adversarial inputs reveal emergent phenomena stemming from fundamental properties of the internal structure of neural networks. An educational loop to train the algorithm against such poisoning is ineffective since the space of all possible images is effectively infinite and the system can fail in ways humans would not. Even without knowing how a specific neural network is structured, an adversary could generate deceptive images in various media, creating false target indicators and concealing actual entities. This latent ability for exploitation of design flaws lays bare the essential requirement for human-machine cooperation in target development activities.

Due to the ability to exceed human capabilities, it has impact on human community, much like GPS has done to human navigation skills. Extended use of MLA in any area of endeavor may increase the psychological distance operators have with people they are planning to influence. The popular devotion to social networking, on-line gaming and internet surfing inculcates a potential for a reduced capacity to empathize with others. This factor has a potential to bias human analytical processes and will require a conscious effort of leaders to regulate.

The rapid adoption of MLA and other disruptive technologies require concurrent operational adaptation. Such transformation requires our forces to re-tool and conduct comprehensive capability analysis. Upgraded training and exercises will be needed for forces to work seamlessly with MLA and other systems which consumes significant investment and management resources. With the MI arms race underway, fear of having one's national project overtaken encourages the technological competition and a race to the bottom. These risks reinforce the fundamental theme that we cannot place trust in MLA or MI systems to be infallible, such systems will require continuous in-depth validation reviews and will still require supervision.

CAF Adaptation

The natural fossilization of institutional thought limits how quickly the CAF can perceive and explore emerging concepts. We possess well-honed industrial age institutions that are struggling to remain relevant in the information age. The CAF does not have the scale to create leading edge capabilities, but we are small and agile enough to rapidly operationalize functional concepts in order to seize relevance in key areas. In this manner the CAF can be "Future-proofed" to the MLA capability gap by establishing an internal centre of excellence for MI. Like many other organizations a culture of continuous improvement is required just to maintain our current relative position, not to mention establishing competitive advantage.

The cornerstone to such future-proofing is the establishment of a multidisciplinary cadre of capable CAF and DRDC members possessing MI/MLA skills and capabilities. Such a community of interest could then be provided venues to conduct formal gap analysis and brainstorm the options for CAF experimentation in this area. This falls under the broad scope of responsibility of the Chief of Force Development (CFD), where MI is understandably difficult to prioritize. The potential for collaboration with the Canadian commercial sector is growing and this may well be where the momentum for institutional involvement will originate.

Once the MLAs are tailored and implemented for the aforementioned three targeting areas of opportunity attains full operating capability, it requires validation. The conduct of challenging and realistic wargames is essential to understand and socialize the use of these improved capabilities. Events such as the Schriever Wargame 2017 rigorously challenge capabilities that are anticipated to be in operation ten years in the future. Integration of our targeting enterprise with our key allies is essential for Canada to participate in future joint coalition operations.

As this technology advances, more MLA will be available for a variety of activities, particularly for the delivery of malicious software. The development of tactics and preparation of attacks still require human expertise for the foreseeable future. The aforementioned impact of MLA accelerates the complexity and velocity of change facing military planners. The central role of the human is perceived to be under threat and there will be institutional resistance to change. However, humans remain essential:

> These and similar errors are often classified as "human errors': it wasn't the system that was at fault; it was the programmer, engineer, or user who did something wrong. But it might be fairer to call them "human to computer translation errors": a human does something that would make sense if they were interacting with another human, but it doesn't make sense to a computer.

Humans are an adaptive species and the integration of MLA within all aspects of civilian society will have transformational effects on global culture. The CAF will need to invest in systems and infrastructure that are capable of running and sustaining the increased computational power that comes with training and deploying MLA. This requires increased ties with commercial and academic institutions to keep CAF deployed hardware and software on the leading edge of the global paradigm.

Looking forward

The private sector is leading the way in MI research and Canadian world-class expertise is actively recruited by US corporations, albeit certain elements within the technology sector appear reluctant to partner with defence or security agencies. Some entities are going as far as publicly stating policies that they will not contract with defence or security agencies. This challenge has been effectively taken up by Canadian national leadership and CAF/DRDC researchers are regularly invited to MI technical seminars, conferences and trade shows.

In the long term, the establishment of a strategic Nash equilibrium in the MI realm may be the global transition solution, a condition where no powerful MI entity has anything to gain by changing their strategy while the other entities keep theirs unchanged.

Ideally Canada should implement a national programme to guide and coordinate effort along the lines of the Israeli Technion Institute cross-sector interdisciplinary research approach that contributes to worldwide technical development. Perhaps we need to secure access rights to expertise, technology and data through national legislation or some other means. It is also worth considering the establishment of a register of security cleared Canadian nationals possessing MI/MLA capabilities to be called upon in times of national emergency.

Somewhere, modern digitally-native youth infused with a culture of innovation and risk-taking will seize and retain the technological initiative. MI systems are driving global economic and military innovations and Western nations must stay in the lead. The combination of people, training, doctrine, experimentation and validation trials is our key advantage and difficult to emulate. Canada has the pieces, but we are not coherently organized to move forward at the moment. Our emerging rivals are well aware of the advantages provided by MI and must be anticipated they will employ all available options to counter our strength in the traditional domains.

Conclusion

The foregoing discussion has asserted that near-term conflicts will involve the use of MLA to support the planning and delivery of cross-domain effects. The ability to produce synchronized rapidly adapting multi-domain effects will become ever more reliant on MI, even if it is tightly paired with human guidance. The *sine qua non* of victory will be the possession of capable Machine Intelligence. In the near term, investment in such capabilities by our rivals will only increase.

Future victory will still be achieved in the Human/Informational domain and it will belong to the humans who retain the responsibility for the effects of the operations that they plan and execute. This article has examined the immediate-term opportunities and challenges arising from the implementation of MLA on the CAF Joint Targeting enterprise arguing for an investment in specific MI capabilities. It also identified some of the key factors for employing MLA in support of military operations and the advantages and disadvantages influencing the transition to MI enhanced capabilities. As the pace of warfare accelerates and trust in automated systems matures, an adaptation of human military culture must occur for the CAF to remain competitive.

In summary, the following CAF investment in emerging MI capabilities and select MLA is required in order to maintain our military value:

- Integrate the nascent MLA capabilities into the current CAF Joint Targeting enterprise (Target Development, Dynamic SA, and Options Analysis) and collaborate with allies in maintaining MI/MLA dominance.
- Future-proof the CAF to the MLA capability gap by establishing an internal centre of excellence for MI.
- Partner with select Canadian commercial and academic entities.

The high economic stakes provide irresistible incentive to compete in what amounts to be a technical arms race. Our rivals are not shrinking from the challenge. President Putin's national education message was a raw challenge to the youth of Russia to become a leader in AI; we must not allow our innate Western hubris to ignore this challenge.