National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Major Glen Dunlop

Information Is Not a Domain

JCSP 47

Exercise Solo Flight

Disclaimer

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.

PCEMI 47

Exercice Solo Flight

Avertissement

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 47 – PCEMI 47
2020 – 2022

Exercise Solo Flight – Exercice Solo Flight

Major Glen Dunlop

Information Is Not a Domain

INFORMATION IS NOT A DOMAIN

Introduction

Information is an instrument of national power, that is how important it is. At the grand strategic (i.e., political) level, the instruments of national power are divided through the Diplomatic, Informational, Military, and Economic. Each instrument exercises its power through inherent capabilities, yet the actions taken happen *in and through* something. The effects that result from these actions leave a mark *somewhere*. The Information Environment (IE) is a global environment that accounts for physical, virtual, and cognitive effects. It is the pond that a pebble is dropped in and ripples are seen and impacts measured. The Military instrument, for its part, must be postured to incorporate and exploit the IE as part of its Whole-of-Government mission. Military power is exercised in a delineated Operating Environment (OE) through five doctrinal domains: Space, Land, Air, Maritime, and Cyber. These domains are bounded within their physical environments, so if Information is an environment as well, should it not be the next emergent domain? The thesis I am proposing is that information cannot and should not be a domain but remain an environment where the effectiveness of actions taken in the five doctrinal domains can be measured. The IE as a global phenomenon alleviates a tendency to turn a domain into a conceptual stovepipe[1] which is a problem domains were arguably created to solve in the first place.[2] Second, there is significant redundancy in the composition of the IE enveloping the characteristics of the five

---

[1] Maj Mark Crimm, "Can We Please Stop Talking about Domains?," *Defense News*, February 18, 2022, https://www.defensenews.com/opinion/commentary/2022/02/18/can-we-please-stop-talking-about-domains/.

[2] Catherine A Theohary, "Defense Primer: Information Operations," Primer (Congressional Research Service, December 1, 2021), 2, https://crsreports.congress.gov/product/details?prodcode=IF10771.

domains, effectively saying the same thing twice. Lastly, and most importantly, the IE further focuses on the results of military activities, in other words, "effects" vice the activities being an end unto themselves. The employment of the Military instrument of power is ultimately designed to achieve specific objectives. Engineering the effects required to achieve those objectives requires activities to take place in certain spaces or in any or all the five doctrinal domains.[3] Focusing on the effects of these activities ensures the military instrument is being used efficiently.

Definitional Disambiguation

The first step to making this case will be looking at the challenges layered into the semantics of current schools of thought on the intersection between informational power, military power and the effects their application has. Pervasive throughout, and not wholly solved in this paper, is the tautological issue in attempting to measure informational activities in an informational layer of the IE. The next roadblock to a clear understanding is the loose use of language in literature, both academic and military. These papers are littered with the words "information," "domain," "layers," and "environment" used doctrinally, academically, and colloquially often in the same work. This disambiguation is important, because at the semantic level "domain" and "environment" are often used interchangeably. Perhaps this loose language works when communications occur in real time, and ideas can be expanded, however, a military planner cannot afford to say "environment" and have the audience hear "domain." Add to this that scouring Allied and Coalition doctrine to provide disambiguation of terms is important,[4] even from a

[3] Joint Chiefs of Staff, "Joint Concept for Operating in the Information Environment (JCOIE)" (Department of Defense, July 25, 2018), 30, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf.
[4] Ibid., 21.

strictly Canadian Armed Forces (CAF) context. It is unlikely that Canada will unilaterally act globally through the military instrument.[5] Therefore, the doctrinal concepts of coalition and allied partners is important. Indeed, when Canada ratifies NATO publications or adopts a non-CAF framework it is with the explicit intent to harmonise national doctrine unless specific caveats are mentioned.[6] This is vital so that development of Canadian operational practice does not diverge too widely from the international frameworks of which it must be a part. This approach is stymied though, as the official definitions from the NATO and Five-Eyes partners (and Canada is no better than its allies in this) often contain tautologies, using information to describe information.[7] The following paragraphs will expand on some of the definitional problems as well as establish a common understanding for the purposes of this essay.

Information Operations and Operating in the Information Environment

Capabilities are used to take actions (or the threat of action), these actions (or in the case of threats: inaction) create effects (intended or otherwise). An Information-Related Capability (IRC) creating an effect in an informational medium creates many opportunities for confusion. The first of these semantic nightmares is the confusion between Information Operations (IO), Information Warfare (IW), and Operating in the Information Environment (OIE). The reality is, there is no "right" answer. Even within a

---

[5] Canada and Department of National Defence, *Strong, Secure, Engaged - Canada's Defence Policy.*, 2017, 89, http://epe.lac-bac.gc.ca/100/201/301/weekly_acquisitions_list-ef/2017/17-23/publications.gc.ca/collections/collection_2017/mdn-dnd/D2-386-2017-eng.pdf.

[6] *CFJP 01 - Canadian Military Doctrine*, First, B-GJ-005-000/FP-001 (Ottawa, Ontario: Colonel Steven P. Noonan, MSC, CD, 2011), 6–5, http://www.cfd-cdf.forces.gc.ca/sites/page-eng.asp?page=3391.

