National Defence | Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Enhancing the Integration of Intelligence Into Military Lines of Effort

Lieutenant-Commander Byron Ross

JCSP 49	PCEMI n° 49
Master of Defense Studies	**Maîtrise en études de la défense**
Disclaimer	**Avertissement**
Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.	Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 49 - PCEMI n° 49
2022 - 2023

Master of Defense Studies – Maîtrise en études de la défense

Enhancing the Integration of Intelligence Into Military Lines of Effort

Lieutenant-Commander Byron Ross

"This paper was written by a candidate 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. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."

« La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de difuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale. »

MIND THE GAP: ENHANCING THE INTEGRATION OF INTELLIGENCE INTO MILITARY LINES OF EFFORT, LEVERAGING MODELLING AND SIMULATION

ABSTRACT

Information has and will almost certainly remain a source of power in the world due to the role it plays in human decision making. In the realm of international relations, the acquisition and analysis of information is executed within the domain of intelligence, which increasingly transcends the spectrum of power. However, within this spectrum, the role of military power remains extant, as the ability to apply force is likely to remain relevant as a means of exerting influence, arguably, increasingly so – given the current state of global affairs as well as increasing scope and magnitude of competition at all levels. For while incentivization can occur in non-violent means – such as diplomatic and economical, violence remains the ultimate escalation available to humankind in competition with one another. Military power is the predominant means by which physical violence is exercised by states, and it is characterized not only in quantity and quality, but also in the ability to employ this power *effectively*. While this effectiveness is influenced by a number of factors, perhaps most importantly is the information available to those deciding when and how to best employ military power. Thus, the pursuit of information in support of this decision-making is of sufficient priority that it is considered a core element of the military effort. This paper explores the current construct of intelligence in the military domain, the implementation thereof within Canada, and the role of *intelligence* (as a source of information) in the development, generation and employment of a military force. Subsequently, opportunities to enhance the integration and effects of intelligence within these lines of effort is explored, with an emphasis on the potential offered through modelling and simulation.

TABLE OF CONTENTS

MIND THE GAP: ENHANCING THE INTEGRATION OF INTELLIGENCE INTO MILITARY LINES OF EFFORT, LEVERAGING MODELLING AND SIMULATION

INTRODUCTION

> *Intelligence is Canada's first line of defence.*
>
> – Canada, *Strong, Secure, Engaged*

With the ability to perceive the environment in which they exist and adapt to it, humanity continues to create ever-increasing capabilities to acquire and store information in support of this notion, almost certainly because of the age-old adage "knowledge equals power"[1] per the late Francis Bacon. Neuroeconomist[2] and author of *Birth of Intelligence* Daeyeol Lee defines intelligence (in the entity-based conceptual sense) as "the ability to solve complex problems or make decisions with outcomes benefiting the actor, and has evolved in lifeforms to adapt to diverse environments for their survival."[3] In the contemporary context, this can be loosely represented as: resolving ambiguities and uncertainties in the past and present times (in order to establish as accurate a foundation of knowledge as desired/possible), and informing extrapolation into the future – often in parallel threads or streams, frequently characterized probabilistically in the absence of the ability to explicitly define in absolute terms.

While the acquisition of information will always be of great importance, as the amount of information available increases, the ability to not only *analyze* it – but also *employ* it to the greatest extent in the most effective manner possible, becomes increasingly difficult. The term "data tomb" was proposed back in 2002,[4] to describe a repository where "data is deposited to merely rest in peace, since in all likelihood it will never be accessed again"[5] in response to the notion that data would be collected and stored, without its actual existence ever being acknowledged (other than the space required to store it)—let alone analyzed and employed.

Information in Competition

So long as there exists competition within the world, despite the many analyses suggesting humans compete to *survive* but *thrive* when they cooperate, the relentless pursuit of advantage will almost certainly endure. Rand and Nowak propose that there

[1] Francis Bacon, 'Meditationes Sacrae and Human Philosphy', 1597.
[2] The Society for NeuroEconomics describes neuroeconomics as "*a field that represents the confluence of economics, psychology and neuroscience in the study of human decision making.*" and that it "*combines the rigorous modeling from economics with psychological studies of social and emotional influences on decision making, and utilizes tools from neuroscience that permit the observation of otherwise latent valuation and decision-making computations that take place in the brain.*", accessed 30 Jan 2023
[3] Annika Weder, 'What Is Intelligence?', The Hub, 5 October 2020, https://hub.jhu.edu/2020/10/05/artificial-intelligence-daeyeol-lee/.
[4] Usama Fayyad and Ramasamy Uthurusamy, 'Evolving Data Mining into Solutions for Insights', *Communications of the ACM* 45, no. 8 (August 2002): 28–31, https://doi.org/10.1145/545151.545174.
[5] Fayyad and Uthurusamy.

exists "[a] tension between what is good for the individual and what is good for the population,"[6] within which it can be deduced that there exists a degree of scalability between the unique individual person and the aggregate global population. Consider how within a nation there often exist subsets of the population with competing ideologies (such as political parties and religions), where the latter is the functional grouping of individuals sharing a common, collective belief. In their article discussing *Cooperation and Competition in Peaceful Societies*, Bonta offers that peaceful societies "devalue achievement because it leads to competition and aggressiveness, which leads to violence they feel"[7] acknowledging that the "lack of individual competition and achievement […] does not imply that those societies are necessarily collectivist,"[8] emphasizing the presence of competitive elements – just not amongst individual *persons* within the community.

As the established notions of states and the rules-based order extant within the current global context continue to be challenged and exploited through the expansion of competition beyond the historically established (and for the most part, agreed upon) frameworks, the deterrence effects traditionally relied upon are waning in perceived effectiveness. While the role of information in competition has always existed, as the complexity of competition increases, it can be offered that so to do the challenges surrounding the employment of information – but also the potential benefits.

In the military domain (though it has extended to non-military domains as well, predominantly the academic and commercial sectors), the outcome of acquiring and analyzing information is typically referred to as *intelligence*, and the application thereof is often executed under a service-provider construct. During an evaluation of the Defence Intelligence Enterprise (finalized in 2020), one of the key findings was that "defence intelligence is critical to the success of CAF operations and the fulfillment of the DND/CAF mandate."[9] Expanding on this, Cox offers that "unlike other decision-support disciplines, the unique purpose of intelligence is to assess an adversary's probable actions, to gain advantage."[10] While this model can be considered sufficiently effective, especially in the sense that it facilitates protection of the sources and methods, issues arise when the credibility of the provider is questioned and/or the consumer demands increased clarity on the sources and methods in seeking to enhance their own understanding and confidence by independently validating the information provided –

[6] David G. Rand and Martin A. Nowak, 'Human Cooperation', *Trends in Cognitive Sciences* 17, no. 8 (1 August 2013): 413–25, https://doi.org/10.1016/j.tics.2013.06.003.
[7] Bruce D. Bonta, 'Cooperation and Competition in Peaceful Societies.', *Psychological Bulletin* 121, no. 2 (March 1997): 299–320, https://doi.org/10.1037/0033-2909.121.2.299.
[8] Bonta.; *Collectivism* is described by Encyclopedia Brittanica as "a social organization in which the individual is seen as being subordinate to a social collectivity such as a state, a nation, a race, or a social class."
[9] National Defence, 'Evaluation of Defence Intelligence' (Canada, 30 March 2021), https://www.canada.ca/en/department-national-defence/corporate/reports-publications/audit-evaluation/evaluation-defence-intelligence.html.
[10] James Cox, 'Lighting the Shadows: An Evaluation of Theory and Practice in Canadian Defence Intelligence' (Doctor of Philosophy, Royal Military College, 2011), https://www.collectionscanada.gc.ca/obj/thesescanada/vol2/002/NR82224.PDF.

sometimes simply as a matter of internal reconciliation of accountability and transparency initiatives.

Multiple excellent observations can be drawn from the latest Russian military efforts in Ukraine. On the topic of the importance of intelligence in modern military operations, Fried (a Weiser Family Distinguished Fellow of The Atlantic Council) offers in the organization's 2022 review on the Russian invasion of Ukraine that two major factors (on Russia's part) contributing to its inability to achieve operational success was its "failure to understand Ukraine and its failure to understand its own system."[11] Either one of these failures on their own could significantly detract from a military force's ability to succeed, drawing back to one of the many infamous quotes by noted scholar Sun Tzu, "if you know the enemy and know yourself, you need not fear the result of a hundred battles."[12] These two areas of knowledge (of the adversary and of one's own force) will be thematic throughout the paper, as the role of intelligence in contributing to both is explored at greater length.

Another observation that can be drawn from the current situation in Ukraine is the perceived increased tolerance for risk associated with the employment of information derived from intelligence, specifically in the pre-emptive and pro-active disclosure of such information by Allies of Ukraine, for a myriad of reasons, including the contestation and discreditation of existing and potential future Russian claims and narratives that were under consideration for employment to justify their future aggressions against Ukraine.[13] Acknowledging the purported successes in doing so,[14] this paper will leverage these and other historical examples as rationalization in support of the discussions and recommendations proposed herein.

Equiponderation

Commensurate with the quest for understanding, there is increasing reliance upon mathematical frameworks to both capture and emulate elements of the world, and quite often (one could argue almost exclusively), within the digital realm for practicality and convenience (predominantly in the form of processing times/speed and the commensurate translation to scalability). Per the Defence Administration Order and Directive on Information Technology, it is explicitly stated that "[t]he DND and the CAF are committed to […] supporting a digitally enabled CAF that is strategically relevant,

[11] Peter Dickinson, '2022 REVIEW: Why Has Vladimir Putin's Ukraine Invasion Gone so Badly Wrong?', *Atlantic Council* (blog), 19 December 2022, https://www.atlanticcouncil.org/blogs/ukrainealert/2022-review-why-has-vladimir-putins-ukraine-invasion-gone-so-badly-wrong/.

[12] Lionel Giles, *Sun Tzu On The Art Of War (1910 Translation)*, Classic ETexts (Routledge, 2000), 11, https://doi.org/10.4324/9781315030081.

[13] Julian E. Barnes and Helene Cooper, 'U.S. Battles Putin by Disclosing His Next Possible Moves', *The New York Times*, 12 February 2022, sec. U.S., https://www.nytimes.com/2022/02/12/us/politics/russia-information-putin-biden.html; Ellen Nakashima et al., 'U.S. Intelligence Shows Russia's Military Pullback Was a Ruse, Officials Say', *Washington Post*, 18 February 2022, https://www.washingtonpost.com/world/2022/02/17/ukraine-russia-putin-nato-munich/.

[14] Huw Dylan and Thomas J. Maguire, 'Secret Intelligence and Public Diplomacy in the Ukraine War', *Survival* 64, no. 4 (4 July 2022): 33–74, https://doi.org/10.1080/00396338.2022.2103257.

operationally responsive and tactically decisive."[15] It goes on to further stipulate the additional requirements to "keep pace with technological changes [and] ensure interoperability with allies."[16] While these two can and should be considered in isolation, it is equally important that their inter-relationship with each other be considered as well, as the ability of a nation to maintain pace with technological developments is not universal, and so it should be expected that variations in individual nation's efforts in this fashion are likely to create inter-operability challenges. This is perhaps best demonstrated through the employment of computer-based modelling and simulation (due to the wide spectrum of employment and means of implementation), which is transitioning from novelty to routine, and thus this will be employed as a guiding theme for select, significant elements of discussion.

Ultimately, the goal of this paper is to explore the potential available to Canada through enhanced integration of intelligence across the defence enterprise, first by reviewing the current implementation, then delving into the application across the force, with specific focus on the development, generation, and employment of the force. Subsequently, modelling and simulation will be explored, both as a function and the capability it provides (under the current and prospective implementations), as well as the potential it offers in managing select risk elements prevalent within the domain of intelligence. Finally, a series of recommendations will be proposed, distilled from the synthesis of thematic trends across the lines of investigation.

[15] National Defence, 'DAOD 6002-0, Information Technology', policies, 29 May 2014, sec. 3.9, https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/6000-series/6002/6002-0-information-technology.html.
[16] *ibid*, sec. 3.10.

PART I – THE MILITARY INTELLIGENCE SERVICE MODEL

Concept

> *There are roads which must not be followed, armies which must not be attacked, towns which must not be besieged, positions which must not be contested, commands of the sovereign which must not be obeyed.*
>
> – Sun Tzu, *The Art of War*

The intention of this section is to familiarize the reader with the concept of intelligence from a military perspective and introduce select elements that shape its implementation within a modern military organization. Before delving into the broader discussion, it is important to establish a basis of understanding and conventions. Per the relevant doctrinal volume in effect with the Canadian Armed Forces at the time of writing, *intelligence* (lower-case *i*) is defined as "the product resulting from processing information concerning foreign nations, hostile (or potentially hostile) forces or elements, or areas of actual or potential operations."[17] The process by which this product is generated is referred to as *Intelligence* (upper case *I*).[18] While the purpose of intelligence is broad, suggested by Breakspear as a "capability to forecast change in time to do something about it,"[19] it is complemented by Pecht and Tishler as "collect[ing] data and develop[ing] knowledge for decision-making by governments and military hierarchies."[20]

Contemplating the quote from Sun Tzu at the beginning of this section, in pursuing the identification of which roads should *not* be followed, those armies that should *not* be attacked, towns that should *not* be sieged, and positions that should *not* be contested,[21] *suitable* information in *sufficient* quantities (note – not necessarily comprehensive nor all-encompassing) is required by military (and by extension, political) leadership to evaluate these entities and situations in order to make these determinations. A complicating effect emerges when the notion of competition enters consideration. Desouza and Vanapalli offer that "[k]nowledge possessed by an organization must be protected and made scarce to the external world"[22] under this context, which, while they

[17] Department of National Defense, 'Canadian Forces Joint Publication 2-0 - Intelligence' (Canada, 25 October 2011), 1–1.
[18] National Defense, 1–1.
[19] Alan Breakspear, 'A New Definition of Intelligence', *Intelligence and National Security* 28, no. 5 (1 October 2013): 678–93, https://doi.org/10.1080/02684527.2012.699285.
[20] Eyal Pecht and Asher Tishler, 'The Value of Military Intelligence', *Defence and Peace Economics* 26, no. 2 (2015): 179–211, https://doi.org/10.1080/10242694.2014.886435.
[21] Giles, *Sun Tzu On The Art Of War (1910 Translation)*.
[22] Kevin C. Desouza and Ganesh K. Vanapalli, 'Securing Knowledge in Organizations: Lessons from the Defense and Intelligence Sectors', *International Journal of Information Management* 25, no. 1 (1 February 2005): 85–98, https://doi.org/10.1016/j.ijinfomgt.2004.10.007.

were directing this statement towards the private (commercial) sector, it was drawn from their review and study of the defense and intelligence sectors.

Returning to Sun Tzu, the statement "if you know the enemy and know yourself, you need not fear the result of a hundred battles"[23] suggests a strong correlation between knowledge and success. The subsequent phrase though, "[i]f you know yourself but not the enemy, for every victory gained you will also suffer a defeat" correlates specific success against knowledge of the enemy/adversary, and by denying your adversary information about your own force, this latter statement can then be applied to them – hence the requirement to protect information about your own force, while demanding increased investment towards acquiring this (expectedly protected) information about your adversary.

While the specifics surrounding the manner in which this intelligence is collected may vary, the process is fundamentally the same – changing in scale, scope and focus, as applicable to the situation and means available. There are two distinct components involved in intelligence process of acquiring information: *sources* and *methods*.[24] The *source* is the originating point of the information (relative to those that seek to acquire it for military purposes in this context), while the *method* is the means by which it is acquired from said source. A source could be a person or information system, while a method could be (alone or in combination with others): another person, a system (such as a radio-receiver) or a platform (such as a submarine or satellite). Sensitivities associated with sources and methods can be generally characterized as factors affecting the risks posed to the ability to acquire information and to the ability to leverage that already acquired.

Current Implementation – Policy

> *Accurate, timely information is a critical commodity for the Defence team and the other federal departments with which it works.*
>
> – Canada, *Strong, Secure, Engaged*

The intent of this section is to familiarize the reader with select policy elements that shape the current implementation of the defence intelligence enterprise within Canada in order to appreciate the impact on the overall function of the intelligence function as implemented, especially the constraints it imposes. While the overarching policy is the *National Defence Act*[25] (from which almost all policy and direction applicable to the military stems from), the guiding directive for Intelligence activities currently stems from the extant *Ministerial Directive on Defence Intelligence* – a document issued by the incumbent Minister of National Defence. The existence of this

[23] Giles, *Sun Tzu On The Art Of War (1910 Translation)*, 11.

[24] "mean(s)" is commonly used in place of "methods" in the author's experience, and as evidenced throughout various publications which use these terms interchangeably (typically uniformly within individual documents though) to describe the same thing – the way by which information is acquired from a source.

[25] Canada, 'National Defence Act', 1985, https://laws.justice.gc.ca/eng/acts/N-5/.

document is overtly acknowledged, but the details are of a sufficiently sensitive nature (as one could and should expect) that the contents are not made publicly available. However, given the references and derivations made throughout a wide range of documents that *are* available publicly, one can deduce the general thematic elements contained within. From the Defence Administrative Order and Directive on Defence Intelligence (8008-0), the role of defence intelligence is offered as "crucial […] in meeting the core responsibilities of the DND, including research and development, capability development and defence procurement, and enables the success of CAF operations."[26]

Further on, acknowledgement is made to the challenges in the administration of Defence Intelligence within Canada due to the "complexity and sensitivity" of the activity itself, compounded by the nature of the environment under which it is conducted – namely in the distribution of resources across functional commands and authorities, as well as geographically.[27] Both of these elements can be attributed to the current disposition of resources and the number of locations in which these functions are required.[28] In order to facilitate such, the Chief of Defence Intelligence is imbued with the authority to "exercise functional authority for all defence intelligence programs, administration and activities across the DND and the CAF, including deployed operations,"[29] while the elemental Commanders are tasked with (among other things): leading and facilitating the identification and management of associated requirements; leading and coordinating the development, integration and management of associated capabilities; and the employment of *all* assigned defence intelligence capabilities from *all* levels and domains "as directed by the CDS."[30] It is important to note that the functional structure of the Canadian Armed Forces does not readily permit the imposition of the direction of one Commander upon another equivalently-ranked Commander (in theory), but in practice, this is accomplished through identification of *supporting* and *supported* Commanders, establishing a *de facto* hierarchical relationship. Further, in the case of defence intelligence, there is a requirement established for each of the elemental Commanders to assign an advisor in this realm for the "application of CDI direction with regard to oversight and verification of their defence intelligence activities" and that they "must be responsive to the CDI direction [sic]."[31] Finally, there is a powerful statement resident within the aptly titled section *Consequences*, where the impact of *not* achieving the results established within this policy document (and by extension, others common to the defence intelligence effort) is considered to have the potential to "affect the ability of the DND and the CAF to ensure that the CAF is prepared to undertake missions for the

[26] National Defence, 'DAOD 8008-0, Defence Intelligence', policies, 18 October 2017, sec. 4.1, https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/8000-series/8008/8008-0-defence-intelligence.html.
[27] Defence, sec. 4.3.
[28] The requirement as established by the Government and Chief of Defence Staff, which almost certainly transcends the concept of a requirement in the purest sense by incorporating a range of subjective, often non-defence related considerations.
[29] Defence, 'DAOD 8008-0, Defence Intelligence'.
[30] Defence, sec. 6.1.
[31] Defence, sec. 4.9.

protection of Canada and Canadians and the maintenance of international peace and stability"[32]—significant in both scope and impact!

Commensurate with the potential adverse effects of failure within the defence intelligence effort and associated sensitivities, there exists a protective requirement. The extant directive on Defence Security for the Department of National Defence in effect at the time of writing states that in order to support the implementation of such a protective policy "a security governance structure is established, with the necessary mechanisms and resources to provide effective and integrated security risk management."[33] From this statement, the intent of managing the risks associated with the handling, processing and storage of information bearing inherent risk to various interests (ranging from departmental to national and international, in the case of partnerships and alliances) – such as that collected, generated and disseminated through the Intelligence apparatus, is established. This should be considered to be analogous to the Intelligence enterprise of other nations as similar principles almost certainly apply under the same pretense – the mitigation of risks stemming from the collection, possession, and employment of information of intelligence value.

Under this construct, information (in the most general sense) is categorized based upon the assessed potential injury that would arise from unauthorized disclosure, which the Directive on Security Management amplifies in Appendix J: Standard on Security Categorization[34], and the categorization is predicated on the assessed level of injury to the relevant interest in the case of unauthorized disclosure. For the purposes of this paper, consider the following characterizations of the risk inherent in unauthorized disclosure, emphasizing the *National* interest (vice an interest *other than* the National – which is addressed in a similar, but separate fashion)[35]:

> Confidential: Applies when unauthorized disclosure could reasonably be expected to cause *limited or moderate* injury to the national interest [emphasis added];
>
> Secret: Applies to information when unauthorized disclosure could reasonably be expected to cause *serious* injury to the national interest [emphasis added]; and
>
> Top Secret: Applies to the very limited amount of information when unauthorized disclosure could reasonably be expected to cause *exceptionally* grave injury to the national interest [emphasis added]

[32] Defence, sec. 5.1.

[33] National Defence, 'DAOD 2006-0, Defence Security', policies, 27 September 2019, https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/2000-series/2006/2006-0-defence-security.html.

[34] Treasury Board of Canada Secretariat, 'Directive on Security Management', 20 June 2019, https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611. Appendix J, Section J.2.4.1 'Information confidentiality categories – Classified'.

[35] National Defence, 'National Defence Security Orders and Directives' (Canada, 31 January 2022), chap. 6.; *Classified* refers to information sensitive to the National Interest, while *Protected* refers to information sensitive to an interest *other than* the National Interest.

In the case of information derived from intelligence efforts, the injury expected to arise from unauthorized disclosure can be attributed to a range of elements beyond defence (such as economical and political), of which this paper will focus on the *attribution* risk associated with the information, specifically in the sense that the disclosure could alert adversaries, allowing them to attribute the specific information to the source(s) and/or method(s) from which the specific it was acquired. This would almost certainly invoke a response by the adversary (including perceived *in*action) that could potentially jeopardize future collection endeavours and undermine any national and Allied efforts which were informed and shaped by the information. Derived from this is the established requirement whereby "[i]nformation in the DND and the CAF must be appropriately protected from unauthorized access, use, disclosure, modification, transmission, disposal or destruction throughout its lifecycle"[36] noting that this applies to *all* information – not just that which has been assigned an elevated classification level in response to the assessed sensitivity.

Associated with this risk is an additional protocol emplaced to mitigate it, that of *need to know*, where there exists an imperative to ensure that the dissemination of any sensitive information is limited to those with a legitimate requirement to receive it (not simply because it may be of personal interest).[37] The implementation of this protocol is varied, ranging from the risk-tolerant (note – *not* ignorant) perspective of any entity bearing an appropriate level of clearance may be exposed to the information, to the risk-averse where specialized access controls are employed to manage access to a much greater extent – often referred to as compartmentalization.[38] However, there is a consequence to this approach, as discussed during an interview hosted by NPR early in 2023 on the topic of over-classification – specifically that while there are a range of consequences for failing to properly protect information that warrants such, there are none for protecting information that does not require it (at least to the extent applied).[39] The (unintended) consequence is that information is often classified in a conservative fashion, and once classified, the process to reduce the level of sensitivity in order to increase dissemination and employability can be arduous, as this often requires a deliberate review by the originating authority. However, in response to this behaviour, attempts are often made to conserve effort by reducing the granularity in correlating accessibility with the concept of need-to-know. This issue should be acknowledged due to the additional challenges introduced into governmental transparency and information management initiatives.

[36] National Defence, 'DAOD 2006-1, Procedures for the Safeguarding and Authorized Disclosure of Information in the DND and the CAF', navigation page, 12 January 2022, sec. 4.6, https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/2000-series/2006/2006-1-procedures-safeguarding-authorized-disclosure-information.html.

[37] Defence, 'NDSOD', chap. 3.

[38] Defence, chap. 6.

[39] Kai McNamee, Ailsa Chang, and Ashley Brown, 'The U.S. Has an Overclassification Problem, Says One Former Special Counsel', *NPR*, 17 January 2023, sec. National Security, https://www.npr.org/2023/01/17/1149426416/the-u-s-has-an-overclassification-problem-says-one-former-special-counsel.

As stated during a hearing held before the United States' Subcommittee on National Security, *Emerging Threats and International Relations* during the 108th session of the United States Congress, a powerful statement is made in the introductory remarks of the second session: "The cold war paradigm of 'need to know' must give way to the modern strategic imperative, 'the need to share'."[40] In an article reviewing the transformation of the United States' intelligence community following 9/11, Clapper proposes a refinement to the above, suggesting that there now exists "the imperative of '*responsibility* [emphasis added] to share'"[41], acknowledging not only the previously established *need*—but now the responsibility to *actively* engage in the sharing of information, breaking away from the conservative approach commonly employed (if you do not share information, you are not incurring the risks associated with unauthorized disclosure by another party). As will be discussed later, the importance of sharing information has increased for a myriad of reasons, including (but not limited to) the increased prevalence of non-state actors (which pose a greater challenge in attribution) and the enhanced ability to correlate seemingly disparate elements of information, enabling the identification of previously undeterminable connections and significance. Domestically, in a 2017 report exploring the state of intelligence sharing within Canada, predominantly focused on the exchange between federal agencies and the private sector, the Conference Board of Canada[42] observes that "information and intelligence sharing is a fundamental element in protecting Canadians and improving our understanding of the Canadian threat landscape"[43] in response to adversaries becoming "increasingly coordinated and […] exploit[ing] technology in innovative ways to remain outside the reach of authorities."[44] While there exists legislation intended to facilitate sharing, the aptly named *Security of Canada Information Disclosure Act*, the nuances of the individual and organizational personalities involved must be accounted for, appreciating that a range is present – from the conservative (alternatively, risk averse) to liberal (risk tolerant). The challenge is almost certainly exacerbated when the personality requesting information trends towards the liberal end of the spectrum, and the personality receiving the request trends towards the conservative. These concepts are important to understand in order to appreciate the deficiencies identified within the current constructs, and later, the recommendations as well as their associated challenges.

[40] 'Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing' (United States Government Publishing Office, 24 August 2004), https://www.govinfo.gov/content/pkg/CHRG-108hhrg98291/html/CHRG-108hhrg98291.htm.

[41] James R. Clapper, 'How 9/11 Transformed the Intelligence Community; It's No Longer about "need to Know." Our Guiding Principle Is "Responsibility to Share."', *Wall Street Journal (Online)*, 7 September 2011, sec. Opinion.

[42] The Conference Board of Canada was founded in 1954 as a not-for-profit think tank, advertising themselves as an "integrated and independent" research institution which "master complexity through our trusted research and unparalleled connections—delivering unique insight into Canada's toughest problems so leaders can build a stronger future." https://www.conferenceboard.ca/about-us/, accessed 02 April 2023.

[43] Ruben Vroegop, 'The State of Information and Intelligence Sharing in Canada', Innovation and Technology (The Conference Board of Canada, 11 January 2017).

[44] Vroegop.

Current Implementation – CAF Organization

The intention of this section is to facilitate comprehension of the defence intelligence enterprise as currently implemented within the Canadian Armed Forces, and thus appreciate how this element could be improved upon within the specific lines of effort discussed subsequently. The intelligence apparatus within the CAF has undergone several iterations over the years since its notional inception during World War II. The current implementation is best embodied by the extant doctrinal publication on the topic and establishment of the Canadian Forces Intelligence Command (CFINTCOM)[45] in 2013, under which a significant amount of the Canadian Armed Forces' intelligence collection and analysis capabilities were consolidated under a unified command, and which is being expanded further under *Strong, Secured, Engaged.*[46] This organization is highlighted as the "only entity within the Government of Canada that employs the full spectrum of intelligence collection capabilities while providing multi-source analysis."[47] This current construct establishes a functional command bearing responsibility for military intelligence, commensurate with the elemental and operational commands it supports, specifically those responsible for the generation and sustainment of combat capabilities within their respective domains (air, land, sea and special operations)[48] and the employment thereof in support of Government-directed and mandated efforts (Canadian Joint Operation Command, CJOC)[49]. This construct enables centralization of common lines of effort, such as the collection and analysis (to varying extents) of various forms of intelligence, ensuring (notionally) consistency and coherency across the force structure. It is important to note that many of these activities are executed in conjunction with the elemental commands, often through the integration of Intelligence Officers and Operators within these commands, and the leveraging of specific platforms and technical capabilities resident within to support the realization of intelligence collection requirements.

Under the extant policy framework for corporate administration management (Defence Administration Order and Directive 1000-10), the Chief of Defence Intelligence (whom also bears responsibility as the Commander of the Canadian Forces Intelligence Command[50]) is assigned as the functional authority for: defence intelligence programs, administration and activities across the DND and the CAF (including deployed

[45] National Defence, 'Canadian Forces Intelligence Command', Official Government, Canadian Forces Intelligence Command, 23 June 2014, https://www.canada.ca/en/department-national-defence/corporate/organizational-structure/canadian-forces-intelligence-command.html.

[46] Canada Department of National Defence, 'Strong, Secure, Engaged: Canada's Defence Policy', 31 May 2019, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html.

[47] Department of National Defence, sec. A new Canadian approach to defence: Anticipate. Adapt. Act.

[48] National Defence, 'Organizational Structure of the Department of National Defence and the Canadian Armed Forces', organizational descriptions, 22 April 2013, https://www.canada.ca/en/department-national-defence/corporate/organizational-structure.html.

[49] National Defence, 'Canadian Joint Operations Command (CJOC)', not available, 19 February 2013, https://www.canada.ca/en/department-national-defence/corporate/organizational-structure/canadian-joint-operations-command.html.

[50] Defence, 'Canadian Forces Intelligence Command'.

operations); oversight and direction of defence intelligence; domestic and international defence intelligence relationships; the collection, production and dissemination of defence intelligence; the management of governance, accountability and review frameworks for defence intelligence; and the development of future defence intelligence capabilities.[51] This translates into (among other things) the authority to act as the "primary intelligence advisor within DND/CAF and to the Government of Canada."[52]

Functionally, the Canadian Forces Intelligence Command is assigned two high-level specified tasks: to collect intelligence, and to enable the analysis thereof. The former is accomplished through the provision of pertinent capabilities dispersed through a series of specialized units focused in a range of intelligence-related fields, such as: imagery, signals, meteorology, geospatial and geomatics, human intelligence and counter-intelligence. The latter is accomplished through a series of task-specific directorates focused on: policy and partnerships (Directorate General of Intelligence Policy and Partnerships [sic]); maintenance of intelligence and analytical guidelines (Directorate of Intelligence Production Management); provision of atmospheric and oceanographic data (Directorate of Meteorology and Oceanography); scientific and technical intelligence (Directorate of Scientific and Technical Intelligence); and the provision of transnational and regional intelligence (Directorate of Transnational and Regional Intelligence).[53] Of specific interest is that mention is made suggesting that the Directorate of Intelligence Production Management is responsible for models – though no further information is available and thus remains ambiguous. Despite the ambiguity, it is suggestive of the intent (if not already in practice) of employing modelling within the defence intelligence effort at the organizational level (vice niche applications managed independently at the sub-directorate level).

A key factor for consideration associated with the domestic and international partnerships are the agreements and mechanisms supporting the exchange of sensitive information between, as well as collaboration in collection and analysis among entities. In the case of receiving such information from others, the expectation to respect the classification of the information as assigned by *the originator* is included and implies the employment of suitable mechanisms to protect the information in a commensurate fashion. The implication to the willingness to engage in the exchange of sensitive information is that the repository(ies) of intelligence information within each entity will likely include (or at least reference to) information originating from others—and the associated constraint to protect it to the extent demanded by the originator.

The discussion within this section should provide for a baseline understanding of the concept of intelligence within the defence environment, and the implementation of such within Canada. In the following section, the various lines of effort within the

[51] National Defence, 'DAOD 1000-10, Policy Framework for Corporate Administration Management', policies, 12 January 2017, https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/1000-series/1000/1000-10-policy-framework-corporate-administration-management.html.
[52] Defence, 'Evaluation of Defence Intelligence'.
[53] Defence, 'Canadian Forces Intelligence Command'.

defence domain will be explored, and the concepts brought forth in this section will be leveraged to manage the scope and perspective in understanding the role of intelligence within them – especially when considering opportunities for improvement.

PART II – EXPLORING THE LINES OF EFFORT

Force Development - Overview

While the Oxford dictionary offers one definition of *force* (as a noun) as "a group of people who have been organized for a particular purpose,"[54] in the military context, the referent object can ostensibly be extended to a broader scope, by substituting *people* for *capabilities*. Within Canada, the *National Defence Act* establishes that the Canadian Armed Forces "shall consist of those of the following elements that are from time to time organized by or under the authority of the Minister: commands, formations, units; and other elements."[55] The composition of the force need not be static – rather, a static force composition is unlikely to maintain pace with the ever-changing (and not necessarily in a consistent fashion) nature of the adversary, let alone the emergence of new, previously unseen or unforecasted adversaries. As highlighted within *Strong, Secure, Engaged*, the composition of the Canadian Armed Forces is being modified in response to the recent and forecasted changes to the operating environment.[56] While these aforementioned changes have undoubtedly been informed by experience, so too have they been informed by intelligence, and thus, it should be expected that intelligence will continue to play a critical role as an *enabler* within this line of effort. The concept of force development is described by the Chief of Force Development as:

> the system of integrated and interdependent processes used to identify, conceptualize and implement necessary changes to existing capabilities, or to develop new capabilities in order to achieve desired effects during Defence operations, activities or services[57]

The composition of the force can be distilled down to three sub-components: the personnel, the capabilities they employ, the manner in which they are organized; and the ability to leverage of the strong inter-relationship between them. While a generalization, it can be considered that the inter-relationship between personnel and capabilities is more tightly correlated, while the fashion in which they are organized – while still influential, is arguably less so. This is not to say that a well-organized force, within which greater consideration has been given towards optimizing a notionally 'lesser' composition of

[54] 'Force_1 Noun - Definition, Pictures, Pronunciation and Usage Notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.Com', accessed 5 March 2023, https://www.oxfordlearnersdictionaries.com/definition/english/force_1.

[55] Canada, 'NDA'.

[56] Department of National Defence, 'Strong, Secure, Engaged', sec. The changing nature of conflict.

[57] National Defence, 'Integrated Strategic Analysis: Force Development', 11 March 2022, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/audit-evaluation/isa-force-development.html.

personnel and capabilities, cannot prevail against an opposing force for which the opposite holds true. History offers several examples where this holds true, such as the Battle of Myeongnyang in 1597,[58] the Siege of Jadotville in 1961,[59] and the most recent aggression by Russia in expanding their invasion into Ukraine at the outset of 2022. This latter example is especially demonstrative, given the perceived disparity between quantity of personnel, alleged quality of equipment, and supposed competence of the forces (all in favour of Russian forces) – and the inability to achieve the rapid, decisive victory suggested by the initial actions, such as the initial airborne assault during the opening days where elite Russian forces sought (but ultimately failed) to secure the Antonov international airport near Kyviv.[60]

Under idealized circumstances, the desirable force composition is one that is comprised of the (notionally) *best* personnel, paired with the *best* capabilities, operating under the *best* organizational structure – not only *best* within each in isolation, but also *best* in conjunction with one another. Granted, there is a contextual element that would influence the specific definition of *best* in any particular situation, and it is from this notion that a globalized element of compromise is derived. It is impractical to establish – let alone maintain, a force that has been (or at least is capable of being) optimized for *any* and *every* situation that may arise, a functionally *infinite* number of possibilities. One of the key objectives under the force development line of effort is pursuing optimization against the inevitable compromises that pervade a military force.

During an audit conducted by the office of the Assistant Deputy Minister of Review Services for Defense (results published in 2022), several observations were made regarding the force development line of effort, such as identifying "a continued need for the [Force Development] Programs", further noting that they contribute positive value and tight correlation with the extant defense policy. However, it is also noted that there exists a requirement for greater emphasis on "collaboration and enablers, technological integration, training and agile processes" due to their influence within the force development line of effort in mitigating the challenges associated with managing the current and future capability requirements.[61]

[58] 'Battle of Myeongnyang', in *Wikipedia*, 23 March 2023, https://en.wikipedia.org/w/index.php?title=Battle_of_Myeongnyang&oldid=1146266877.; According to historical records, the Korean naval forces achieved a successful outcome against a larger and better-equipped Japanese naval force.

[59] John Terrence O'Neill, 'EYEWITNESS - The Irish Company at Jadotville, Congo, 1961: Soldiers or Symbols?', 8 September 2010, https://doi.org/10.1080/714002781.; In this engagement, a small number of poorly-equipped (but well-trained) Irish soldiers deployed in support of a United Nations mission in the Congo held off a much larger and better equipped force until they were forced to surrender after expending all of their ammunition.

[60] Jack Watling, 'Russia's Underperforming Military Capability May Be Key to Its Downfall', *The Observer*, 18 September 2022, sec. World news, https://www.theguardian.com/world/2022/sep/18/russia-military-underperforming-ukraine; James Marson, 'Putin Thought Ukraine Would Fall Quickly. An Airport Battle Proved Him Wrong.', *Wall Street Journal*, 3 March 2022, sec. World, https://www.wsj.com/articles/putin-thought-ukraine-would-fall-quickly-an-airport-battle-proved-him-wrong-11646343121.

[61] Defence, 'Integrated Strategic Analysis'.

It is important to note the recommendation to place additional emphasis on *enablers*, of which intelligence is frequently identified as *core* or *key*. For it is from intelligence that many requirements are derived – especially those pertaining to the ability to affect the adversary, and likewise, resist or counter the adversary's attempts to affect the Canadian Armed Forces. However, one of the challenges faced within this line of effort is balancing the fidelity of these requirements against the expectation of broad dissemination to the industrial sector in the interests of competition, transparency, traceability and fairness. One of the principal sources of this aforementioned conflict pertains to the sensitivities of the information employed in the creation and refinement of the subject requirements. This is due to the deliberate confrontationally-collaborative construct common to many military procurement models within modern liberal democracies – one where the military (in Canada's case, represented by the Department of National Defence, DND) takes on the role of client, providing the requirements and funding, and another agency and/or department (currently identified within Canada as Public Services and Procurement Canada, PSPC), under the auspices of "support[ing] federal departments and agencies in their daily operations as their *central purchasing agent* [emphasis added]."[62] Thus, the current governmental construct of centralizing the responsibility and authority to enter into contracts on behalf of the Government of Canada resides with this organization. However, with this comes the requirement to shield the Government from undue liability – such as that which may arise from allegations from industry pertaining to unfair/unjust procurement practices.[63] This is likely a source of resistance to the employment of requirements at elevated classification levels – often traceable to the classification of the information employed in the generation of the requirements, as protocol may preclude the necessary degree of transparency to resolve such situations without alienating industry.[64]

Equally, in the interests of managing the implications to established contracts (many of which span numerous years, approaching decades in the case of major platform such as ships[65] and aircraft[66]), modifying these requirements can be difficult, bordering

[62] Public Services and Procurement Canada, 'Public Services and Procurement Canada', organizational descriptions;navigation page - institutional profile, 27 October 2020, https://www.canada.ca/en/public-services-procurement.html.

[63] 'Evidence - NDDN (44-1) - No. 34 - House of Commons of Canada', accessed 11 February 2023, https://www.ourcommons.ca/DocumentViewer/en/44-1/NDDN/meeting-34/evidence; Paul Emanuelli, 'Canadian Government Loses Direct Award Challenge', *Procurement Office* (blog), 3 June 2019, https://procurementoffice.com/canadian-government-loses-direct-award-challenge/; The Line, 'Mitch Heimpel: Want to Fix Canadian Military Procurement? This Is What It'll Take', Substack newsletter, *The Line* (blog), 14 March 2022, https://theline.substack.com/p/mitch-heimpel-want-to-fix-canadian.

[64] Acknowledging that there are likely select procurement activities that do occur at elevated levels (beyond SECRET for the purposes of this paper), the presumption here is that such instances are unlikely to be contested due to a sufficiently small scope and very small pool of potential suppliers, in addition to the management of derived sensitivities.

[65] National Defence, 'Canadian Surface Combatant', education and awareness, Canadian surface combatant Project Summary, 13 March 2013, https://www.canada.ca/en/department-national-defence/services/procurement/canadian-surface-combatant.html.

[66] National Defence, 'Future Fighter Capability Project', education and awareness, 13 December 2018, https://www.canada.ca/en/department-national-defence/services/procurement/fighter-jets/future-fighter-capability-project.html.

on impossible, for a variety of reasons. This will often result in requirements being considered fixed once a contract has been awarded to avoid incurring additional costs under the pretense of deviating from the initially agreed-upon terms, or voiding of the contract in entirety—which could lead to functional obsolescence prior to initial delivery. Under the Defence purchase and upgrade process, high-level requirements are reviewed during the Identification phase, which is the first, and subsequently refined throughout the following Options Analysis and Definition phases.[67] These phases can span a number of years themselves, and are often removed by an even greater amount of time from the delivery phase of a project, where the capability and/or effect is actually deliveredto the force (at least, initially, let alone in full).

Force Development – Case Study: The Canadian Surface Combatant Project

Consider the Canadian Surface Combatant project, which, according to the Government of Canada's Project Summary website dedicated to this project, commenced in June of 2012[68] – but this would not have marked the consideration and generation of requirements for this project. Rather, it is far more likely that many of the requirements were generated (at least conceptually) in the years leading up to this point, derived from current operational experience and informed by the intelligence *available at that time*. Subsequently, in order to commence the Request for Proposals phase, a more specific and rigidly defined set of requirements would have been established (to support the establishment of contractual metrics associated with contractor performance during, and validation of design following delivery). The Requirements Reconciliation phase was advertised as "substantially completed"[69] and the project transitioned to the Preliminary Design phase as of November 2019[70] – over seven years later. This strongly suggests that only minor changes can be tolerated to the end-product moving forward, focused more so on *how* the established requirements will be satisfied, vice changing the requirements themselves.

Now, this may appear tolerable and sound through the lens of best-business practices – but does not provide for much flexibility should there be a significant change to the current and future operating environment, such as the recent proliferation of complex and capable anti-ship-capable ballistic missiles, including the world's first ship-launched anti-ship ballistic missile – the Chinese YJ-21 *Eagle Strike,*[71] the Russian Kh-

[67] National Defence, 'Defence Purchases and Upgrades Process', education and awareness, 11 March 2013, https://www.canada.ca/en/department-national-defence/services/procurement/defence-purchases-and-upgrades-process.html.
[68] Defence, 'Canadian Surface Combatant'.
[69] Defence.
[70] Defence.
[71] Tayfun Ozberk, 'China Test-Fires New YJ-21 Hypersonic Missile', *Naval News* (blog), 20 April 2022, https://www.navalnews.com/naval-news/2022/04/china-test-fires-new-yj-21-hypersonic-missile/; Ridzwan Rahmat, 'China Expounds Capabilities of YJ-21 Hypersonic Anti-Ship Missile', *Jane's Defence Weekly*, 7 February 2023, https://customer.janes.com/Janes/Display/BSP_53424-JDW.

47M2 *Kinzhal* air-launched anti-ship-capable aeroballistic missile,[72] and hypersonic weapons such as the Chinese DF-ZF hypersonic glide vehicle.[73] These examples are notable as all have been introduced into service since 2021 (nine years since the initial requirements for this project were established) and attributed as possessing the ability to challenge conventional missile defences.[74]

While there was likely a general awareness of these systems at the time the requirements for CSC were being generated, information pertaining to the performance characteristics of these threat systems may not have been available (or significantly limited) given that all of these systems were still undergoing development at the time, and are only just now entering service. The paradox the CAF currently faces is that the next-generation surface combatant for the Royal Canadian Navy has passed the point of having significant changes made to the combat-related requirements, which were effectively finalized less than four years ago – but the first (let alone last) vessel has yet to be constructed (and is not expected until *at least* the "early 2030s",[75] assuming no delays…), functionally equating to approximately *an entire decade's* worth of lag. Several new threat capabilities have already entered the operating environment since the associated requirements for the class were functionally finalized, and indications strongly suggest more are to come. As Courtney states "[t]oday's surface fleet must be capable to detect, track and engage our adversaries' most capable anti-ship missiles",[76] and if this situation already presents a challenge (the author's experience suggests that it does), extrapolating this situation into the future strongly suggests exacerbation of the challenge.

While a naval theme was chosen to describe the challenge via this brief case study, it is readily applicable across all domains. In a 2016 paper exploring the

[72] Jane's, 'Kh-47M2 Kinzhal (AS-24 'Killjoy')', in *Weapons: Air Launched*, Air-to-Surface Missiles - Stand-off and Cruise (IHS Markit, 14 April 2022), https://customer.janes.com/display/JALWA161-JALW; Thomas Newdick, 'Russian MiG-31s Armed With Anti-Ship Ballistic Missiles Join Tu-22M3 Bombers In Syria', The Drive, 25 June 2021, https://www.thedrive.com/the-war-zone/41276/russian-mig-31s-armed-with-anti-ship-ballistic-missiles-join-tu-22m3-bombers-in-syria.

[73] Jane's, 'DF-17', in *Weapons: Strategic*, Offensive Weapons (IHS Markit, 15 September 2022), https://customer.janes.com/display/JALWA161-JALW.; The DF-ZF is the hypersonic glide vehicle payload associated with the DF-17 weapon system.

[74] Joe Courtney, 'Moskva's Sinking, the Rise of Anti-Ship Cruise Missiles and What That Means for the US Navy', Defense News, 3 May 2022, https://www.defensenews.com/opinion/commentary/2022/05/03/moskvas-sinking-the-rise-of-anti-ship-cruise-missiles-and-what-that-means-for-the-us-navy/; Ronald O'Rourke, 'China Naval Modernization: Implications for U.S. Navy Capabilities - Background and Issues for Congress (Updated)' (Hauppauge, United States: Nova Science Publishers, Inc., 2021), https://www.proquest.com/docview/2577533124/abstract/8CE8E32C5ECC46B1PQ/1; Ronald O'Rourke, 'China Naval Modernization: Implications for U.S. Navy Capabilities—Background and Issues for Congress' (Congressional Research Services, 1 December 2022), https://sgp.fas.org/crs/row/RL33153.pdf; Office of the Secretary Of Defense, 'Military and Security Developments Involving the People's Republic of China 2020 - Annual Report to Congress' (United States, 21 August 2020), https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.

[75] Defence, 'Canadian Surface Combatant'.

[76] Courtney, 'Moskva's Sinking, the Rise of Anti-Ship Cruise Missiles and What That Means for the US Navy'.

dependency of military capabilities on technological development, Kuikka et al (members of the Finnish Defense Research Agency) provide an insightful observation pertaining to the characteristic uncertainty pervasive in many technologies, offering that a military force "cannot know which emerging technologies mature to have profound impacts, how long that maturing will take nor the technological trajectory."[77] They subsequently expand further, delineating between continuous and discontinuous technological changes, drawing upon the model established by Dosi in 1982,[78] highlighting that continuous changes are often constrained to an existing technological paradigm (and thus, easier to forecast/predict), while discontinuous changes are more likely to be associated with the emergence of a new paradigm.[79]

Force Development – Outlook Not So Good

> *The characteristics of conflict have changed significantly over the last 10 years – from the underlying causes to the actors involved and their methods of warfare.*
>
> – National Defence*, Strong, Secure, Engaged*

In 2018, O'Hanlon stated that "technological change of relevance to military innovation may be faster and more consequential in the next 20 years than it has proven to be over the last 20"[80] in a paper forecasting change in military technology in the period of 2020 through 2040. A key driver is offered in identifying that "multiple countries (most notably China, but also Russia) now have the resources to compete with Western nations in military innovation."[81] In light of the shrinking gap (and in some cases, inverting) within the innovation space – especially where adversaries can and should be expected to deliberately focus on exploiting vulnerabilities and creating disruptive effects, can force development continue effectively under the current construct? Consider the reliance upon intelligence to inform the requirements for capabilities intended to enable the CAF in the present and future – and how the CAF is functionally constrained in the ability to leverage it in a comprehensive and fulsome manner. The complexity of this particular question increases when increased machine-learning and autonomous decision-making capabilities are considered, significantly reducing the benefits offered by select operational advantages frequently touted, such as experience in conflict and competence.[82] Returning to the work of Kuikka et al, their efforts in modelling the

[77] Vesa Kuikka, Juha-Pekka Nikkarila, and Marko Suojanen, 'Dependency of Military Capabilities on Technological Development', *Journal of Military Studies* 6, no. 2 (30 November 2015): 29–58, https://doi.org/10.1515/jms-2016-0170.

[78] Giovanni Dosi, 'Technological Paradigms and Technological Trajectories: A Suggested Interpretation of the Determinants and Directions of Technical Change', *Research Policy* 11, no. 3 (1 June 1982): 147–62, https://doi.org/10.1016/0048-7333(82)90016-6.

[79] Kuikka, Nikkarila, and Suojanen, 'Dependency of Military Capabilities on Technological Development'.

[80] Michael E. O'Hanlon, 'Forecasting Change in Military Technology, 2020-2040', *Brookings* (blog), 11 September 2018, https://www.brookings.edu/research/forecasting-change-in-military-technology-2020-2040/.

[81] O'Hanlon.

[82] Timothy R. Heath, 'China's Military Has No Combat Experience: Does It Matter?', 27 November 2018, https://www.rand.org/blog/2018/11/chinas-military-has-no-combat-experience-does-it-matter.html; Alastair

dependency between military capabilities and technological developments rely heavily on the use of operational scenarios (as do many others) – which are inevitably informed (to varying extents) by intelligence.[83]

It would be naïve to presume that the conceptualization and development of force capabilities could occur in isolation – a theme frequently debated significantly in a variety of forms, often associated with the anticipated onset, or continued persistence of conflict. As such, and as expected, the dominant efforts in force development are often aligned with the most recent experience – likely driven by recency bias. A statement made in 2021 by Major General Donahoe – then commanding general of the US Army Maneuver Center of Excellence, and Spencer – the current chair of Urban Warfare Studies with the Modern War Institute at West Point, in their editorial article *A Status Check on The Army's Preparation For The Next War*, where they offer insight into the implication, specifically that "military forces often fail to focus on the enemy they should be preparing for—the ones they are most likely to fight in the future."[84] In order to strive to remain competitive in the modern military operating environment, it is no longer tolerable that significant own force capability developments *nor* (timely) reactions to those of the adversary, unfold over timeframes spanning multiple years—let alone decades, as is increasingly common with the complex capabilities and platforms in demand with modern military forces. Rather, opportunities to increase the efficiency in executing these tasks should be continually *sought out*, *prioritized* for implementation, and *sustained*.

Hodický et al highlight that "[a]chieving military credibility in parallel to mathematical rigor to support decision-making processes is therefore a continuous effort"[85] emphasizing the entwined nature of credibility and decision-making – but also the increased demand for traceability and rationalization within the establishment of the former and outcome of the latter. It is practically untenable that any procurement (especially defense-related) would be supported under the pretense of unsubstantiated and functionally philosophically-derived decisions based upon an individual's experience alone. Rather, the demand for detail surrounding such decisions and the processes that led up to them is likely to increase, especially in an environment where multiple demands compete for limited resources – as is common to defence procurement within Canada. Consequently, modelling and simulation is being increasingly employed to facilitate the conveyance of information, often through the provision of visualizations to convey complex concepts/scenarios and validation of claims associated with both requirements

Gale, 'China's Military Is Catching Up to the U.S. Is It Ready for Battle?', *Wall Street Journal*, 20 October 2022, sec. World, https://www.wsj.com/articles/china-military-us-taiwan-xi-11666268994; Watling, 'Russia's Underperforming Military Capability May Be Key to Its Downfall'.

[83] Kuikka, Nikkarila, and Suojanen, 'Dependency of Military Capabilities on Technological Development'.

[84] Maj Gen Patrick J. Donahoe Spencer John, 'A Status Check on the Army's Preparation for the Next War', Modern War Institute, 6 July 2021, https://mwi.usma.edu/a-status-check-on-the-armys-preparation-for-the-next-war/.

[85] Jan Hodický et al., 'Computer Assisted Wargame for Military Capability-Based Planning', *Entropy* 22, no. 8 (August 2020): 861, https://doi.org/10.3390/e22080861.

and proposals. This will be discussed further in a subsequent section dedicated to this topic.

The preceding discussions on force development should be considered as additional context for the discussions that will follow, for it is from this line of effort that all others are functionally derived and are thus dependent upon. Equally though, it should be acknowledged that there exists an iterative, integrated and cyclical interaction amongst the lines of effort. The following subsection describes the line of effort that follows this, the generation of the force as conceived by the development process.

Force Generation - Overview

> *People who write about spring training not being necessary have never tried to throw a baseball.*
>
> – Sandy Koufax

Canadian military doctrine describes force generation as: "organizing, training, and equipping forces for employment. [It] integrates four major components: force structure, equipment, readiness, and sustainability."[86] This translates into the preparation of military elements that can subsequently be assigned to operational commanders in order to create a military capability that can be leveraged by the Government in pursuit of the National Interest. Within this framework, intelligence contributes to *supporting* (in contributing component capabilities that will compose the force employment elements) and *enabling* (in the form of informing training elements) roles.

As a subset to the composition of a military force, the capabilities with which they are equipped is fundamental. While the discussion earlier in the section on force development addressed the identification of capabilities and conceptual application thereof, it is under the force generation construct that those capabilities are paired with the people that will employ them. Crucial to this pairing is the delivery of training to the personnel to operate and employ these capabilities both as intended, and in as effective a manner as possible. In a resource-constrained environment, such as the one the CAF currently finds itself operating within (a shortage of approximately 10,000 regular force personnel, according to media engagement by the Department of National Defence and comments delivered by the Chief of Defence Staff in late 2022[87]), it is necessary that efficiencies be sought out wherever and whenever possible.

[86] Department of National Defence, 'Canadian Military Doctrine', *Canadian Forces Joint Publication* Canadian Military Doctrine, no. CFJP 01 (September 2011): 27.

[87] Lee Berthiaume, 'Defence Chief Calls on Canadians to Rally behind Military during Personnel Crisis | CBC News', CBC, 15 October 2022, https://www.cbc.ca/news/politics/wayne-eyre-canada-military-personnel-shortage-1.6617951; Murray Brewster and Richard Raycraft · CBC News ·, 'Military Personnel Shortage Will Get Worse before It Gets Better, Top Soldier Says | CBC News', CBC, 6 October 2022, https://www.cbc.ca/news/politics/eyre-shortage-directive-1.6608107.

Force Generation – Training the Force

In the context of training, a compromise must be made between quality and time – often biased towards the latter, as the goal of force generation is to prepare both the individual members as well as the larger organization (and all sub-groupings in between) for service in as little (as reasonable) time as possible. Equally, an additional balance is sought between accessibility (and by extension, currency) and relatability. Within their review on the multiple factors affecting the effect of knowledge transfer in PC-based simulations and games under the US Defense Advanced Research Projects Agency's (DARPA)[88] DARWARS Training Superiority Initiative in 2003, Alexander et al offer a great synopsis applicable herein, notably that "[all] training…entails transfer of lessons learned in the structured environment to the relatively unstructured atmosphere of real-world application"[89] and further establish four specific factors that are relevant to military training: fidelity, immersion, presence, and operator buy-in.[90] While their work is specific to the virtual domain, these factors can be considered relevant to the more fulsome spectrum of training employed by the military.

Consider the inter-relationship of the first two (fidelity and immersion) with the last (operator buy-in), where the first can be directly influenced by the integration (or conversely, lack thereof) of available information, which in the context of incorporating adversarial operational concepts (doctrine, tactics, and protocols) and combat capabilities would almost certainly benefit from a greater ability to draw upon more timely intelligence information – as this information significantly influences the representation of these elements in the training environment. Rózsa et al provide an expanded interpretation of immersion in one of their submissions to Frontiers in Psychology in 2022, describing it as "a psychological response to a precisely drawn-up and realistic stimulus set generated by a computer or other medium" and subsequently highlight a dependency upon what they refer to as "technical instrumental conditions".[91] Fundamentally, as the fidelity of the simulation environment approaches that of reality, those immersed within it are likely to benefit from the experience to a greater extent as less effort is required on their behalf to reconcile the training environment against their reality. A readily accessible example would be that of screen resolutions, whereby technological advancements in both hardware and software have facilitated the design and manufacture of screens and monitors capable of visual resolutions which approach (and in some cases/circumstances, exceed) the ability of the average human to distinguish

[88] 'Defense Advanced Research Projects Agency', accessed 25 February 2023, https://www.darpa.mil/.
[89] Amy L Alexander et al., 'From Gaming to Training: A Review of Studies on Fidelity, Immersion, Presence, and Buy-in and Their Effects on Transfer in PC-Based Simulations and Games', 2005.
[90] Alexander et al.; 'DARPA Defense Sciences Office - Training Superiority (DARWARS)', 20 July 2006, https://web.archive.org/web/20060720163726/http://www.darpa.mil/dso/thrust/biosci/training_super.htm.
[91] Sándor Rózsa et al., 'Measuring Immersion, Involvement, and Attention Focusing Tendencies in the Mediated Environment: The Applicability of the Immersive Tendencies Questionnaire', *Frontiers in Psychology* 13 (14 July 2022): 931955, https://doi.org/10.3389/fpsyg.2022.931955.

from reality.[92] Conversely, it is likely a challenge for a pilot flying across a flat, open plain at high altitude attempting to practice terrain-following through a mountain range to reconcile their current environment against the actual environment in which this learning would be applied.

The employment of digital means and methods provide opportunities not previously available, namely in reducing the requirement for live training (*real* people with *real* equipment in the *real* world, such as a mechanized brigade conducting exercises in the field with their troops, equipment and vehicles), as such events are often complex (relatively speaking) and resource-intensive. In their book discussing military power, Biddle observes that "The defense debate is increasingly focused on technology […] fueling growing pressure to speed modernization by spending less on training and readiness."[93] The inherent irony of this statement is that much as technology is viewed as enabling combat capability, so to does it enable the training element fundamental to the generation of said capability. While there will almost certainly always be a benefit to live training, there is increasing appetite for digital supplements and supplants – driven by the increase in immersiveness offered through technological advancements and resource savings.[94]

Increasingly, modern military forces are adopting what is referred to as the live, virtual, constructive (LVC) synthetic training environment model, where the full spectrum of training means and methods are integrated in a holistic, blended manner, with a goal of enhancing coherency across the training experience for the individual and collective.[95] Under this model, a distinction is made between *real* and *simulated* entities/environments, and the categorization represents the manner in which they are

[92] Christina M. Funke et al., 'Five Points to Check When Comparing Visual Perception in Humans and Machines', *Journal of Vision* 21, no. 3 (March 2021), https://doi.org/10.1167/jov.21.3.16; Jingdong Wang et al., 'Deep High-Resolution Representation Learning for Visual Recognition', *IEEE Transactions on Pattern Analysis and Machine Intelligence* 43, no. 10 (October 2021): 3349–64, https://doi.org/10.1109/TPAMI.2020.2983686.

[93] Stephen D. Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle*, STU-Student, Book, Whole (Princeton, N.J: Princeton University Press, 2004), 15, https://doi.org/10.1515/9781400837823.

[94] Barry Kirby, Graham Fletcher, and Helen Dudfield, 'Live Virtual Constructive Training Blend Optimisation Study' (NATO Modeling and Simulation Group Symposium, Bern: NATO, 2011), 18, https://www.researchgate.net/profile/Barry-Kirby/publication/260451734_Live_Virtual_Constructive_Training_Blend_Optimisation_Study/links/00b495315a1f869c60000000/Live-Virtual-Constructive-Training-Blend-Optimisation-Study; Jeremiah Rozman, 'The Synthetic Training Environment', *Association of the United States Army SPOTLIGHT* 20, no. 6 (December 2020), https://www.ausa.org/sites/default/files/publications/SL-20-6-The-Synthetic-Training-Environment.pdf; Mike Hernandez et al., 'Enhancing the Total Learning Architecture for Experiential Learning', in *Best Paper Sesssion 1* (Interservice/Industry Training, Simulation and Education Conference, Orlando, FL: National Training & Simulation Association, 2022), https://s3.amazonaws.com/amz.xcdsystem.com/44ECEE4F-033C-295C-BAE73278B7F9CA1D_abstract_File16562/PaperUpload_22461_0826100039.pdf.

[95] Under Secretary of Defense for Research and Engineering, 'DEM&S Glossary – DCTO(MC)', Database, The Digital Engineering, Modeling and Simulation (DEM&S) Glossary, accessed 26 February 2023, https://ac.cto.mil/de-ms-glossary/.

combined.[96] This model represents a functional paradigm shift, whereby the role of modelling and simulation within training is shifting from niche, specific applications, towards a more fulsome integrated approach, with digital frameworks offering the means to integrate the individual elements together in a common synthetic environment.

Consider that annually (in various forms since 1966[97]), the US' National Training and Simulation Association (itself, an affiliate subsidiary of the US National Defence Industrial Association) hosts the *Interservice/Industry Training, Simulation and Education Conference*, touted as "the world's largest modeling, simulation and training event"[98] which brings together parties across a wide range of academic, commercial, industry and government entities from around the globe[99] to "[promote] international and interdisciplinary cooperation within the fields of modeling and simulation (M&S), training, education, analysis, and related disciplines"[100]—with a nexus in defence. The attractiveness and significance of this event has continued to grow in response to the training demands in the defence domain, with an almost exclusive focus on digitally-enabled concepts and offerings.

While there exist a number of distinct elements within the force generation line of effort, the training element can be considered the critically dominant of these for the role it plays in integrating the personnel with the capabilities they will employ, and its contribution to the effectiveness of the force for application, as will be discussed in the next chapter. Equally, emphasis was placed on this element due to the reliance upon intelligence in support of its execution. Therefore, as the training effort shifts further towards a holistically integrated model within a synthetic environment, residing on a common digital framework, there exists opportunity to enhance the integration of intelligence with this effort – by leveraging a similar construct and approach.

Force Employment – Overview

> *No ship goes to sea, no aircraft takes flight, and no boots hit the ground anywhere in the world without the input of specialists from the defence intelligence community.*
>
> – Canada, *Strong, Secure, Engaged*

In their book exploring the concept of military power, Biddle postulates that "force employment has played a more important role than either technology or preponderance for twentieth-century warfare. *How forces are used is critical*. [emphasis

[96] Live = almost everything *real* (ie. Live operators operating real equipment in a live environment); Virtual = *real* people leveraging *simulated* equipment and/or environments (ie. Live operators operating simulated equipment in a simulated environment); Constructive = almost everything *simulated* (ie. Simulated operators operating simulated equipment in a simulated environment).

[97] National Training and Simulation Association, 'History | I/ITSEC', History | I/ITSEC, accessed 16 April 2023, https://www.iitsec.org/about-iitsec/history.

[98] National Training and Simulation Association, 'About I/ITSEC | I/ITSEC', About I/ITSEC, accessed 16 April 2023, https://www.iitsec.org/about-iitsec.

[99] While overall participation is quite open, access is limited to US, its Allies and NATO members.

[100] National Training and Simulation Association, 'About I/ITSEC | I/ITSEC'.

added]"[101] Current Canadian military doctrine defines force employment as: "the application of allocated military means to achieve specified objectives or effects through activities such as operations, defence diplomacy, and […] defence activities"[102] and further describes the force employment effort as the process which includes "all activities required to plan, execute, and review joint operations,"[103] which are further delineated in seven distinct phases: planning, preparation, buildup, execution, termination, reconstitution, and analysis.[104] *Strong, Secure, Engaged* espouses this when articulating the new vision for the Canadian Armed Forces, stating that the application of military force will be "part of a coherent, coordinated, whole-of-government effort in concert with diplomatic engagement, humanitarian and development aid, and other measures."[105] Equally, deference to the unique capabilities nascent within the armed forces is established by acknowledging the existence of situations where the "military may be *uniquely* [emphasis added] called upon to act in Canada's interests."[106] Within all of these, defence intelligence is drawn upon to ensure understanding (of the environment and adversaries) and serve in a validation role (confirming or refuting previously established, and informing future assumptions), and this is elegantly captured within *Strong, Secure, Engaged* where it is stated that "[the] ability to collect, understand and disseminate relevant information and intelligence has become *fundamental* [emphasis added] to the military's ability to succeed on operations."[107] The discussion that follows will explore select functions and capabilities core to the effective employment of a force.

Force Employment – Communication and Decision Making

Communication is a concept fundamental to the universe, applying to a wide range of interactions, transcending physics (at least as we currently understand them). There are numerous definitions, often stemming from the generalization common to many dictionaries, specifically "the imparting or exchanging of something"[108] (or some variation thereof), where said *thing* can itself be drawn from a broad range – not just information. There is an inherent flexibility imbued within the broad applicability of the term, and for the purposes of this paper, consider the following, qualitative definition: "[t]he transmission or exchange of information, knowledge, or ideas"[109] moving forward, and where appropriate, that the information or knowledge is derived from *intelligence*, as well as the ideas themselves deriving from *Intelligence*. Commensurate with this

[101] Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle*, 16.

[102] Department of National Defence, 'Canadian Forces Joint Publication 1.0 - Canadian Military Doctrine' (Canada, April 2009), para. 0529, https://publications.gc.ca/collections/collection_2010/forces/D2-252-2009-eng.pdf.

[103] Department of National Defence, 'Canadian Forces Joint Publication 3.0 - Operations' (Canada, July 2010), para. 0201, https://publications.gc.ca/collections/collection_2011/dn-nd/D2-252-300-2010-eng.pdf.

[104] National Defence, para. 0205.

[105] Department of National Defence, 'Strong, Secure, Engaged', sec. Articulating a New Vision for Defence.

[106] Department of National Defence, sec. Articulating a New Vision for Defence.

[107] Department of National Defence, sec. A new Canadian approach to defence: Anticipate. Adapt. Act.

[108] 'Communication, n.', in *Oxford English Dictionary - Online* (Oxford University Press), accessed 5 March 2023, https://www.oed.com/view/Entry/37309.

[109] 'Communication, n.'

definition is the requirement to characterize the exchange, specifically in terms of effectiveness, for which the following subsets are considered applicable: throughput (the rate at which information can be passed/exchanged),[110] accuracy ("the state of being exact or correct")[111] and precision ("the quality of being exact, accurate and careful").[112]

The ability to communicate remains core to the execution of military matters, often in support of decision making and force coordination (in support of the decisions rendered). In many modern military forces, digital technology continues to be incorporated and leveraged to the greatest extent possible, with the intent of accelerating a force's ability to acquire and exchange information (ideally, outpacing that of the adversary), and increasing the effectiveness of the exchange by reducing the likelihood of errors and omissions (again, ideally outmatching the adversary). In terms of the contribution to effectiveness in the military environment, Lewińska offers that "the informational and organisational function of communication is decisively dominant."[113]

One of the manifestations espousing these principles is known as the tactical data link.[114] Rather than relying on the passage of information by voice or teletype, data link systems "offer a […] solution for exchanging information over a common [digital] network."[115] While the original concept was to facilitate the (limited) exchange of aerial track information between terrestrial air defence locations over earthbound communication cables,[116] the latest iterations offer significantly expanded capabilities and capacities.[117] Modern data link systems typically operate over wireless communication bearers (ranging from short-range line-of-sight systems to the functionally unlimited range of satellite communication systems), sometimes interfacing with existing radio systems, or incorporating a dedicated, bespoke radio-frequency component.[118] In anticipation of signature reduction requirements and/or adversarial action in denying use of the radio-frequency spectrum, most remain capable of operating

[110] 'Throughput Noun - Definition, Pictures, Pronunciation and Usage Notes | Oxford Advanced American Dictionary at OxfordLearnersDictionaries.Com', accessed 5 March 2023, https://www.oxfordlearnersdictionaries.com/definition/american_english/throughput.; derived from definition provided: "the amount of work that is done…in a particular period of time"

[111] Oxford University Press, 'Accuracy Noun - Definition, Pictures, Pronunciation and Usage Notes | Oxford Learner's Dictionary of Academic English at OxfordLearnersDictionaries.Com', accessed 5 March 2023, https://www.oxfordlearnersdictionaries.com/definition/academic/accuracy.

[112] 'Precision Noun - Definition, Pictures, Pronunciation and Usage Notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.Com', accessed 5 March 2023, https://www.oxfordlearnersdictionaries.com/definition/english/precision.

[113] Monika Lewińska, 'The Role of Communication in Military Leadership', *Journal of Corporate Responsibility and Leadership* 2 (9 March 2016): 37, https://doi.org/10.12775/JCRL.2015.003.

[114] Historically, the term Tactical Data Information Link (TADIL) was employed, but has been supplanted by the current terminology, Tactical Data Link (TDL).

[115] 'TACTICAL DATA LINK – FROM LINK 1 TO LINK 22', *Scientific Bulletin of Naval Academy* 19, no. 2 (15 December 2016), https://doi.org/10.21279/1454-864X-16-I2-046.

[116] C. Golliday, 'Data Link Communications in Tactical Air Command and Control Systems', *IEEE Journal on Selected Areas in Communications* 3, no. 5 (September 1985): 779–91, https://doi.org/10.1109/JSAC.1985.1146251; 'TACTICAL DATA LINK – FROM LINK 1 TO LINK 22'.

[117] 'TACTICAL DATA LINK – FROM LINK 1 TO LINK 22'.

[118] 'TACTICAL DATA LINK – FROM LINK 1 TO LINK 22'.

over physical interconnecting cables – increasingly including high-bandwidth fiber-optic types.

As the capacity of these systems has increased, so too has the demand for increased diversity in information to be passed by them, and their centralized role in what has come to be known as "network-centric warfare"[119], where, as the name suggests, the networking component of the warfighting capabilities in play are central to the overall function (as a result of the emphasis placed on the ability to exchange information), and thus contingent to the intended employment of the force, acknowledging that there often exists a variety of resilience and redundancy measures within the force to permit the continuation of operations if and when the network is degraded or otherwise unavailable. The discussion above on communication and tactical data links is relevant to the future discussions herein for two specific reasons. First, the establishment of the requirement and generated capability to exchange information. The second is the willingness to assign an elevated level of credibility to an information source that is both removed from the consumer (indirect observation) as well as a function that is increasingly less reliant on human input and interaction.

As the speed and complexity of conflict continues to increase, Gray offers in their book exploring shifts in the political domain of conflict that "the central role of human bodies in war is being eclipsed rhetorically by the growing importance of machines."[120] While the context was seeking to address the supplantation of humans by machines in conflict (perhaps best represented by the rapid and prolific introduction of uninhabited autonomous vehicles in military capabilities and capacities), this can be extended to decision-making – specifically in the form of aids for human commanders, as captured by Chin in their publication exploring the inter-relationships between the state, war and technology, where they state "humans are now being challenged by machines in the cognitive as well as the physical domains of work."[121]

This section discussed the role of communication and growing impacts to decision making within the force employment effort. The reliance on timely and effective communication for conveying information derived from intelligence is related to the decision-making abilities of military commanders and government decision makers. Subsequently, a brief discussion on the rapidly expanding scope and magnitude of information both available to, and expected to be incorporated by decision-makers reinforces the case for optimization of the intelligence effort, namely in reducing the burden imposed upon decision-makers without detracting from the outcome of their process.

[119] Erik J. Dahl, 'NET-CENTRIC BEFORE ITS TIME: The Jeune École and Its Lessons for Today', *Naval War College Review* 58, no. 4 (2005): 109–36.

[120] Chris Hables Gray, *Postmodern War: The New Politics of Conflict* (Routledge, 2013), 22.

[121] Warren Chin, 'Technology, War and the State: Past, Present and Future', *International Affairs* 95, no. 4 (1 July 2019): 765–83, https://doi.org/10.1093/ia/iiz106.

Challenges Within the Lines of Effort

Over-classification hinders.

– Flynn and Flynn, *Integrating Intelligence and Information*

One of the key challenges facing the effective integration and employment of intelligence in operations is that of balancing the classification assigned to information derived from intelligence – presumedly arising from a conservative approach to protecting the sources and methods associated with the acquisition and analysis of the intelligence, and the ability to employ this information in an effective manner at the operational level. Flynn and Flynn identify a fundamental issue – the perceived incongruity between those who work with Intelligence (the collection and analysis), and those who employ intelligence (the analytical product that emerges from the military intelligence apparatus) when it comes to understanding the domain of the other, summarizing in explaining that the intelligence community "sees integration with two components (collection and analysis)"[122] while the operational community "seeks an outcome, an action, a result from the enormous amount of collection and analysis [intelligence] performs."[123]

As alluded to earlier, this creates a service provider/client relationship between the apparatus that collects and analyzes the information that arises from Intelligence activities, and those that rely on the products that emerge. Pothoven, Rietjens and de Werd explore this concept in their work exploring the producer-client paradigms within defence intelligence, contrasting these organizations against the similar (but sufficiently different) civilian intelligence organizations. One of the key compounding effects identified is that while defence intelligence efforts are predominantly focused on "military topics aimed at military clients"[124] the "networked and multifaceted character of defense intelligence warrants a conceptualization more closely approaching one of overlapping roles,"[125] speaking to the prevalent role this effort plays within the much broader intelligence effort at the national level, by virtue of the role defence plays in national security.

The compound effect of these competing requirements, which may not always be reconciled (in whole, or in part) with any regularity, are discussed by a variety of authors, including Davies in their work investigating the United Kingdom's Defence Intelligence

[122] Michael T. Flynn and Charles A. Flynn, 'Integrating Intelligence and Information: "Ten Points for the Commander"', *Military Review* 92, no. 1 (2012): 4.
[123] Flynn and Flynn.
[124] Saskia Pothoven, Sebastiaan Rietjens, and Peter de Werd, 'Producer-Client Paradigms for Defense Intelligence', *Defence Studies* 23, no. 1 (2 January 2023): 68–85, https://doi.org/10.1080/14702436.2022.2089658.
[125] Pothoven, Rietjens, and de Werd.

construct. In this work, they highlight the severity of the difficulty in reconciling the "seemingly intuitive inferences"[126] of correlating the defence intelligence effort with those of both the requirements of the military *and* those of the broader political body.[127] Marrin discusses the relationship between the intelligence apparatus and decision-makers as it pertains to politicization and receptivity, establishing what is now known as the *proximity hypothesis*, suggesting that "greater distance between intelligence and policy produces a more accurate but less influential product whereas greater closeness leads to increased influence but decreased accuracy."[128] In general, while many may agree *in principle*, Pothoven, Rietjens and de Werd disagree under their earlier pretense of "overlapping roles,"[129] suggesting that the challenge of exerting of influence is countered by the broadened scope of engagements, effectively reducing the likelihood of successful influence due to the competition between the various entities under engagement. One critical element of influence that remains extant though is that of the larger department within which the defence intelligence apparatus is embedded, upon it, which can lead to contradicting demands – objectivity and (departmental) loyalty.

Decisions, Decisions…(Everywhere!)

Within this section, the three lines of effort within the CAF force construct were explored, with emphasis on the role of intelligence as an enabler – but also on the constraints and restraints associated with its employment and the extant challenges. Common to all lines of effort is the presence of decisions – broad in scope, temporality, and impact. The nature of the various lines of effort and their inter-relationships with each other provides for complex interactions and outcomes. Understanding these interactions and their influence on potential outcomes is fundamental to effective decision-making, which in turn, is influenced by the range of information under consideration by the decision-maker(s). As established throughout the earlier portions of this section, the role of intelligence is both significant and influential across the lines of effort – predominantly as a source of information to enable decision-making. Intelligence informs the development, facilitates the generation, and enables the employment of the force, through the appreciation of the environment in which the force will operate as well as the capabilities and intentions of known and potential adversaries it may encounter. Given the complexities of many decisions prevalent within the defence domain, and the increasing demand to rationalize these decisions in a traceable, evidence-based fashion, efforts must be made to optimize the flow and analysis of information such that decisions can be rendered in a timely manner with confidence.

A noted academic in the field of decision-making (predominantly the subfield of *naturalistic decision making*), in their study of decision-making by firefighting

[126] Philip H. J. Davies, 'The Problem of Defence Intelligence', *Intelligence and National Security* 31, no. 6 (18 September 2016): 797–809, https://doi.org/10.1080/02684527.2015.1115234.
[127] Davies.
[128] Stephen Patrick Marrin, 'Intelligence Analysis and Decisionmaking: Proximity Matters' (Ph.D., United States -- Virginia, University of Virginia), accessed 26 February 2023, https://www.proquest.com/docview/305010888/abstract/215F1521A0FD4B55PQ/1.
[129] Pothoven, Rietjens, and de Werd, 'Producer-Client Paradigms for Defense Intelligence'.

commanders, Klein observes that “commanders relied on their abilities to recognize and appropriately classify a situation”[130] when making decisions on how to respond to a particular scenario, which served as a basis for their earlier identification of recognition-based decision-making – established to be equally applicable to military decision-makers.[131] While the study of decision-making remains long-standing and ongoing, there is a shift towards not only the decision-making of artificial intelligences[132] (exclusively machine-based) – but also of what is being referred to as *intelligence augmentation*, in which both human and machine competencies are integrated with one another in a collaborative fashion to enhance decision making.[133] Wren and Adya further offer that “rapidly evolving, high gain/loss events such as […] warfare should be treated as [a] special [case] of [decision making under stress]”[134] in their work exploring the role of information overload, temporal pressure, complexity and uncertainty in stressful decision making – and the role decision support aids or systems can play in mitigating the various stressors common to decision-making-under-stress scenarios. They make reference to the work of Janis, where they highlight the following found under the decision conflict theory they established, notably that “decision makers cope with stress by becoming hyper-vigilant in their search for information”[135].

While this was originally conceived back in 1977, where access to information was still relatively constrained (by today’s standards), it remains extant. As noted by Isselin in exploring the correlation between the quantity and quality of data and the outcome of decision-making, they note the influence of these characteristics on complexity and the compound effect on decision making, specifically that “[c]omplexity resulting from diverse quality and quantity of information is also found to lower decision accuracy and increase time to decision making.”[136] As the quantity of data continues to increase, the diversification of quality is likely to expand commensurately – especially in the absence of a rigorously implemented quality control regime, such as the framework proposed by Taleb, Sehrani and Dssouli in their survey on “Big Data Quality.”[137] The

[130] Gary A. Klein, ed., ‘A Recognition-Primed Decision (RPD) Model of Rapid Decision Making’, in *Decision Making in Action: Models and Methods* (Norwood, N.J: Ablex Pub, 1993).

[131] Gary Klein, ‘Naturalistic Decision Making’, *Human Factors* 50, no. 3 (1 June 2008): 456–60, https://doi.org/10.1518/001872008X288385.

[132] Employed in the cognitive context here

[133] Paul Souren et al., ‘Intelligence Augmentation: Human Factors in AI and Future of Work’, *AIS Transactions on Human-Computer Interactions* 14, no. 3 (September 2022): 426–45, https://doi.org/10.17705/1thci.00174.

[134] Gloria Phillips-Wren and Monica Adya, ‘Decision Making under Stress: The Role of Information Overload, Time Pressure, Complexity, and Uncertainty’, *Journal of Decision Systems* 29, no. sup1 (18 August 2020): 213–25, https://doi.org/10.1080/12460125.2020.1768680.

[135] Irving L Janis and Leon Mann, *Decision Making: A Psychological Analysis of Conflict, Choice, and Commitment.* (Free press, 1977).

[136] Errol R. Iselin, ‘The Effects of Information Load and Information Diversity on Decision Quality in a Structured Decision Task’, *Accounting, Organizations and Society* 13, no. 2 (1 January 1988): 147–64, https://doi.org/10.1016/0361-3682(88)90041-4.

[137] Ikbal Taleb, Mohamed Adel Serhani, and Rachida Dssouli, ‘Big Data Quality: A Survey’, in *2018 IEEE International Congress on Big Data (BigData Congress)*, 2018, 166–73, https://doi.org/10.1109/BigDataCongress.2018.00029.

inherent challenge is the pace at which data is generated and revised, acknowledged to greatly outpace the rate at which it can be moderated and curated in various studies.

However, these effects are almost certainly compounded in modern times when considering the amount and rate at which information is available to decision makers – hence the term "information overload,"[138] which can lead to the inability to actually make a decision, referred to as "analysis paralysis."[139] In a case study reviewing the design and development of landing craft for employment by the Allies in World War II, Roberts offers the following: "There is a common impulse that often impels those who are risk-averse to seek more from analysis than analysis is able to give—namely, the elimination of uncertainty."[140] As the demand for traceability and accountability within the decision-making processes of the Canadian Armed Forces, it is highly likely that the aforementioned quest for absolute certainty induces paralysis in the decision-making process—particularly in the case of force development and major capital acquisitions, such as the Ground-Based Air Defence,[141] Joint Support Ship,[142] and Future Fighter Capability[143] projects. In all of the aforementioned projects, several criticisms have been raised about the decisions rendered (or not) and often the argument is made that the pursuit of perceived perfection (frequently referred to as *Canadianization* – the imposition of changes to an existing design or build to satisfy Canadian-specific requirements, not all of which are explicitly related to military employment requirements) is to blame.[144]

[138] Phillips-Wren and Adya, 'Decision Making under Stress'.

[139] Ann Langley, 'Between "Paralysis by Analysis" and "Extinction by Instinct"', *Sloan Management Review* 36, no. 3 (Spring 1995): 63.

[140] Lon Roberts, 'Analysis Paralysis: A Case of Terminological Inexactitude', *Defence AT&L* January-February (2010), https://www.dau.edu/library/defense-atl/DATLFiles/Jan-Feb/robersts_jan-feb10.pdf.

[141] Murray Lee, 'We Have No Air Defence For Our Army – Why?', *RUSI(NS)* (blog), 24 January 2022, https://rusi-ns.ca/air-defence/; Lee Berthiaume, 'Canadian Army Waiting for Air-Defence Systems as Ottawa Buys Equipment for Ukraine', CTVNews, 11 January 2023, https://www.ctvnews.ca/politics/canadian-army-waiting-for-air-defence-systems-as-ottawa-buys-equipment-for-ukraine-1.6226657.

[142] Douglas Campbell, 'The Canadianization of the Joint Support Ship: From Mature Design to a Unique Canadian Solution', Canadian Global Affairs Institute, accessed 22 March 2023, https://www.cgai.ca/the_canadianization_of_the_joint_support_ship_from_mature_design_to_a_unique_canadian_solution; David Pugliese, 'New Navy Supply Ships Face More Delays and Cost Increases, Federal Officials Confirm', ottawacitizen, accessed 22 March 2023, https://ottawacitizen.com/news/national/defence-watch/new-navy-supply-ships-face-more-delays-and-cost-increases-federal-officials-confirm.

[143] Murray Brewster, 'ANALYSIS | A Tale of Two Fighter Jets — and What It Means for Canada's Defence and Place in the World | CBC News', CBC, 3 January 2022, https://www.cbc.ca/news/politics/canada-fighter-jets-defence-1.6296021.

[144] Berthiaume, 'Canadian Army Waiting for Air-Defence Systems as Ottawa Buys Equipment for Ukraine'; Pugliese, 'New Navy Supply Ships Face More Delays and Cost Increases, Federal Officials Confirm'; Brewster, 'ANALYSIS | A Tale of Two Fighter Jets — and What It Means for Canada's Defence and Place in the World | CBC News'.

PART III – MODELLING AND SIMULATION

As a Capability

One manner in which the capability of human decision-makers is supported is through the use of various simulations, ranging from singular entity-on-entity interactions (such as a defensive engagement exploring the interaction of a single gun-fired munition against a single threat missile) through to wargaming campaign level force-on-force engagements (such as those being employed to explore the current conflict in Ukraine[145] and predicting potential conflict-derived outcomes on and around the island of Taiwan[146]), enabled by the models which are employed within the simulations, representing various entities in a wide-ranging spectrum of scope and detail. Best captured by Rothenberg in their iconic work in the field of data quality (and the verification and validation thereof) "[t]he quality of any model is relative to its purpose,"[147] which tightly correlates with the now infamous quote by the famous statistician Box, "all models are wrong, but some are useful."[148] Together, these statements highlight the inter-relationship between the information employed in the creation of a model, and the manner in which it is employed. Just as a model with poor or erroneous information can deliver poor results when employed as intended, a model generated with the absolute best information can also deliver poor results if employed in a manner inconsistent with that for which it was created.

Contemporarily, the qualitative characterization of extent to which a model or simulation is representative of reality is referred to as *fidelity*. While there exist a plethora of definitions and interpretations of the term *fidelity*, one element of that proposed and endorsed by the Fidelity Implementation Study Group[149] is considered to be most applicable here. Specifically, the institution describes it (generalized) as "a measure of

[145] Jonathan Masters, 'Ukraine: Conflict at the Crossroads of Europe and Russia', Council on Foreign Relations, accessed 15 March 2023, https://www.cfr.org/backgrounder/ukraine-conflict-crossroads-europe-and-russia.
[146] Mark F. Cancian, Matthew Cancian, and Eric Heginbotham, 'The First Battle of the Next War: Wargaming a Chinese Invasion of Taiwan', 9 January 2023, https://www.csis.org/analysis/first-battle-next-war-wargaming-chinese-invasion-taiwan.
[147] Jeff Rothenberg, 'A Discussion of Data Quality for Verification, Validation, and Certification (VV&C) of Data to Be Used in Modeling' (RAND Corporation, 1997).
[148] George E. P. Box, 'Science and Statistics', *Journal of the American Statistical Association* 71, no. 356 (1 December 1976): 791–99, https://doi.org/10.1080/01621459.1976.10480949.
[149] The Fidelity Implementation Study Group (Fidelity ISG) has the objective of leveraging the current interest and excitement in describing, quantifying, and using simulation fidelity, particularly in the context of the HLA. Recognition of the importance of capability to characterize simulation fidelity has been growing in the SISO community for some time. At least five SIW forums (Analysis, T&E, RD&E, Logistics, VV&A), recommended the establishment of the Fidelity ISG to address a number of specific simulation fidelity issues which cut across the concerns of virtually all SISO forums. The ability to describe and quantify simulation fidelity appropriately will be essential for effective interoperability and support of endeavors such as Simulation Based Acquisition.

the realism of a model or simulation; faithfulness [to reality]."[150] Building from this, Roza et al expand further into applying the concept of fidelity to simulation requirements, offering that "[f]idelity requirements represent the level of realism the simulation must display in order to fulfil the user's needs and objectives,"[151] noting the influence of the fidelity of the models employed within the simulation on the fidelity of the simulation itself. Rothenberg details this in the following: "It is impossible to define the quality of a model without first defining its intended relationship to the reality that it models, where this relationship must be derived from the purpose for which the model is intended."[152] The concept of immersion continues to be explored by a range of academic, commercial and military interests, especially with the rise of augmented and virtual reality technologies. This has likely contributed to the the (arguably inevitable) demand for greater and greater levels of detail in the construction of models and the simulation environments in which they are employed.

However, increased fidelity typically comes at a cost, namely in the amount of data required to achieve it, and derived compromises in terms of storage and processing. As such, efforts are frequently invested in optimizing the level of fidelity, often biased towards the minimum level acceptable for the purpose in order to manage time, cost and complexity. Two popular techniques for managing fidelity requirements are approximation and/or abstraction. While both rely upon existing models, the former achieves optimization by foregoing accuracy and precision, and the latter seeks to preserve accuracy and precision while reducing the complexity of the model in pursuit of optimization.[153]

The Quality of Quantity

As it remains that all models will remain imperfect due to the presence of errors (as insignificant as they may be), largely derived from the current inability to capture and replicate reality to what could be considered a functionally infinite level of detail, quantity retains significant value within this domain. The concept of statistical distribution is leveraged frequently within modelling and simulation efforts as a means of compensating for the imperfect quality of any models and simulations currently employed, through the generation of statistically-relevant data derived predominantly by stochastic elements within the model.[154] Equally, it may also be leveraged for optimization purposes in cases where it may be more efficient from a computational

[150] David C Gross, 'Report from the Fidelity Implementation Study Group', 1999, https://www.sisostds.org/DesktopModules/Bring2mind/DMX/API/Entries/Download?Command=Core_Download&EntryId=32793&PortalId=0&TabId=105.

[151] Manfred Roza et al., 'Fidelity Requirements Specification: A Process Oriented View', n.d.

[152] Rothenberg, 'A Discussion of Data Quality for Verification, Validation, and Certification (VV&C) of Data to Be Used in Modeling'.

[153] Frederick K Frantz and A John Ellor, 'Model Abstraction Techniques', Scientific and Technical Report - Final (New York: United States Air Force Materiel Command, Rome Laboratory, August 1996), https://apps-dtic-mil.cfc.idm.oclc.org/sti/pdfs/ADA319039.pdf.

[154] J.S. Carson, 'Introduction to Modeling and Simulation', in *Proceedings of the Winter Simulation Conference, 2005.*, 2005, 8 pp.-, https://doi.org/10.1109/WSC.2005.1574235.

processing perspective to preference quantity (in terms of number of simulation runs) over quality (of the models and simulation environment under consideration).

One particular strategy often employed is referred to as a sensitivity analysis – a process in which one or more elements of a model are deliberately adjusted over a range in order to review the influence on the simulation outcome.[155] This can be leveraged for a myriad of reasons, such as verifying and validating a model or exploring possibilities for values in cases of unknown or uncertain elements within the model. In such cases, the elements subject to investigation and the manner in which they should be investigated are influenced by a variety of bounding constraints, some imposed artificially – such as human intent, while others such as the laws of physics understood, are considered universal. Of course, in both cases there exists a universal caveat – the constraints are only as effective as they are currently understood.[156] This latter application is of significant interest within this paper, as a potential avenue towards providing an alternative source for information about a (potential) adversary, in the sense that for select cases, it could be reasonably assumed that a particular parametric value or insight was derived from such an activity – vice a deliberate intelligence acquisition effort. Consider the aerodynamic performance of a adversarial missile that had been displayed publicly or the line of advance under consideration for an adversarial military action – both of these could be informed by sensitive intelligence activities, but what if it could also be established that the specifics considered by a military force could have been determined to be *most likely* (and thus weighted appropriately in a decision-making process) as the outcome of a sensitivity analysis executed by a simulation of sufficient fidelity?

Across the military, due to the range of activities in which modelling and simulation is currently, or likely to be employed, the requisite level of fidelity is dynamic, commensurate with the specific activity. However, that is not to say that this creates an insurmountable issue – one where in the absence of a singular standard, no standard is achievable. Rather, the case could be made that a unified, central repository for all information *contributing* to fidelity, capable of being adapted and applied *dynamically* to specific model and simulation-related requirements (and potentially even scaled to account for sensitivity?), could be of great benefit across the institution. The unification and centralization of all information into a single source could facilitate reconciliation, verification, validation, and accreditation efforts – especially when multiple applications

[155] Raymond J Madachy and Daniel Houston, *What Every Engineer Should Know About Modeling and Simulation* (CRC Press, 2017), chaps 2, 4, https://books.google.ca/books?hl=en&lr=&id=fDwPEAAAQBAJ&oi=fnd&pg=PP1&dq=modelling+and+simulation+statistics&ots=hFd7P0lc6y&sig=YoW4fKgW9oZHyt9_yvm4bnmEFaM&redir_esc=y#v=onepage&q=modelling%20and%20simulation%20statistics&f=false.
[156] Research and Engineering, 'DEM&S Glossary – DCTO(MC)'; Andreas Tolk, *Engineering Principles of Combat Modeling and Distributed Simulation*, Book, Whole (Hoboken: Wiley, 2012); Science and Technology Organization, 'Guidelines for Modelling and Simulation (M&S) Use Risk Identification, Analysis, and Mitigation' (North Atlantic Treaty Organization, September 2021), https://apps.dtic.mil/sti/pdfs/AD1183690.pdf.

exist with differing degrees of fidelity requirements, as is common to many complex military procurement activities.

Conversely, the aggregation of information poses its own challenges, namely the increase of risk derived from the impact of inadvertent or malicious access – the proverbial *many eggs in one basket* scenario. Consider now the pretext under which this risk is characterized – specifically in the distribution or density of the sensitive data (relative to the whole). If the notion of aggregation increasing the risk is entertained, it is done so acknowledging the qualitative element of *quantity* – specifically in the sense that if the density of sensitive information increases past a certain point within a data set, then an elevation in sensitivity is created (or at least, considered). This will be re-visited in the next section where it will be proposed that an opposing condition could be leveraged for benefit.

PART IV – OPPORTUNITIES FOR OPTIMIZATION

Unified Consolidation – "One Stop Shopping"

In their work exploring the application of ontology to modelling and simulation – specifically when employed in the development of a product, Ball and Runge observe that "[t]he abundance and constant growth of information […] has driven companies to invest in large enterprise […] systems in which to store and provide repository services for engineering data."[157] From their perspective on ontological relationships – focusing on the interrelationships between individual elements of data, they suggest that while the establishment of these interrelationships is often influenced heavily at the domain level, once established, these interrelationships enable the identification and exploitation of what they refer to as "informational intersections,"[158] which may transcend the traditional boundaries common to multi-disciplinary efforts. Given the breadth of scope of intelligence in the military domain, it can be considered to satisfy the criteria of a multi-disciplinary effort. Equally though, a shortfall common (but not exclusively) to military intelligence is that of *stovepiping* or *siloing* – where the dissemination of information is constrained to a small subset of the larger community, and therefore many subsets may be naive to the information held by others. This hinders the effective correlation of information across these functional domains or silos of expertise. One method employed within the Canadian construct is the employment of *all-source* analysts, which, as their name suggests, are tasked with conducting analyses across the spectrum of information sources. However, functional constraints (both individual and organizational capacity limitations) result in partial success, as many of these analysts focus their efforts in a relatively narrow (but still broad, comparatively speaking) scope.

[157] George L. Ball and Christopher (Kit) Runge, 'Producing Reusable Engineered Systems through Ontology: Implementing an Information Sciences Approach to Architecture-Driven, Model-Based, Concurrent Engineering', *The Journal of Defense Modeling and Simulation* 11, no. 3 (1 July 2014): 219–26, https://doi.org/10.1177/1548512913502259.
[158] Ball and Runge.

Under a construct in which all intelligence is consolidated within a singular repository (vice the segregation that is much more common), it is almost certain that the data set arising from such would fit the definition of *big data*, in that it would be: large in *volume*, high in *velocity* and *resolution* (in the global sense, acknowledging that localized velocities are likely to be dynamic over time, and resolutions varied), vast in both *variety* and *scope*, significant in inter-*relatability* (as a core element of the analysis of intelligence is the *correlation* of separate, often diverse elements of information), and able to be scaled and extended in a *flexible* fashion. Of specific note, the ability to correlate information within the current environment is dependent upon knowledge of the various elements of information subject to possible correlation and where they reside – something that can be especially challenging when the elements do not reside within the same repository, a situation common to the Canadian Armed Forces. In many cases, it could be offered that some instances of correlation are only achievable due to the underlying knowledge of various information repositories held by the individual analyst working across them. This creates an element of institutional risk, where there may not exist a formalized mechanic to identify and track the various elements of information across these repositories and should an individual bearing specific knowledge of overlapping information become unavailable (and they are the sole possessor of this knowledge), this knowledge may be functionally lost—at least until re-discovered by another analyst. Consolidation of all information under a unified, curated repository could serve to reduce this specific risk.

Consider the Directorate of Scientific and Technical Intelligence within CFINTCOM, for which one of their mandates is the provision of all-source intelligence assessments on adversarial military (technical) capabilities.[159] This mandate is satisfied through the provision of personnel from the Air, Land and Maritime elements who bring with them a wide range of knowledge and experience – but not necessarily in the analysis of intelligence. This unit is well-positioned (functionally) to fulfil this mandate with a wide range of connections and accesses. However, it is less so in terms of overall resources, with *entire domains* covered by relatively few individuals (the average number as of 2022 was approximately four personnel per domain)[160] – many of whom, by virtue of being military members, are only expected to serve in this role for a very limited period, and likely never returning as they pursue other opportunities for professional development and experience. This directorate is the *de facto* centralized repository under the current construct – solely by virtue of the individuals working within possessing the appropriate knowledge of the various sources and repositories for this type of information, responsible for liaising with numerous entities spread across the three lines of effort, endeavouring to ensure they are kept apprised of developments, and providing corrected information to senior decision-makers in instances of the delivery of inaccurate and/or obsolete information by others. Given the functional constraints imposed under this construct, it should be appreciated the impact of inefficiencies, such as the monitoring of multiple disparate sources and repositories of information – and the

[159] Defence, ‘Canadian Forces Intelligence Command’.
[160] Anecdotal, based upon the total number of personnel expected to be posted into the Directorate at the time of the author’s departure.

reconciliation thereof, followed by the expectation to disseminate pertinent (*highly* subjective to the recipient) information across a number of different channels to parties of (varying) interest in a timely and responsive manner in the execution of their duties.

One of the challenges is that this Directorate's existence is relatively unknown to the general population of the department due to its size and limited interaction with the broader population, and it is not uncommon for analysts external to CFINTCOM to remain unaware for extended periods of time. In such cases, these analysts will often defer to their immediate colleagues and supervisors (who may also be unaware) when seeking out information and sources for their own efforts. While this can be considered an institutional issue that could be (and does get) resolved through improved management practices, it could be surmounted altogether if there was a singular repository where any analyst (old or new) could go to seek out information of interest, with the confidence that it provided access to the vast majority of information (deferring to the sensitivities for select topics that warrant additional protection), that it was properly curated (readily searchable and cross-referenced), and reflected the most recent developments (to the extent achievable, practically).

Ideally, such a repository would not necessarily contain the entire body of information within the intelligence domain (effectively replicating everything generated and received locally). Rather, it would likely be a hybridized combination of storage (for internally generated and held information) and connectivity (for externally generated and held information). The physical storage itself could be centralized into a single location, or alternatively, distributed across a range of locations. The networking elements could leverage already existing infrastructure – but could do so on a greater scale, attaining the elevated security of information demanded of such through the use of modern encryption applications and processing techniques. This approach could mitigate the infrastructure challenges associated with common storage and networking overhead costs (frequently duplicated when one considers the requirements common to an individual network), emulating many current *cloud*-based data management systems offered and employed by major enterprises.[161]

However, current policy dictates that the classification of any body of information shall be at the level of the highest classification of information contained within, commensurate with the expectation to exercise due diligence in considering the risk posed by the possibility of inadvertent disclosure (independent of likelihood).[162] Thus, under this directive, as soon as any *singular* element of information bearing a higher sensitivity is incorporated into a data set, the entire data set now bears that elevated sensitivity under the assumption that if unauthorized access is gained in part, it is gained

[161] Amazon, 'What Is Cloud Storage? - Cloud Storage Explained - AWS', Amazon Web Services, Inc., accessed 23 March 2023, https://aws.amazon.com/what-is/cloud-storage/; Google, 'What Is Cloud Storage & How Does It Work?', Google Cloud, accessed 23 March 2023, https://cloud.google.com/learn/what-is-cloud-storage; IBM, 'What Is Cloud Storage? | IBM', accessed 23 March 2023, https://www.ibm.com/topics/cloud-storage.

[162] Defence, 'NDSOD', chap. 6; Defence, 'DAOD 2006-0, Defence Security'; Secretariat, 'Directive on Security Management'.

in functional entirety. Therefore, any such repository will bear the highest sensitivity of any *one* element contained within—notwithstanding the aggregation clause, under which a higher sensitivity may be assigned to a body of information containing a large amount of information at a lower sensitivity level.[163] It can be argued that this particular element of policy contributes significantly to the conservative approach employed in managing the risks associated with sensitive information. Therefore, a potential question that could be posed is: Independent of any metadata[164] and access controls,[165] in terms of the amount of data and distribution of sensitivities across a given quantity, when can a case be made that the risk of attribution for each individual element of information is *reduced* by virtue of a sufficiently large-sized *amount* of data, with a sufficiently *small* concentration of data assigned an elevated sensitivity? Noting the aforementioned exclusion of metadata, there would remain a requirement to maintain some means of retaining the contextual information to support credibility management efforts. However, this could be implemented under a suitably established information management construct. Equally, the exclusion of access controls simplifies the original consideration, as these mechanisms are already frequently employed to reduce the risk of exposure and have been discussed previously (recall the relevant discussion in Part I).

Managing Attribution – "Laundering Data"

As discussed previously, one of the key challenges encountered in seeking to leverage information derived from sensitive intelligence sources and methods is managing the risk associated with the attribution of the information to these sources and methods. Perhaps one of the most appropriate, contemporary examples of managing attribution risk is the criminal activity colloquially known as *money laundering*. The United Nations' Office on Drugs and Crime (UNODC) monitors a wide range of illegal and illicit activities, one of which is money laundering. The current description provided by this office is drawn from the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, established under the UN Vienna Protocol of 1988, as "the conversion or transfer of property, knowing that such property is derived from any offense(s), for the purpose of *concealing or disguising* the illicit *origin* of the property."[emphasis added throughout][166] In the modern context, criminals have been known to "leverage both the legitimate and illegitimate economies to disguise their financial transactions"[167] with the intended purpose of "making it impossible to

[163] Defence, 'NDSOD', chaps 3, 6, 7.

[164] Metadata is information which provides context to individual elements of data, is scalable (can apply to a single value, or a large database containing a large amount of values), and can be dynamic.

[165] R.S. Sandhu and P. Samarati, 'Access Control: Principle and Practice', *IEEE Communications Magazine* 32, no. 9 (September 1994): 40–48, https://doi.org/10.1109/35.312842.

[166] United Nations, 'United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances' (United Nations, 1988), https://www.unodc.org/pdf/convention_1988_en.pdf; United Nations, 'Money Laundering', United Nations: Office on Drugs and Crime, accessed 14 March 2023, https://www.unodc.org/unodc/en/money-laundering/overview.html.

[167] Ola M. Tucker, *The Flow of Illicit Funds: A Case Study Approach to Anti-Money Laundering Compliance* (Washington, UNITED STATES: Georgetown University Press, 2022), 8, http://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/detail.action?docID=29276966.

distinguish between their licit and illicit funds."[168] The effect of this is the challenge in quantifying the scope and magnitude of this activity, though the global estimate of money laundered in one year is often cited as "2 - 5% [*sic*] of global GDP, or $800 billion - $2 trillion in current US dollars" per the UNODC,[169] comparable to "national economies in magnitude."[170]

Functionally, the laundering is accomplished across three commonly-accepted phases: *Placement* - the introduction of the *illicit* funds into the financial system; *Layering* – the employment of multiple (often complex and convoluted) transactions involving the illicit funds, intended to complicate identification of and attribution to the source; and *Integration* – the legitimization of the funds by (falsely) attributing their origin to *licit* sources. The complexity of the effort (and thus, the commensurate difficulty in determining the origin) can be increased by repeating the cycle (in whole, or in part), or interleaving multiple different cycles with one another. Tucker explains one tenet to the ongoing success of this activity is that those employing it is that they "critically, and perhaps most importantly […] understand the value of anonymity"[171] which, contextually, translates to managing the attribution of illicit funds to the point of origin (or source) by external and/or undesired parties through obfuscation.

Equally important to the successful employment of this technique is the ability to delineate between the legitimate and illegitimate funds. This is often accomplished through the maintenance of two separate ledger documents – one aggregating both funds in a homogeneous manner (that which is overt or public-facing), and another which explicitly delineates between the two (that which is covert or kept confidential – often referred to as the *full* ledger). This latter ledger need not directly link the illicit funds with their true origin – just that from which they originated prior to entering the system being recorded in the particular ledger. Rather, it need only enable the accounting of the separate streams of funds.[172] Ultimately, while there will exist the potential to link the illicit funds to the origin, the ability to do so is highly reliant on the commensurate ability to trace the attribution – something which is typically only possible with the *full* ledger(s).

Given the requirement to leverage legitimate income sources in the *layering* process (often in the form of high-traffic and cash-flow businesses heavily reliant on physical currency), much of this can be considered to transpire in (relatively speaking) full view of the public. While the introduction of cryptocurrencies is almost certainly of interest to those interested in laundering funds due to the anonymity offered as well as a

[168] Tucker, 8.
[169] United Nations, 'Money Laundering'.
[170] Benjámin Villányi, 'Money Laundering: History, Regulations, and Techniques', Oxford Research Encyclopedia of Criminology and Criminal Justice, 26 April 2021, https://doi.org/10.1093/acrefore/9780190264079.013.708.
[171] Tucker, *The Flow of Illicit Funds*, 8.
[172] Ai Sar, 'The History Of Money Laundering And It's Origins', financialcrimesacademy.org, 18 January 2023, https://financialcrimeacademy.org/the-history-of-money-laundering-and-its-origins/; James Chen, 'Money Laundering: What It Is and How to Prevent It', Investopedia, 29 June 2022, https://www.investopedia.com/terms/m/moneylaundering.asp.

lack of rigid regulation and oversight (both of which are hindered by the lack of understanding of their functionality by those responsible for these elements), it is expected that more traditional forms of currency will remain prevalent until cryptocurrencies supplant them and appropriate infrastructure exists to facilitate their employment for licit purposes.[173]

From the discussion above on money laundering, one might consider how a similar approach could be employed to manage the attribution risk associated with information derived from intelligence – specifically in obfuscating the origin of the information. Currently, the sensitivity assigned to the information is directly related to that of the origin, whether it is the source(s) and/or method(s). If multiple sources exist – especially if at least one is of a lower sensitivity (and arguably a more likely source), then a case can be made that the attribution risk is mitigatable by the challenge posed in attributing the specific information directly to a *specific* origin – thereby reducing the risk of exposure of the more sensitive source or method. As an example, consider a piece of information derived from sensitive intelligence origins which subsequently becomes available in the public domain. From a *plausibility* perspective, it is *reasonable* to assume that anyone possessing the information *after* the point in time where it became available publicly, *likely* acquired the information from the public source. Much like a business owner running a legitimate business which is employed to facilitate the laundering of money – creating a *plausible* source for the income alleged to have originated from within. In both cases, care must be taken to avoid creating a situation that raises doubt by reducing the coherency between the output (*funds*, in the case of money laundering; *information*, in the case of intelligence) and the proposed source.

Now, consider the change in *scope* of data sets in the modern age. Previously, the amount of information possessed or accessible by an individual was relatively limited. With the ever-increasing expansion of digital capabilities – specifically storage and processing, the amount of information available to (and the rate at which it can be accessed by) any one individual continues to expand geometrically. Building upon the earlier work of many notable academics across a range of fields pertaining to the generation, processing, analysis, storage, and consumption of data, Kitchin consolidates the following characteristics to describe sufficiently large datasets, what is colloquially referred to as *big data*: *volume* – typically measured in tera or petabytes[174]; *velocity* – specifically that it is created in or near real-time; *variety* – often diverse, appearing in both structured and unstructured forms; *scope* – typically characterized as 'exhaustive'; *resolution* – often qualified as fine-grained and as detailed as possible; *relationality* – specifically in that various elements are able to be related to one another; and *flexibility* –

[173] United Nations, 'Money Laundering'; Villányi, 'Money Laundering'; Chen, 'Money Laundering'.
[174] A *byte* is defined as a grouping of eight binary *bits*, and is typically considered to be the smallest form of functional data, in the sense that a single byte can be used to represent a single ASCII character, such as a letter or number; The prefix t*era* denotes a factor of 10^{12}, and *peta* a factor of 10^{15}. In the digital realm, the conversion is approximated, noting that the actual scaling is by a factor of 1,024 (ie. A *petabyte* contains 1,024 *terabytes*), and not 1,000. According to Teradata.com, 1 *petabyte* is roughly equivalent to "500 billion pages of standard text", www.teradata.com/glossary/What-is-a-Petabyte, accessed 20 March 2023.

in that the data can be readily extended and scaled.[175] However, the human mind is still constrained in terms of *processing* the information presented to it (and by extension, *analyzing* it), and therefore it can be offered that as the *amount* of data available to an individual increases, their ability to process it does not increase commensurately,[176] emphasized by the defining traits presented above. Challenges in analyzing such data sets arise from these traits and the manner in which they increase the complexity of the analytical process (individually and in conjunction with others), specifically in the "abundance, exhaustivity and variety, timeliness and dynamism, messiness and uncertainty, [and] high relationality,"[177] further compounded by the increasingly common trait where the data may be collected with "no specific question in mind or is a by-product of another activity."[178]

If such challenges exist for the analysis of information collected by an entity, these same challenges are almost certainly applicable to an adversarial entity seeking to review such a body of information for the purposes of counter-intelligence—presuming they are able to obtain access in the first place, let alone persist for a sufficient amount of time to analyze the information contained and/or extract it. The subsequent question becomes whether or not these challenges could be leveraged in support of amending the current policy on the classification of information – specifically the requirement to assign a level of protection to a body of information commensurate with the *highest* level of any *singular* element. If the data contained within a repository has been functionally de-linked from that which influences the sensitivity the greatest, could it not be employed as an element within a larger dataset in a broader application – such as those common to modelling and simulation efforts, without incurring the constraints of elevated sensitivities, a proverbial needle in a pile of (less sensitive) needles?

Conflicting Requirements – Irreconcilable Differences?

Earlier discussions highlighted that attribution (in the form of *traceability*) is a consideration common to both intelligence as well as modelling and simulation efforts, as a mechanism for managing risk.[179] In the case of intelligence, it is leveraged to assess the credibility of the information under consideration. Likewise, in the case of modelling and simulation, it enables the verification, validation, and accreditation efforts.[180]

Equally, as the amount of data increases across the spectrum of employment, so to does the requirement to analyze, transport and store it (to varying extents) in order to

[175] Rob Kitchin, 'Big Data and Human Geography: Opportunities, Challenges and Risks', *Dialogues in Human Geography* 3, no. 3 (1 November 2013): 262–67, https://doi.org/10.1177/2043820613513388.

[176] Philipp Korherr and Dominik Kanbach, 'Human-Related Capabilities in Big Data Analytics: A Taxonomy of Human Factors with Impact on Firm Performance', *Review of Managerial Science*, 28 November 2021, https://doi.org/10.1007/s11846-021-00506-4.

[177] Rob Kitchin, 'Big Data, New Epistemologies and Paradigm Shifts', *Big Data & Society* 1, no. 1 (1 April 2014): 2053951714528481, https://doi.org/10.1177/2053951714528481.

[178] Kitchin.

[179] National Defense, 'CFJP 2-0'.

[180] Dale K Pace, 'Modeling and Simulation Verification and Validation Challenges', *JOHNS HOPKINS APL TECHNICAL DIGEST* 25, no. 2 (2004).

leverage it for advantage. This can create challenges in reconciling the desire to centralize against the costs incurred to do so. As mentioned previously, these challenges are exacerbated when considering the range of sensitivities and disparate systems on which this information is not only intended (by virtue of a supported requirement and supporting capability), but also *desired* to reside. In many cases, there exists a proverbial gap between information held by a military force, and the ability to employ it to greatest operational effect, without unduly jeopardizing the ability to acquire (and thus, exploit) similar information in the future.

During a panel discussion on the US Army's *Project Convergence 20* (one of their multi-domain operation experiments, this one focused on interconnectivity), hosted by the Center for Strategic and International Studies, Lieutenant General James Richardson – the head of the program, stated that one of the key findings was that "the network was the backbone, […] the center of gravity"[181] referring to the criticality of this capability in not only enabling future operations – but being critical to the *ability to operate*. As ought to be expected, as global militaries seek to leverage digital technologies in pursuit of military advantage, there is a commensurate effort in seeking to deny potential adversaries the same. Thus, many modern militaries account for this in their planning, specifically in considering denied, degraded, intermittent, and limited communications environments, describing the functional qualitative state of any communication links established in support of operations—all of which impose challenges on the data-intense operational environment.

One of the core issues concerning policy and decision makers surrounding the employment of artificial intelligence and machine-learning constructs in the military environment is *explainability*. Functionally, this is the ability to map the process and trace the information employed in decision-making by these systems. In their article exploring the technical and ethical dimensions of this tenet, McDermid et al offer "[t]he use of critical [machine learning]-based systems to assist or to replace the human decision-maker raises many questions about when, and whether, we should trust them."[182] Amplifying this statement, there exists a plethora of critical research and publications on the extant deficiencies in artificial intelligence and machine learning implementations, as observed in 2020 by Lieutenant Colonel (Retired) Paul Maxwell, the Cyber Fellow of Computer Engineering and associate professor at the Army Cyber Institute at the United States Military Academy, who highlights a few sub-elements affecting the current inability of these systems to explain their decisions, specifically that these systems "struggle to distinguish between correlation and causation"[183] and their poor ability to understand the contextual (sub)elements of the inputs they are

[181] 'Project Convergence: An Experiment for Multidomain Operations', 16 February 2022, https://www.csis.org/analysis/project-convergence-experiment-multidomain-operations.

[182] John A. McDermid et al., 'Artificial Intelligence Explainability: The Technical and Ethical Dimensions', *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 379, no. 2207 (16 August 2021): 20200363, https://doi.org/10.1098/rsta.2020.0363.

[183] Paul Maxwell, 'Artificial Intelligence Is the Future of Warfare (Just Not in the Way You Think)', Modern War Institute, 20 April 2020, https://mwi.usma.edu/artificial-intelligence-future-warfare-just-not-way-think/.

provided.[184] The iterative development cycle associated with these systems increases the complexity of the matter, exacerbating the extant concerns surrounding the desired assurances pertaining to repeatability and reproducibility.[185]

PART VI – CONCLUSION

As the scope, depth and availability of information continues to grow, it stands to reason that those relying upon it in their endeavours will continue to pursue opportunities to improve their ability to leverage information in pursuit of their interests—especially when those interests involve nations vying for power on the global stage. The military retains a position of prominence within the arsenal of established nation states, by virtue of the reason for which they exist – to visit violence upon those who would threaten the interests of the entity they serve (or at least establish the threat thereof). The establishment of the threat is predicated upon the perceived ability to deliver on the threat, and as established by many notable scholars, information is a key factor to the effective application of force by a military. The military intelligence apparatus is the avenue from which this information is collected and analyzed in order to enable the aforementioned application of force.

Summary of Findings

> *In today's information age, the old closed-loop system of intelligence, especially that which is over-classified, is rapidly becoming irrelevant.*
>
> – Flynn and Flynn*, Integrating Intelligence and Information*

This paper sought to explore the current role of military intelligence within the three lines of effort within the Canadian Armed Forces, emphasizing the critical analysis of how the intelligence effort is integrated within these lines of effort, and equally, areas and manners in which opportunities for improvement may reside. Across the three lines of effort, it can be deduced that there are multiple areas in which greater benefit could be achieved. A common element emergent from the analyses is the blurring of boundaries between information technology, operational technology and platform technology – specifically that the difficulty in defining these boundaries is complicated by "continuous advancements in technologies and many defence capabilities being enabled by technologies that span the boundaries between [information technology], [operational technology] and [platform technology]."[186] This is likely to be exacerbated by the continued pursuit of opportunities to increase overall effectiveness and efficiencies through the integration of increasingly-capable (and complex) digital technologies. Outlined below are three recommendations derived from the findings of this project. These recommendations are not intended to be fulsome nor all-encompassing, and while

[184] Maxwell.

[185] McDermid et al., 'Artificial Intelligence Explainability'.

[186] Defence, 'DAOD 6002-0, Information Technology', sec. 3.6.

there are specific elements within, they are provided as generalized concepts – vice prescriptive dictations.

Recommendation A – Unification and Consolidation of Information Management and Technologies involved with Intelligence

In order to support consolidation of information into a universal repository, an appropriate framework to support such must exist. Currently, knowledge and information derived from intelligence is often fragmented across a variety of networks and repositories as the current risk management strategies within the CAF (and many other nations) often drive the decision to segregate networks based upon the assessed level of sensitivity necessary to *reasonably* support the function. Acknowledging that while a case almost always exists to suggest that improved effectiveness is available from increased access to information, the commensurate increase in risk is not necessarily outweighed by the potential benefits. However, what is not necessarily captured under this construct is the elevated risk associated with a lack of coherency among the various repositories, and the additional effort required on behalf of individual personnel to assess the validity of and track access to the information within each of the repositories.

In their essay exploring how *big* data differs from the conventional understanding of data, Davenport, Barth and Bean discuss the requirement to enhance focus on information technology, as it becomes increasingly important in enabling the employment of larger data sets, where the focus is no longer exclusive to the individual stock of elements of data, but shifting towards the *flow* of information – specifically the manner in which it changes and the patterns that emerge over time and across these changes.[187] In order to permit this, there must exist an ability to track the information throughout its lifecycle in a coherent fashion – something extremely challenging under the current construct, where data is replicated across networks and repositories in a predominantly manual, and not necessarily coherent (in time, detail or quality) fashion. A unified information technology implementation, supported by a robust information management policy could offer enhanced opportunities for collaboration and analysis, with the additional benefit of potentially reducing the amount of duplication in physical assets like workstations and storage. However, current policy and risk mitigation measures preclude such an approach and will be discussed further in a later recommendation.

Recommendation B – Enhanced Integration of Intelligence into Defence M&S Efforts

Currently, while Intelligence is incorporated within extant modelling and simulation efforts, it is often at a distance and in a non-coherent fashion, typically constituting the discrete provision of information to another entity – or direction to an appropriate source. As established at various points throughout, there exists rationale to

[187] Thomas H. Davenport, Paul Barth, and Randy Bean, 'How Big Data Is Different', *MIT Sloan Management Review* 54, no. 1 (Fall 2012): 43–46.

promote a more fulsome incorporation of the intelligence apparatus into defence modelling and simulation efforts. Within force development, such integration could facilitate the establishment of more robust, defensible requirements in a more time-sensitive and dynamic fashion. Likewise, similar integration could be leveraged within force generation to improve training outcomes at the individual and collective levels by enhancing immersion, improving uptake by individuals through the provision of models and environments that are further representative of reality – and thus, less likely to be challenged.

Equally, and perhaps most prominently, force employment potentially offers the greatest amount of opportunity, some of which could be argued to be a matter of necessity in light of the evolving nature of the threat environment. The rate at which innovations emerge, and subsequently are assessed for and later incorporated within the defence domain continues to increase, and it can be offered that this rate has in many cases approached (and in others, exceeded) the limits of current human capacities. Thus, efficiencies facilitating the appreciation and analysis of these innovations and developments—and their implications to the threats potentially faced by the Canadian Armed Forces, should be sought out in order to ensure the viability of the military's ability to operate.

One key element common to all three lines of effort is *time* – both from the perspective of the time available to leverage an advantage for gain, and that available to respond when others likewise leverage their own advantages, all in the interests of improving the likelihood of desirable (or favourable, as a minimum) outcomes. Emerging from this principle is the prolific efforts invested in pursuing temporal efficiencies—such as the continued development of modelling and simulation. The employment of modelling and simulation, enabled by the ever-increasing capabilities offered within the digital realm, is not new to the military apparatus, though it does remain hindered by the perceived implications to liability and accountability in some areas – especially ones where human lives are at stake.

Recommendation C – Review of Extant Policy and Risk Management Procedures

Before delving into this recommendation, consider that the presence of a sensitive space within a building does not necessarily necessitate that the entire building adopts the highest-level of sensitivity of the information contained within. If access controls (ranging from physical site and workstation, to physical and logical network accesses) are robust and implemented effectively, then (at least under ideal circumstances) a user will only have the ability to access that which they are intended to. Returning back to the risk of inadvertent exposure, if an individual can be precluded from accessing information in a digital repository using access controls, can this not be considered analogous to comparable physical measures, akin to restricting access to physical spaces in which comparable information is stored in a physical medium?

Ultimately, in the modern age information security is reliant upon the fulsome integration of both the physical and the digital realms, where protecting the digital access to information is as important as protecting the physical assets on which the digital information is stored. Till offers that "[i]dentity is the core of security, both cyber and physical, but managing it is very complex,"[188] and it is from this complexity that risk aversion will likely continue to emanate, hindering the implementation of the proposed unified consolidation of intelligence information. While beyond the scope of this paper, it is worth noting that the CAF *still does not operate a centralized identity management system for its personnel*. The identity of the individual remains fixed to their physical identification card, which is not even recognized as a suitable form of identification for boarding a commercial aircraft anymore. A posting to a new geographical location requires the establishment of a functionally new (but typically identical) network identity. Perhaps once the CAF resolves its issues in managing the identities of their personnel, the current perception of risk derived from the potential for an individual to inadvertently or unintentionally access sensitive information can be revisited.

Future Research

While several proposed recommendations have been made – each of which includes a variety of potential branches that could be explored in future work, the variety and scope of potential recommendations in this domain greatly exceed that which could be reasonably considered in this work. In their article exploring the changes of the intelligence community following 9/11, Clapper offers that "the tangible benefits of vertical and horizontal integration are indisputable,"[189] and this is espoused among the recommendations that were made herein. However, there exists a significant amount of potential to be explored further in the overall integration of the intelligence effort across a wide range of entities and groupings, from ensuring that the solider on the ground has ready access to near-real time intelligence derived from strategic assets, to ensuring that the efforts of multiple nations are further enhanced and optimized in a more fulsome manner (assuming the requisite level of trust can be established).

Equally, the role of modelling and simulation continues to be explored, and as new innovations emerge, so to do further opportunities to review and refine the manner in which it is employed in the military domain.

Finally, the community stands to benefit from additional research into the policy framework surrounding the intelligence effort. This is potentially one of the most challenging aspects for review and critique due to the sensitivities and associated risks—arguably, some of the *most* sensitive within a nation, compounded by the engagement in the practice of intelligence with partners and allies, adding an additional layer of complexity (the maintenance of relations). However, that should not dissuade such an investigation. In an age of growing disparity in terms of risk tolerance, it can be offered that the imperative to shift away from extant risk averse stance continues to grow – and in some cases it has, as evidenced by the continued disclosure of information derived from

[188] Steve Van Till, 'The Convergence of the Physical and Digital Security Worlds', Security Info Watch, 14 July 2021, https://www.securityinfowatch.com/access-identity/article/21227403/the-convergence-of-the-physical-and-digital-security-worlds.

[189] Clapper, 'How 9/11 Transformed the Intelligence Community; It's No Longer about "need to Know." Our Guiding Principle Is "Responsibility to Share."'

traditionally sensitive intelligence sources in support of Ukraine. Perhaps the issue is not that the community itself is hesitant, but rather that those establishing policy have yet to truly appreciate the realities of the modern intelligence environment (and by extension, the environment in which the military will be expected to operate). Equally, there exists opportunity to revisit the enduring perception and understanding of the risks and current mitigation measures in effect, possibly establishing a new characterization of the risks prevalent—and the availability of the means to mitigate them.

Concluding Thoughts

In order to retain the ability to contribute to global stability abroad and defense of its sovereignty at home, the Canadian Armed Forces must remain (some would argue it must first be regained…) a credible threat to those who would seek to challenge the ideologies of the Canada and its partners/allies, for this is the role of a military within a nation's policy endeavours. The effectiveness of a nation's military is dependent upon a large number of factors, typically grouped under three lines of effort: the ability to develop the force, the ability to generate the force as developed, and the ability to employ it. Contingent to all of these efforts is the role of information, much of which is derived from intelligence (especially as it pertains to adversarial capabilities and intent) and thus, it can be offered that the role of the intelligence effort is crucial to enabling the establishment and employment of an effective fighting force.

Reaching back to a White Paper on Defence from 1964, the authors state: "One cannot be a member of a military alliance and at the same time avoid some share of responsibility for its strategic policies."[190] While they were speaking to the role of Canada as a non-nuclear middle-power within the broader alliance of nuclear nations at the time, this concept can be mapped to the modern day and the extant alliances and partnerships within the sphere of military intelligence. Given the increased role of intelligence in the modern world – both in anticipating and reacting to adversarial actions, and the resource-constraints extant within the Canadian military and intelligence apparatuses, Canada can not afford to fall astern of our partners and allies and thus, should review opportunities to enhance its ability to not only consume the intelligence generated by others—but become a key contributor to the overall effort.

This paper sought to explore opportunities to do so by investigating the current implementation of intelligence within the Canadian Defence effort, with additional focus on the three lines of military effort within CAF doctrine. Further, modelling and simulation within the defence domain was explored, seeking out potential avenues to improving the integration of intelligence with these lines of effort. Finally, three recommendations were proposed in support of enhancing this integration, with a thematic focus on exploring the opportunities afforded through modelling and simulation –

[190] Paul Hellyer and Lucien Cardin, 'White Paper on Defence' (Queen's Printer and Controller of Stationery, March 1964), MLM, Department of National Defence Technical Library, https://walterdorn.net/pdf/DefenceWhitePaper-1964_D3-6-1964-eng_ReducedSize-OCR.pdf.

perhaps most poignant is the potential to obfuscate the origin of a range of information typically derived from sensitive intelligence sources and methods.

While it is impractical to expect that every opportunity identified be pursued, as competition increases, so too should the pursuit of advantage. With the ever-increasing amount of information, in ever-increasing variety and detail, comes great potential. Given Canada's long-standing categorization as a middle power, information can be disproportionately effective in its relations with other nations, and in enhancing the effectiveness of its military, so this is one area in which the pursuit of opportunities should be actively and aggressively pursued.

BIBLIOGRAPHY

Alexander, Amy L, Tad Brunyé, Jason Sidman, and Shawn A Weil. 'From Gaming to Training: A Review of Studies on Fidelity, Immersion, Presence, and Buy-in and Their Effects on Transfer in PC-Based Simulations and Games', 2005.

Amazon. 'What Is Cloud Storage? - Cloud Storage Explained - AWS'. Amazon Web Services, Inc. Accessed 23 March 2023. https://aws.amazon.com/what-is/cloud-storage/.

Bacon, Francis. 'Meditationes Sacrae and Human Philosphy', 1597.

Ball, George L., and Christopher (Kit) Runge. 'Producing Reusable Engineered Systems through Ontology: Implementing an Information Sciences Approach to Architecture-Driven, Model-Based, Concurrent Engineering'. *The Journal of Defense Modeling and Simulation* 11, no. 3 (1 July 2014): 219–26. https://doi.org/10.1177/1548512913502259.

Barnes, Julian E., and Helene Cooper. 'U.S. Battles Putin by Disclosing His Next Possible Moves'. *The New York Times*, 12 February 2022, sec. U.S. https://www.nytimes.com/2022/02/12/us/politics/russia-information-putin-biden.html.

'Battle of Myeongnyang'. In *Wikipedia*, 23 March 2023. https://en.wikipedia.org/w/index.php?title=Battle_of_Myeongnyang&oldid=1146266877.

Berthiaume, Lee. 'Canadian Army Waiting for Air-Defence Systems as Ottawa Buys Equipment for Ukraine'. CTVNews, 11 January 2023. https://www.ctvnews.ca/politics/canadian-army-waiting-for-air-defence-systems-as-ottawa-buys-equipment-for-ukraine-1.6226657.

———. 'Defence Chief Calls on Canadians to Rally behind Military during Personnel Crisis | CBC News'. CBC, 15 October 2022. https://www.cbc.ca/news/politics/wayne-eyre-canada-military-personnel-shortage-1.6617951.

Biddle, Stephen D. *Military Power: Explaining Victory and Defeat in Modern Battle*. STU-Student. Book, Whole. Princeton, N.J: Princeton University Press, 2004. https://doi.org/10.1515/9781400837823.

Bonta, Bruce D. 'Cooperation and Competition in Peaceful Societies.' *Psychological Bulletin* 121, no. 2 (March 1997): 299–320. https://doi.org/10.1037/0033-2909.121.2.299.

Box, George E. P. 'Science and Statistics'. *Journal of the American Statistical Association* 71, no. 356 (1 December 1976): 791–99. https://doi.org/10.1080/01621459.1976.10480949.

Breakspear, Alan. 'A New Definition of Intelligence'. *Intelligence and National Security* 28, no. 5 (1 October 2013): 678–93. https://doi.org/10.1080/02684527.2012.699285.

Brewster, Murray. 'ANALYSIS | A Tale of Two Fighter Jets — and What It Means for Canada's Defence and Place in the World | CBC News'. CBC, 3 January 2022. https://www.cbc.ca/news/politics/canada-fighter-jets-defence-1.6296021.

Brewster, Murray, and Richard Raycraft · CBC News ·. 'Military Personnel Shortage Will Get Worse before It Gets Better, Top Soldier Says | CBC News'. CBC, 6 October 2022. https://www.cbc.ca/news/politics/eyre-shortage-directive-1.6608107.

Campbell, Douglas. 'The Canadianization of the Joint Support Ship: From Mature Design to a Unique Canadian Solution'. Canadian Global Affairs Institute. Accessed 22 March 2023. https://www.cgai.ca/the_canadianization_of_the_joint_support_ship_from_mature_design_to_a_unique_canadian_solution.

Canada. 'National Defence Act', 1985. https://laws.justice.gc.ca/eng/acts/N-5/.

Canada, Public Services and Procurement. 'Public Services and Procurement Canada'. Organizational descriptions;navigation page - institutional profile, 27 October 2020. https://www.canada.ca/en/public-services-procurement.html.

Cancian, Mark F., Matthew Cancian, and Eric Heginbotham. 'The First Battle of the Next War: Wargaming a Chinese Invasion of Taiwan', 9 January 2023. https://www.csis.org/analysis/first-battle-next-war-wargaming-chinese-invasion-taiwan.

Carson, J.S. 'Introduction to Modeling and Simulation'. In *Proceedings of the Winter Simulation Conference, 2005.*, 8 pp.-, 2005. https://doi.org/10.1109/WSC.2005.1574235.

Chen, James. 'Money Laundering: What It Is and How to Prevent It'. Investopedia, 29 June 2022. https://www.investopedia.com/terms/m/moneylaundering.asp.

Chin, Warren. 'Technology, War and the State: Past, Present and Future'. *International Affairs* 95, no. 4 (1 July 2019): 765–83. https://doi.org/10.1093/ia/iiz106.

Clapper, James R. 'How 9/11 Transformed the Intelligence Community; It's No Longer about "need to Know." Our Guiding Principle Is "Responsibility to Share."' *Wall Street Journal (Online)*, 7 September 2011, sec. Opinion.

'Communication, n.' In *Oxford English Dictionary - Online*. Oxford University Press. Accessed 5 March 2023. https://www.oed.com/view/Entry/37309.

Courtney, Joe. 'Moskva's Sinking, the Rise of Anti-Ship Cruise Missiles and What That Means for the US Navy'. Defense News, 3 May 2022. https://www.defensenews.com/opinion/commentary/2022/05/03/moskvas-sinking-the-rise-of-anti-ship-cruise-missiles-and-what-that-means-for-the-us-navy/.

Cox, James. 'Lighting the Shadows: An Evaluation of Theory and Practice in Canadian Defence Intelligence'. Doctor of Philosophy, Royal Military College, 2011. https://www.collectionscanada.gc.ca/obj/thesescanada/vol2/002/NR82224.PDF.

Dahl, Erik J. 'NET-CENTRIC BEFORE ITS TIME: The Jeune École and Its Lessons for Today'. *Naval War College Review* 58, no. 4 (2005): 109–36.

'DARPA Defense Sciences Office - Training Superiority (DARWARS)', 20 July 2006. https://web.archive.org/web/20060720163726/http://www.darpa.mil/dso/thrust/biosci/training_super.htm.

Davenport, Thomas H., Paul Barth, and Randy Bean. 'How Big Data Is Different'. *MIT Sloan Management Review* 54, no. 1 (Fall 2012): 43–46.

Davies, Philip H. J. 'The Problem of Defence Intelligence'. *Intelligence and National Security* 31, no. 6 (18 September 2016): 797–809. https://doi.org/10.1080/02684527.2015.1115234.

Defence, National. 'Canadian Forces Intelligence Command'. Official Government. Canadian Forces Intelligence Command, 23 June 2014. https://www.canada.ca/en/department-national-defence/corporate/organizational-structure/canadian-forces-intelligence-command.html.

———. 'Canadian Joint Operations Command (CJOC)'. Not available, 19 February 2013. https://www.canada.ca/en/department-national-defence/corporate/organizational-structure/canadian-joint-operations-command.html.

———. 'Canadian Surface Combatant'. Education and awareness. Canadian surface combatant Project Summary, 13 March 2013. https://www.canada.ca/en/department-national-defence/services/procurement/canadian-surface-combatant.html.

———. 'DAOD 1000-10, Policy Framework for Corporate Administration Management'. Policies, 12 January 2017. https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/1000-series/1000/1000-10-policy-framework-corporate-administration-management.html.

———. 'DAOD 2006-0, Defence Security'. Policies, 27 September 2019. https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/2000-series/2006/2006-0-defence-security.html.

———. 'DAOD 2006-1, Procedures for the Safeguarding and Authorized Disclosure of Information in the DND and the CAF'. Navigation page, 12 January 2022. https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/2000-series/2006/2006-1-procedures-safeguarding-authorized-disclosure-information.html.

———. 'DAOD 6002-0, Information Technology'. Policies, 29 May 2014. https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/6000-series/6002/6002-0-information-technology.html.

———. 'DAOD 8008-0, Defence Intelligence'. Policies, 18 October 2017. https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/8000-series/8008/8008-0-defence-intelligence.html.

———. ‘Defence Purchases and Upgrades Process’. Education and awareness, 11 March 2013. https://www.canada.ca/en/department-national-defence/services/procurement/defence-purchases-and-upgrades-process.html.

———. ‘Evaluation of Defence Intelligence’. Canada, 30 March 2021. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/audit-evaluation/evaluation-defence-intelligence.html.

———. ‘Future Fighter Capability Project’. Education and awareness, 13 December 2018. https://www.canada.ca/en/department-national-defence/services/procurement/fighter-jets/future-fighter-capability-project.html.

———. ‘Integrated Strategic Analysis: Force Development’, 11 March 2022. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/audit-evaluation/isa-force-development.html.

———. ‘National Defence Security Orders and Directives’. Canada, 31 January 2022.

———. ‘Organizational Structure of the Department of National Defence and the Canadian Armed Forces’. Organizational descriptions, 22 April 2013. https://www.canada.ca/en/department-national-defence/corporate/organizational-structure.html.

‘Defense Advanced Research Projects Agency’. Accessed 25 February 2023. https://www.darpa.mil/.

Department of National Defence, Canada. ‘Strong, Secure, Engaged: Canada’s Defence Policy’, 31 May 2019. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html.

Desouza, Kevin C., and Ganesh K. Vanapalli. ‘Securing Knowledge in Organizations: Lessons from the Defense and Intelligence Sectors’. *International Journal of Information Management* 25, no. 1 (1 February 2005): 85–98. https://doi.org/10.1016/j.ijinfomgt.2004.10.007.

Dickinson, Peter. ‘2022 REVIEW: Why Has Vladimir Putin’s Ukraine Invasion Gone so Badly Wrong?’ *Atlantic Council* (blog), 19 December 2022. https://www.atlanticcouncil.org/blogs/ukrainealert/2022-review-why-has-vladimir-putins-ukraine-invasion-gone-so-badly-wrong/.

Dosi, Giovanni. ‘Technological Paradigms and Technological Trajectories: A Suggested Interpretation of the Determinants and Directions of Technical Change’. *Research Policy* 11, no. 3 (1 June 1982): 147–62. https://doi.org/10.1016/0048-7333(82)90016-6.

Dylan, Huw, and Thomas J. Maguire. ‘Secret Intelligence and Public Diplomacy in the Ukraine War’. *Survival* 64, no. 4 (4 July 2022): 33–74. https://doi.org/10.1080/00396338.2022.2103257.

Emanuelli, Paul. ‘Canadian Government Loses Direct Award Challenge’. *Procurement Office* (blog), 3 June 2019. https://procurementoffice.com/canadian-government-loses-direct-award-challenge/.

‘Evidence - NDDN (44-1) - No. 34 - House of Commons of Canada’. Accessed 11 February 2023. https://www.ourcommons.ca/DocumentViewer/en/44-1/NDDN/meeting-34/evidence.

Fayyad, Usama, and Ramasamy Uthurusamy. ‘Evolving Data Mining into Solutions for Insights’. *Communications of the ACM* 45, no. 8 (August 2002): 28–31. https://doi.org/10.1145/545151.545174.

Flynn, Michael T., and Charles A. Flynn. ‘Integrating Intelligence and Information: “Ten Points for the Commander”’. *Military Review* 92, no. 1 (2012): 4.

‘Force_1 Noun - Definition, Pictures, Pronunciation and Usage Notes | Oxford Advanced Learner’s Dictionary at OxfordLearnersDictionaries.Com’. Accessed 5 March 2023. https://www.oxfordlearnersdictionaries.com/definition/english/force_1.

Frantz, Frederick K, and A John Ellor. ‘Model Abstraction Techniques’. Scientific and Technical Report - Final. New York: United States Air Force Materiel Command, Rome Laboratory, August 1996. https://apps-dtic-mil.cfc.idm.oclc.org/sti/pdfs/ADA319039.pdf.

Funke, Christina M., Judy Borowski, Karolina Stosio, Brendel Wieland, Thomas S.A. Wallis, and Matthias Bethge. ‘Five Points to Check When Comparing Visual Perception in Humans and Machines’. *Journal of Vision* 21, no. 3 (March 2021). https://doi.org/10.1167/jov.21.3.16.

Gale, Alastair. ‘China’s Military Is Catching Up to the U.S. Is It Ready for Battle?’ *Wall Street Journal*, 20 October 2022, sec. World. https://www.wsj.com/articles/china-military-us-taiwan-xi-11666268994.

Giles, Lionel. *Sun Tzu On The Art Of War (1910 Translation)*. Classic ETexts. Routledge, 2000. https://doi.org/10.4324/9781315030081.

Golliday, C. ‘Data Link Communications in Tactical Air Command and Control Systems’. *IEEE Journal on Selected Areas in Communications* 3, no. 5 (September 1985): 779–91. https://doi.org/10.1109/JSAC.1985.1146251.

Google. ‘What Is Cloud Storage & How Does It Work?’ Google Cloud. Accessed 23 March 2023. https://cloud.google.com/learn/what-is-cloud-storage.

Gray, Chris Hables. *Postmodern War: The New Politics of Conflict*. Routledge, 2013.

Gross, David C. ‘Report from the Fidelity Implementation Study Group’, 1999. https://www.sisostds.org/DesktopModules/Bring2mind/DMX/API/Entries/Download?Command=Core_Download&EntryId=32793&PortalId=0&TabId=105.

Heath, Timothy R. ‘China’s Military Has No Combat Experience: Does It Matter?’, 27 November 2018. https://www.rand.org/blog/2018/11/chinas-military-has-no-combat-experience-does-it-matter.html.

Hellyer, Paul, and Lucien Cardin. ‘White Paper on Defence’. Queen’s Printer and Controller of Stationery, March 1964. MLM. Department of National Defence Technical Library. https://walterdorn.net/pdf/DefenceWhitePaper-1964_D3-6-1964-eng_ReducedSize-OCR.pdf.

Hernandez, Mike, Eduworks Corporation, Shelly Blake-Plock, Kevin Owens, and Benjamin Goldberg. ‘Enhancing the Total Learning Architecture for Experiential Learning’. In *Best Paper Sesssion 1*. Orlando, FL: National Training & Simulation Association, 2022. https://s3.amazonaws.com/amz.xcdsystem.com/44ECEE4F-033C-295C-BAE73278B7F9CA1D_abstract_File16562/PaperUpload_22461_0826100039.pdf.

Hodický, Jan, Dalibor Procházka, Fabian Baxa, Josef Melichar, Milan Krejčík, Petr Křížek, Petr Stodola, and Jan Drozd. ‘Computer Assisted Wargame for Military Capability-Based Planning’. *Entropy* 22, no. 8 (August 2020): 861. https://doi.org/10.3390/e22080861.

IBM. ‘What Is Cloud Storage? | IBM’. Accessed 23 March 2023. https://www.ibm.com/topics/cloud-storage.

Iselin, Errol R. ‘The Effects of Information Load and Information Diversity on Decision Quality in a Structured Decision Task’. *Accounting, Organizations and Society* 13, no. 2 (1 January 1988): 147–64. https://doi.org/10.1016/0361-3682(88)90041-4.

Jane’s. ‘DF-17’. In *Weapons: Strategic*. Vol. Online. Offensive Weapons. IHS Markit, 15 September 2022. https://customer.janes.com/display/JALWA161-JALW.

———. ‘Kh-47M2 Kinzhal (AS-24 ’Killjoy’)’. In *Weapons: Air Launched*. Vol. Online. Air-to-Surface Missiles - Stand-off and Cruise. IHS Markit, 14 April 2022. https://customer.janes.com/display/JALWA161-JALW.

Janis, Irving L, and Leon Mann. *Decision Making: A Psychological Analysis of Conflict, Choice, and Commitment.* Free press, 1977.

Kirby, Barry, Graham Fletcher, and Helen Dudfield. ‘Live Virtual Constructive Training Blend Optimisation Study’, 18. Bern: NATO, 2011. https://www.researchgate.net/profile/Barry-Kirby/publication/260451734_Live_Virtual_Constructive_Training_Blend_Optimisation_Study/links/00b495315a1f869c60000000/Live-Virtual-Constructive-Training-Blend-Optimisation-Study.

Kitchin, Rob. ‘Big Data and Human Geography: Opportunities, Challenges and Risks’. *Dialogues in Human Geography* 3, no. 3 (1 November 2013): 262–67. https://doi.org/10.1177/2043820613513388.

———. ‘Big Data, New Epistemologies and Paradigm Shifts’. *Big Data & Society* 1, no. 1 (1 April 2014): 2053951714528481. https://doi.org/10.1177/2053951714528481.

Klein, Gary. ‘Naturalistic Decision Making’. *Human Factors* 50, no. 3 (1 June 2008): 456–60. https://doi.org/10.1518/001872008X288385.

Klein, Gary A., ed. 'A Recognition-Primed Decision (RPD) Model of Rapid Decision Making'. In *Decision Making in Action: Models and Methods*. Norwood, N.J: Ablex Pub, 1993.

Korherr, Philipp, and Dominik Kanbach. 'Human-Related Capabilities in Big Data Analytics: A Taxonomy of Human Factors with Impact on Firm Performance'. *Review of Managerial Science*, 28 November 2021. https://doi.org/10.1007/s11846-021-00506-4.

Kuikka, Vesa, Juha-Pekka Nikkarila, and Marko Suojanen. 'Dependency of Military Capabilities on Technological Development'. *Journal of Military Studies* 6, no. 2 (30 November 2015): 29–58. https://doi.org/10.1515/jms-2016-0170.

Langley, Ann. 'Between "Paralysis by Analysis" and "Extinction by Instinct"'. *Sloan Management Review* 36, no. 3 (Spring 1995): 63.

Lee, Murray. 'We Have No Air Defence For Our Army – Why?' *RUSI(NS)* (blog), 24 January 2022. https://rusi-ns.ca/air-defence/.

Lewińska, Monika. 'The Role of Communication in Military Leadership'. *Journal of Corporate Responsibility and Leadership* 2 (9 March 2016): 37. https://doi.org/10.12775/JCRL.2015.003.

Line, The. 'Mitch Heimpel: Want to Fix Canadian Military Procurement? This Is What It'll Take'. Substack newsletter. *The Line* (blog), 14 March 2022. https://theline.substack.com/p/mitch-heimpel-want-to-fix-canadian.

Madachy, Raymond J, and Daniel Houston. *What Every Engineer Should Know About Modeling and Simulation*. CRC Press, 2017. https://books.google.ca/books?hl=en&lr=&id=fDwPEAAAQBAJ&oi=fnd&pg=PP1&dq=modelling+and+simulation+statistics&ots=hFd7P0lc6y&sig=YoW4fKgW9oZHyt9_yvm4bnmEFaM&redir_esc=y#v=onepage&q=modelling%20and%20simulation%20statistics&f=false.

Marrin, Stephen Patrick. 'Intelligence Analysis and Decisionmaking: Proximity Matters'. Ph.D., University of Virginia. Accessed 26 February 2023. https://www.proquest.com/docview/305010888/abstract/215F1521A0FD4B55PQ/1.

Marson, James. 'Putin Thought Ukraine Would Fall Quickly. An Airport Battle Proved Him Wrong.' *Wall Street Journal*, 3 March 2022, sec. World. https://www.wsj.com/articles/putin-thought-ukraine-would-fall-quickly-an-airport-battle-proved-him-wrong-11646343121.

Masters, Jonathan. 'Ukraine: Conflict at the Crossroads of Europe and Russia'. Council on Foreign Relations. Accessed 15 March 2023. https://www.cfr.org/backgrounder/ukraine-conflict-crossroads-europe-and-russia.

Maxwell, Paul. 'Artificial Intelligence Is the Future of Warfare (Just Not in the Way You Think)'. Modern War Institute, 20 April 2020. https://mwi.usma.edu/artificial-intelligence-future-warfare-just-not-way-think/.

McDermid, John A., Yan Jia, Zoe Porter, and Ibrahim Habli. ‘Artificial Intelligence Explainability: The Technical and Ethical Dimensions’. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 379, no. 2207 (16 August 2021): 20200363. https://doi.org/10.1098/rsta.2020.0363.

McNamee, Kai, Ailsa Chang, and Ashley Brown. ‘The U.S. Has an Overclassification Problem, Says One Former Special Counsel’. *NPR*, 17 January 2023, sec. National Security. https://www.npr.org/2023/01/17/1149426416/the-u-s-has-an-overclassification-problem-says-one-former-special-counsel.

Nakashima, Ellen, Shane Harris, Alex Horton, and Michael Birnbaum. ‘U.S. Intelligence Shows Russia’s Military Pullback Was a Ruse, Officials Say’. *Washington Post*, 18 February 2022. https://www.washingtonpost.com/world/2022/02/17/ukraine-russia-putin-nato-munich/.

National Defence, Department of. ‘Canadian Forces Joint Publication 1.0 - Canadian Military Doctrine’. Canada, April 2009. https://publications.gc.ca/collections/collection_2010/forces/D2-252-2009-eng.pdf.

———. ‘Canadian Forces Joint Publication 3.0 - Operations’. Canada, July 2010. https://publications.gc.ca/collections/collection_2011/dn-nd/D2-252-300-2010-eng.pdf.

———. ‘Canadian Military Doctrine’. *Canadian Forces Joint Publication* Canadian Military Doctrine, no. CFJP 01 (September 2011): 27.

National Defense, Department of. ‘Canadian Forces Joint Publication 2-0 - Intelligence’. Canada, 25 October 2011.

National Training and Simulation Association. ‘About I/ITSEC | I/ITSEC’. About I/ITSEC. Accessed 16 April 2023. https://www.iitsec.org/about-iitsec.

———. ‘History | I/ITSEC’. History | I/ITSEC. Accessed 16 April 2023. https://www.iitsec.org/about-iitsec/history.

Newdick, Thomas. ‘Russian MiG-31s Armed With Anti-Ship Ballistic Missiles Join Tu-22M3 Bombers In Syria’. The Drive, 25 June 2021. https://www.thedrive.com/the-war-zone/41276/russian-mig-31s-armed-with-anti-ship-ballistic-missiles-join-tu-22m3-bombers-in-syria.

O’Hanlon, Michael E. ‘Forecasting Change in Military Technology, 2020-2040’. *Brookings* (blog), 11 September 2018. https://www.brookings.edu/research/forecasting-change-in-military-technology-2020-2040/.

O’Neill, John Terrence. ‘EYEWITNESS - The Irish Company at Jadotville, Congo, 1961: Soldiers or Symbols?’, 8 September 2010. https://doi.org/10.1080/714002781.

O’Rourke, Ronald. ‘China Naval Modernization: Implications for U.S. Navy Capabilities - Background and Issues for Congress (Updated)’. Hauppauge, United States:

Nova Science Publishers, Inc., 2021. https://www.proquest.com/docview/2577533124/abstract/8CE8E32C5ECC46B1PQ/1.

———. 'China Naval Modernization: Implications for U.S. Navy Capabilities—Background and Issues for Congress'. Congressional Research Services, 1 December 2022. https://sgp.fas.org/crs/row/RL33153.pdf.

Oxford University Press. 'Accuracy Noun - Definition, Pictures, Pronunciation and Usage Notes | Oxford Learner's Dictionary of Academic English at OxfordLearnersDictionaries.Com'. Accessed 5 March 2023. https://www.oxfordlearnersdictionaries.com/definition/academic/accuracy.

Ozberk, Tayfun. 'China Test-Fires New YJ-21 Hypersonic Missile'. *Naval News* (blog), 20 April 2022. https://www.navalnews.com/naval-news/2022/04/china-test-fires-new-yj-21-hypersonic-missile/.

Pace, Dale K. 'Modeling and Simulation Verification and Validation Challenges'. *JOHNS HOPKINS APL TECHNICAL DIGEST* 25, no. 2 (2004).

Pecht, Eyal, and Asher Tishler. 'The Value of Military Intelligence'. *Defence and Peace Economics* 26, no. 2 (2015): 179–211. https://doi.org/10.1080/10242694.2014.886435.

Phillips-Wren, Gloria, and Monica Adya. 'Decision Making under Stress: The Role of Information Overload, Time Pressure, Complexity, and Uncertainty'. *Journal of Decision Systems* 29, no. sup1 (18 August 2020): 213–25. https://doi.org/10.1080/12460125.2020.1768680.

Pothoven, Saskia, Sebastiaan Rietjens, and Peter de Werd. 'Producer-Client Paradigms for Defense Intelligence'. *Defence Studies* 23, no. 1 (2 January 2023): 68–85. https://doi.org/10.1080/14702436.2022.2089658.

'Precision Noun - Definition, Pictures, Pronunciation and Usage Notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.Com'. Accessed 5 March 2023. https://www.oxfordlearnersdictionaries.com/definition/english/precision.

'Project Convergence: An Experiment for Multidomain Operations', 16 February 2022. https://www.csis.org/analysis/project-convergence-experiment-multidomain-operations.

Pugliese, David. 'New Navy Supply Ships Face More Delays and Cost Increases, Federal Officials Confirm'. ottawacitizen. Accessed 22 March 2023. https://ottawacitizen.com/news/national/defence-watch/new-navy-supply-ships-face-more-delays-and-cost-increases-federal-officials-confirm.

Rahmat, Ridzwan. 'China Expounds Capabilities of YJ-21 Hypersonic Anti-Ship Missile'. *Jane's Defence Weekly*, 7 February 2023. https://customer.janes.com/Janes/Display/BSP_53424-JDW.

Rand, David G., and Martin A. Nowak. ‘Human Cooperation’. *Trends in Cognitive Sciences* 17, no. 8 (1 August 2013): 413–25. https://doi.org/10.1016/j.tics.2013.06.003.

Research and Engineering, Under Secretary of Defense for. ‘DEM&S Glossary – DCTO(MC)’. Database. The Digital Engineering, Modeling and Simulation (DEM&S) Glossary. Accessed 26 February 2023. https://ac.cto.mil/de-ms-glossary/.

Roberts, Lon. ‘Analysis Paralysis: A Case of Terminological Inexactitude’. *Defence AT&L* January-February (2010). https://www.dau.edu/library/defense-atl/DATLFiles/Jan-Feb/robersts_jan-feb10.pdf.

Rothenberg, Jeff. ‘A Discussion of Data Quality for Verification, Validation, and Certification (VV&C) of Data to Be Used in Modeling’. RAND Corporation, 1997.

Roza, Manfred, Jeroen Voogd, Hans Jense, and Paul van Gool. ‘Fidelity Requirements Specification: A Process Oriented View’, n.d.

Rozman, Jeremiah. ‘The Synthetic Training Environment’. *Association of the United States Army SPOTLIGHT* 20, no. 6 (December 2020). https://www.ausa.org/sites/default/files/publications/SL-20-6-The-Synthetic-Training-Environment.pdf.

Rózsa, Sándor, Rita Hargitai, András Láng, Anikó Osváth, Ernő Hupuczi, István Tamás, and János Kállai. ‘Measuring Immersion, Involvement, and Attention Focusing Tendencies in the Mediated Environment: The Applicability of the Immersive Tendencies Questionnaire’. *Frontiers in Psychology* 13 (14 July 2022): 931955. https://doi.org/10.3389/fpsyg.2022.931955.

Sandhu, R.S., and P. Samarati. ‘Access Control: Principle and Practice’. *IEEE Communications Magazine* 32, no. 9 (September 1994): 40–48. https://doi.org/10.1109/35.312842.

Sar, Ai. ‘The History Of Money Laundering And It’s Origins’. financialcrimesacademy.org, 18 January 2023. https://financialcrimeacademy.org/the-history-of-money-laundering-and-its-origins/.

Science and Technology Organization. ‘Guidelines for Modelling and Simulation (M&S) Use Risk Identification, Analysis, and Mitigation’. North Atlantic Treaty Organization, September 2021. https://apps.dtic.mil/sti/pdfs/AD1183690.pdf.

Secretariat, Treasury Board of Canada. ‘Directive on Security Management’, 20 June 2019. https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611.

Secretary Of Defense, Office of the. ‘Military and Security Developments Involving the People’s Republic of China 2020 - Annual Report to Congress’. United States, 21 August 2020. https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.

Souren, Paul, Lingyao Yuan, Hemant K. Jain, Lionel P. Robert, Jim Spohrer, and Hila Lifshitz-Assaf. 'Intelligence Augmentation: Human Factors in AI and Future of Work'. *AIS Transactions on Human-Computer Interactions* 14, no. 3 (September 2022): 426–45. https://doi.org/10.17705/1thci.00174.

Spencer, Maj Gen Patrick J. Donahoe, John. 'A Status Check on the Army's Preparation for the Next War'. Modern War Institute, 6 July 2021. https://mwi.usma.edu/a-status-check-on-the-armys-preparation-for-the-next-war/.

'TACTICAL DATA LINK – FROM LINK 1 TO LINK 22'. *Scientific Bulletin of Naval Academy* 19, no. 2 (15 December 2016). https://doi.org/10.21279/1454-864X-16-I2-046.

Taleb, Ikbal, Mohamed Adel Serhani, and Rachida Dssouli. 'Big Data Quality: A Survey'. In *2018 IEEE International Congress on Big Data (BigData Congress)*, 166–73, 2018. https://doi.org/10.1109/BigDataCongress.2018.00029.

'Throughput Noun - Definition, Pictures, Pronunciation and Usage Notes | Oxford Advanced American Dictionary at OxfordLearnersDictionaries.Com'. Accessed 5 March 2023. https://www.oxfordlearnersdictionaries.com/definition/american_english/throughput.

Till, Steve Van. 'The Convergence of the Physical and Digital Security Worlds'. Security Info Watch, 14 July 2021. https://www.securityinfowatch.com/access-identity/article/21227403/the-convergence-of-the-physical-and-digital-security-worlds.

Tolk, Andreas. *Engineering Principles of Combat Modeling and Distributed Simulation*. Book, Whole. Hoboken: Wiley, 2012.

'Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing'. United States Government Publishing Office, 24 August 2004. https://www.govinfo.gov/content/pkg/CHRG-108hhrg98291/html/CHRG-108hhrg98291.htm.

Tucker, Ola M. *The Flow of Illicit Funds: A Case Study Approach to Anti-Money Laundering Compliance*. Washington, UNITED STATES: Georgetown University Press, 2022. http://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/detail.action?docID=29276966.

United Nations. 'Money Laundering'. United Nations: Office on Drugs and Crime. Accessed 14 March 2023. https://www.unodc.org/unodc/en/money-laundering/overview.html.

———. 'United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances'. United Nations, 1988. https://www.unodc.org/pdf/convention_1988_en.pdf.

Villányi, Benjámin. 'Money Laundering: History, Regulations, and Techniques'. Oxford Research Encyclopedia of Criminology and Criminal Justice, 26 April 2021. https://doi.org/10.1093/acrefore/9780190264079.013.708.

Vroegop, Ruben. ‘The State of Information and Intelligence Sharing in Canada’. Innovation and Technology. The Conference Board of Canada, 11 January 2017.

Wang, Jingdong, Ke Sun, Tianheng Cheng, Borui Jiang, Chaorui Deng, Yang Zhao, Dong Liu, et al. ‘Deep High-Resolution Representation Learning for Visual Recognition’. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 43, no. 10 (October 2021): 3349–64. https://doi.org/10.1109/TPAMI.2020.2983686.

Watling, Jack. ‘Russia’s Underperforming Military Capability May Be Key to Its Downfall’. *The Observer*, 18 September 2022, sec. World news. https://www.theguardian.com/world/2022/sep/18/russia-military-underperforming-ukraine.

Weder, Annika. ‘What Is Intelligence?’ The Hub, 5 October 2020. https://hub.jhu.edu/2020/10/05/artificial-intelligence-daeyeol-lee/.

SUPPLEMENTAL BIBLIOGRAPHY

The references below were all consulted in the generation of this work. While not directly referenced or cited, they indirectly influenced the lines of inquiry and provided background context in support of the author's efforts. Acknowledgement is made herein to this effect.

Aickelin, Uwe, Jenna Marie Reps, Peer-Olaf Siebers, and Peng Li. 'Using Simulation to Incorporate Dynamic Criteria into Multiple Criteria Decision-Making'. Journal of the Operational Research Society 69, no. 7 (3 July 2018): 1021–32. https://doi.org/10.1080/01605682.2017.1410010.

Alessi, Stephen M. 'Fidelity in the Design of Instructional Simulations'. Journal of Computer-Based Instruction 15 (1988): 40–47.

Almazan, Jose E. 'Dissention Through Red Teaming'. Marine Corps Gazette 98, no. 8 (August 2014): 35–37.

Aslett, Matt. 'A Pathfinder Paper Navigates Decision-Makers through the Issues Surrounding a Specific Technology or Business Case, Explores the Business Value of Adoption, and Recommends the Range of Considerations and Concrete next Steps in the Decision-Making Process.', n.d.

Balci. 'Verification, Validation, and Certification of Modeling and Simulation Applications'. In Proceedings of the 2003 Winter Simulation Conference, 2003., 1:150-158 Vol.1, 2003. https://doi.org/10.1109/WSC.2003.1261418.

Becker, David, Trish Dunn King, and Bill McMullen. 'Big Data, Big Data Quality Problem'. In 2015 IEEE International Conference on Big Data (Big Data), 2644–53, 2015. https://doi.org/10.1109/BigData.2015.7364064.

Behlendorf, Brandon, and Gary Ackerman. 'DESSRT: A Novel Framework for Empirical Red Teaming at Scale'. Simulation & Gaming 54, no. 1 (1 February 2023): 5–27. https://doi.org/10.1177/10468781221135199.

Belton, Valerie, and Theodor Stewart. Multiple Criteria Decision Analysis: An Integrated Approach. Springer Science & Business Media, 2002.

Biermann, Joachim and Research Establishment For Applied Sciences Wachtberg-Werthhoven (Germany) Ergonomics/Information Sys. 'A Knowledge-Based Approach to Information Fusion for the Support of Military Intelligence', no. Generic (2004).

Box, George EP, William H Hunter, and Stuart Hunter. Statistics for Experimenters. Vol. 664. John Wiley and sons New York, 1978.

Carvin, Stephanie, and Michael John Williams. Law, Science, Liberalism, and the American Way of Warfare: The Quest for Humanity in Conflict. Book, Whole. Cambridge, UK;New York; Cambridge University Press, 2015. https://doi.org/10.1017/CBO9781107589704.

Chengalur-Smith, I.N., D.P. Ballou, and H.L. Pazer. 'The Impact of Data Quality Information on Decision Making: An Exploratory Analysis'. IEEE Transactions on Knowledge and Data Engineering 11, no. 6 (November 1999): 853–64. https://doi.org/10.1109/69.824597.

Connable, Ben, Rand Corporation, International Security and Defense Policy Center, and National Defense Research Institute (U.S.). Modeling, Simulation, and Operations Analysis in Afghanistan and Iraq: Operational Vignettes, Lessons Learned, and a Survey of Selected Efforts. Vol. RR-382-OSD. Book, Whole. Santa Monica, CA: Rand Corporation, 2014. https://doi.org/10.7249/j.ctt5vjwt0.

Cordner, Gary, and Kathryn Scarborough. ‘Information Sharing: Exploring the Intersection of Policing with National and Military Intelligence’. Homeland Security Affairs, 2010.

Cox, James. ‘A Fundamental Re-Conceputalization of Intelligence: Cognitive Activity and the Pursuit of Advantage’. Intelligence and National Security 37, no. 2 (23 February 2022): 197–215. https://doi.org/10.1080/02684527.2021.2005884.

———. ‘Defence Leadership of Intelligence Education’. Vimy Paper 51 (October 2022). https://cdainstitute.ca/wp-content/uploads/2022/11/Vimy_Paper_51.pdf.

Dalle, Olivier. ‘On Reproducibility and Traceability of Simulations’. In Proceedings of the 2012 Winter Simulation Conference (WSC), 1–12, 2012. https://doi.org/10.1109/WSC.2012.6465284.

Davies, Philip H. J., and Kristian Gustafson. ‘Intelligence and Military Doctrine: Paradox or Oxymoron?’ Defence Studies 19, no. 1 (2 January 2019): 19–36. https://doi.org/10.1080/14702436.2018.1538698.

Davis, Paul K., Jonathan Kulick, Michael Egner, Rand Corporation, and Project Air Force (U.S.). Implications of Modern Decision Science for Military Decision-Support Systems. 1st ed. Vol. MG-360. Book, Whole. Santa Monica, CA: Rand Project Air Force, 2005. https://doi.org/10.7249/mg360af.

De Prada, Cesar, Costas Pantelides, and Jose Luis Pitarch. Process Modelling and Simulation. MDPI, Basel, 2019. https://doi.org/10.3390/books978-3-03921-456-3.

Dent, Matthew, Simon Shield, Andy Reeves, and Jamie Royston. ‘Whose Line Is It Anyway? Using MBSE in the Management and Acceptance of the Defence Lines of Development’. INCOSE International Symposium 27, no. 1 (2017): 1314–26. https://doi.org/10.1002/j.2334-5837.2017.00430.x.

Ding, Ru-Xi, Iván Palomares, Xueqing Wang, Guo-Rui Yang, Bingsheng Liu, Yucheng Dong, Enrique Herrera-Viedma, and Francisco Herrera. ‘Large-Scale Decision-Making: Characterization, Taxonomy, Challenges and Future Directions from an Artificial Intelligence and Applications Perspective’. Information Fusion 59 (1 July 2020): 84–102. https://doi.org/10.1016/j.inffus.2020.01.006.

Fishwick, P.A. ‘The Role of Process Abstraction in Simulation’. IEEE Transactions on Systems, Man, and Cybernetics 18, no. 1 (January 1988): 18–39. https://doi.org/10.1109/21.87052.

Gentry, John A. ‘Intelligence in War: How Important Is It? How Do We Know?’ Intelligence and National Security 34, no. 6 (19 September 2019): 833–50. https://doi.org/10.1080/02684527.2019.1611205.

Giarlotta, Alfio. ‘New Trends in Preference, Utility, and Choice: From a Mono-Approach to a Multi-Approach’. In New Perspectives in Multiple Criteria Decision Making: Innovative Applications and Case Studies, edited by Michalis Doumpos, José Rui Figueira, Salvatore Greco, and Constantin Zopounidis, 3–80. Multiple Criteria Decision Making. Cham: Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-11482-4_1.

Gray, Wayne D. ‘Simulated Task Environments: The Role of High-Fidelity Simulations, Scaled Worlds, Synthetic Environments, and Laboratory Tasks in Basic and Applied Cognitive Research’, n.d.

Greasley, Andrew. Enabling a Simulation Capability in the Organisation. Book, Whole. London: Springer, 2008.

Hartley, Dean S. Unconventional Conflict: A Modeling Perspective. Book, Whole. Cham, Switzerland: Springer, 2017.

Horowitz, Michael C. ‘When Speed Kills: Lethal Autonomous Weapon Systems, Deterrence and Stability’. Journal of Strategic Studies 42, no. 6 (19 September 2019): 764–88. https://doi.org/10.1080/01402390.2019.1621174.

Hue, Meredith. ‘An Analysis of SE and MBSE Concepts to Support Defence Capability Acquisition’, n.d.

Janis, Irving L, and Leon Mann. Decision Making: A Psychological Analysis of Conflict, Choice, and Commitment. Free press, 1977.

Johnston, Catherine, Elmo C. Wright, Jr., Jessica Bice, Jennifer Almendarez, and Linwood Creekmore. ‘Transforming Defense Analysis’. Joint Force Quaterly, 1 October 2015. https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-79/Article/621117/transforming-defense-analysis/https%3A%2F%2Fndupress.ndu.edu%2FMedia%2FNews%2FNews-Article-View%2FArticle%2F621117%2Ftransforming-defense-analysis%2F.

Jung, Sang-Rae, and Hyun-Shik Shin. ‘Analysis on Technology Development of NCW and Tactical Data Link’. The Journal of the Korea institute of electronic communication sciences 7, no. 5 (2012): 991–98. https://doi.org/10.13067/JKIECS.2012.7.5.991.

Kimmons, Jeff, and Graham Gilmer. ‘REMAKING INTELLIGENCE PROCESSING, EXPLOITATION AND DISSEMINATION’. Defense One, Booz Allen Hamilton Thought Pieces, n.d. Accessed 31 January 2023.

Kincaid, John. ‘Of Time, Body, and Scarcity: Policy Options and Theoretic Considerations’. International Political Science Review / Revue Internationale de Science Politique 4, no. 3 (1983): 401–16.

Kołodziej, Joanna, and Horacio González-Vélez. High-Performance Modelling and Simulation for Big Data Applications: Selected Results of the COST Action

IC1406 CHiPSet. Book, Whole. Cham: Springer International Publishing AG, 2019.

Korherr, Philipp, and Dominik Kanbach. ‘Human-Related Capabilities in Big Data Analytics: A Taxonomy of Human Factors with Impact on Firm Performance’. Review of Managerial Science, 28 November 2021. https://doi.org/10.1007/s11846-021-00506-4.

Kosow, Hannah. ‘New Outlooks in Traceability and Consistency of Integrated Scenarios’. European Journal of Futures Research 3, no. 1 (7 December 2015): 16. https://doi.org/10.1007/s40309-015-0077-6.

Libicki, Martin C., Brian A. Jackson, David R. Frelinger, Beth E. Lachman, Cesse Ip, Nidhi Kalra, and RAND NATIONAL DEFENSE RESEARCH INST SANTA MONICA CA. ‘What Should Be Classified? A Framework with Application to the Global Force Management Data Initiative’, no. Generic (2010).

Linthicum, David. ‘Data Management on the Edge: Time to Get Partitioning’. TechBeacon. Accessed 16 March 2023. https://techbeacon.com/enterprise-it/data-management-edge-time-get-partitioning.

Liu, Dahai, Nikolas Macchiarella, and Dennis Vincenzi. ‘Simulation Fidelity’. In Human Factors in Simulation and Training, 61–73, 2008. https://doi.org/10.1201/9781420072846.ch4.

Lohr, Steve. ‘For Big-Data Scientists, “Janitor Work” Is Key Hurdle to Insights’. The New York Times, 18 August 2014, sec. Technology. https://www.nytimes.com/2014/08/18/technology/for-big-data-scientists-hurdle-to-insights-is-janitor-work.html.

Lugmayr, Artur, Björn Stockleben, Christoph Scheib, and Mathew A. Mailaparampil. ‘Cognitive Big Data: Survey and Review on Big Data Research and Its Implications. What Is Really “New” in Big Data?’ Journal of Knowledge Management 21, no. 1 (2017): 197–212. https://doi.org/10.1108/JKM-07-2016-0307.

Marrin, Stephen. ‘Revisiting Intelligence and Policy: Problems with Politicization and Receptivity’. Intelligence and National Security 28, no. 1 (1 February 2013): 1–4. https://doi.org/10.1080/02684527.2012.749063.

Marsella, Nicholas R. ‘Red Teaming and the Intelligence Professional: The Environment and the Challenge’. Military Intelligence Professional Bulletin 34, no. 3 (September 2008): 28–32.

Moon, Il-Chul, and Jeong Hee Hong. ‘Theoretic Interplay between Abstraction, Resolution, and Fidelity in Model Information’. In 2013 Winter Simulations Conference (WSC), 1283–91. Washington, DC, USA: IEEE, 2013. https://doi.org/10.1109/WSC.2013.6721515.

Noguchi, Ryan A. ‘Lessons Learned and Recommended Best Practices from Model-Based Systems Engineering (MBSE) Pilot Projects’, 14 June 2016.

Raska, Michael. ‘The Sixth RMA Wave: Disruption in Military Affairs?’ Journal of Strategic Studies 44, no. 4 (7 June 2021): 456–79. https://doi.org/10.1080/01402390.2020.1848818.

Raybourn, Elaine M. ‘A New Paradigm for Serious Games: Transmedia Learning for More Effective Training and Education’. Journal of Computational Science 5, no. 3 (1 May 2014): 471–81. https://doi.org/10.1016/j.jocs.2013.08.005.

Sabin, Philip A. G. Simulating War: Studying Conflict through Simulation Games. 1st ed. Book, Whole. London;New York; Continuum, 2012. https://doi.org/10.5040/9781474211239.

Saini, Rijul, Gunter Mussbacher, Jin L. C. Guo, and Jörg Kienzle. ‘Automated Traceability for Domain Modelling Decisions Empowered by Artificial Intelligence’. In 2021 IEEE 29th International Requirements Engineering Conference (RE), 173–84, 2021. https://doi.org/10.1109/RE51729.2021.00023.

Sargent, Robert. ‘Verification and Validation of Simulation Models’, 37:166–83, 2011. https://doi.org/10.1109/WSC.2010.5679166.

Talbert, Bonnie. ‘Overthinking and Other Minds: The Analysis Paralysis’. Social Epistemology 31, no. 6 (2 November 2017): 545–56. https://doi.org/10.1080/02691728.2017.1346933.

Tiwari, Milind, Adrian Gepp, and Kuldeep Kumar. ‘A Review of Money Laundering Literature: The State of Research in Key Areas’. Pacific Accounting Review 32, no. 2 (1 January 2020): 271–303. https://doi.org/10.1108/PAR-06-2019-0065.

Vlahopoulos, Nickolas, Syed Mohammad, Geng Zhang, Sungmin Lee, and Ann Arbor. ‘Probabilistic Analysis for Structuring an Effective Defense against Adversarial Attacks’. In ECIT 5: Analysis against Deep Threats and Adversarial Attacks. Orlando, FL: National Training & Simulation Association, 2022. https://s3.amazonaws.com/amz.xcdsystem.com/44ECEE4F-033C-295C-BAE73278B7F9CA1D_abstract_File16562/PaperUpload_22203_0825091834.pdf.

Washburn, Alan, and Moshe Kress. Combat Modeling. 1. Aufl. Vol. 134. Book, Whole. New York;Dordrecht; Springer, 2009. https://doi.org/10.1007/978-1-4419-0790-5.

Watling, Jack. ‘Preparing Military Intelligence for Great Power Competition: Retooling the 2-Shop’. The RUSI Journal 166, no. 1 (2021): 68–80. https://doi.org/10.1080/03071847.2021.1923408.

White, K. Preston, and Ricki G. Ingalls. ‘Introduction to Simulation’. In 2015 Winter Simulation Conference (WSC), 1741–55, 2015. https://doi.org/10.1109/WSC.2015.7408292.

Williams, Kara, and Gargi Sharma. ‘A Look Back at Anti-Money Laundering in 2022 | FINRA.Org’. Accessed 14 March 2023. https://www.finra.org/media-center/blog/a-look-back-at-anti-money-laundering-in-2022.

Witmer, Bob G, and Michael J Singer. 'Measuring Immersion in Virtual Environments'. ARI Technical Report. Arlington, VA: US Army Research Institute for Behavioural and Social Sciences, 1994.

Wright, MGen Michael. 'CFINTCOM 101 Placemat'. Placemat, 2 February 2022. https://www.canada.ca/content/dam/dnd-mdn/documents/reports/2022/placemat-cfintcom.pdf.

Yaqoob, Ibrar, Ibrahim Abaker Targio Hashem, Abdullah Gani, Salimah Mokhtar, Ejaz Ahmed, Nor Badrul Anuar, and Athanasios V. Vasilakos. 'Big Data: From Beginning to Future'. International Journal of Information Management 36, no. 6, Part B (1 December 2016): 1231–47. https://doi.org/10.1016/j.ijinfomgt.2016.07.009.

Zyda, Michael. 'Modeling and Simulation: Linking Entertainment & Defense'. 22 October 1997. https://core.ac.uk/download/pdf/36733811.pdf.