[7] Thomas A. Drohan, "Paper #38. What 'Talk-Fight' Ideologues Understand About Warfare: All-Domain, All-Effects in the Information Environment.," *International Center for Security and Leadership*, April 19, 2021, 1, https://securityandleadership.com/paper-38-what-vietnamese-nationalists-understood-taliban-fundamentalists-understand-and-we-do-not-all-domain-all-effects-warfare/.

single nation, let alone an alliance, these terms are at times interchangeable and in some cases evolutionary. At one point IW was the strategy and IO was the operational level that bridged tactics (IRCs) with strategy.[8] Older paradigms, however, have been demonstrably shown to be ineffective within the more prevalent grey zone and the emerging hybrid warfare that occurs outside the threshold of armed conflict.[9] IO focuses on adversarial opponents in a defined OE. Something therefore is needed to account for this current reality inclusive of a global audience be they allies, competitors, or outright adversaries. OIE then sought to replace, or depending on the nation supersede IO,[10] which is the direction the United States Government's (USG) Department of Defense (DOD) is going in[11]. Canada also seems to be going down this path, at the time of writing this paper the current Working Draft of CFJP 3-10 now titled "Operating in the Information Environment" whereas it was formerly "Information Operations."[12] This paper is focussing on the concept of the Information Environment as the medium for the application of military power, be that application based on munitions or non-munitions based capabilities. Recognising that the IE is global in nature, and present-day reality calls for the application of military power outside the threshold of armed conflict, OIE will be the term used going forward.

---

[8] Theohary, "Defense Primer: Information Operations," 1.
[9] Joint Chiefs of Staff, "Joint Concept for Operating in the Information Environment (JCOIE)," 7.
[10] Theohary, "Defense Primer: Information Operations," 2.
[11] LtCol C Travis Reese, "Operations in the Information Environment," *Marine Corps Gazette*, Ideas and Issues, 104, no. 8 (August 2020): 31.
[12] *CFJP3-10 Operations in the Information Environment (OIE) Working Draft 1*, CFJP 3-10 2022-xx, 2022, http://collaboration-cjoc.forces.mil.ca/sites/JDoc/SitePages/Home.aspx.

The Five Domains

Having established that the IE is the medium, what then is used to describe and classify the activities themselves? This is where domains come into play. The extant doctrinal domains are Space, Land, Air, Maritime, and Cyber.[13] What, then, does it mean to have a domain? Merriam-Webster's definitions provide some interesting fodder for consideration before moving on to the military concept. First it implies "complete, and absolute ownership." Second is "a region distinctively marked by some physical feature." Third, and last for military relevance, it is "a sphere of knowledge, influence, or activity." Just these definitions alone explain why it would be easy to have the military implications of all three approaches conflated with more than one concept. Canada defines an "operating domain" as "…all entities, activities and information related to or affecting it. Note: In the CAF, there are five operating domains: maritime, land, air, space and cyber."[14] A review of US literature finds no single approved definition of the term "domain," yet each domain (the same five as Canada) is defined in several Joint Publications. While the specific definitions of particular domains is interesting, more relevant to this paper, is that information is not a domain in neither the US or NATO lexicon. NATO Operational domains are defined as: "discrete spheres of military activity within which operations are undertaken to achieve objectives in support of the mission."[15] Most importantly, domains were never intended to be stovepipes.[16] Quite the opposite, domains were meant to be viewed as an ecosystem, interconnected with activities synchronized to maximise effects leading to the attainment of military

[13] DTB record 694692
[14] DTB record 694692
[15] NATO Terminology Tracking file (TTF) 2018-0276.
[16] Crimm, "Can We Please Stop Talking about Domains?"

objectives. In other words: "[t]he domains are where the activity takes place to create effects and ultimately compel an adversary to comply with the will of the victorious state."[17] The composite of these domains is the OE, and prior to describing why the IE cannot be sliced into domains this paper will look at the framework of the OE.

The Operating Environment

In Canada, the Operating Environment is "the surroundings in which military operations take place. Note: Operating environments are physical (maritime, land, air, space, cyber and electromagnetic) and non-physical (information)."[18] This definition shares some of the tautological problems that information related definitions have. The sum of this definition is the OE is the environment operations occur in. Not wrong, but not helpful either. Canada is not alone in this challenge, many of the concepts Canada, the US, FVEY, and NATO allied partners practice in operations are not uniquely captured.[19] Conceptually, the OE is where activities take place, receiving and delivering inputs.[20] Having as complete an understanding of the OE as practical is how military planners can correctly apply military capabilities to achieve military objectives.[21] This is where the importance of the framework of the OE becomes apparent. Differentiating the space that activities take place in from the impacts of those activities helps to parse data into useful information that supports decision making. Domains are what give shape to the OE, therefore the sum of all domains is the OE. A final point with respect to the OE,

---

[17] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the Practice of Warfare," *International Journal: Canada's Journal of Global Policy Analysis* 69, no. 3 (September 2014): 398, doi:10.1177/0020702014540618.
[18] DTB record 43606
[19] Drohan, "Paper #38. What 'Talk-Fight' Ideologues Understand About Warfare," 2.
[20] Robert S. Ehlers Jr. and Patrick Blannin, "Making Sense of the Information Environment | Small Wars Journal," March 3, 2020, 2, https://smallwarsjournal.com/jrnl/art/making-sense-information-environment.
[21] Joint Chiefs of Staff, "Joint Concept for Operating in the Information Environment (JCOIE)," 25.

it is no longer the sole purview of state powers. This is important because with a wider range of state and non-state actors able to influence or impose effects onto the IE, the CAF and its Allies need a broader framework with which to analyse and assess the impacts of activities, not confined to a traditional Joint Operations Area (JOA). Simply conducting a threat oriented JIPOE is not enough. This idea was captured at the JCOIE Core Team Workshop held at Quantico, 18–19 April 2017, where it was noted that "The IE directly affects and transcends all OE."[22] These ideas will be included in the "recommendations" section of this paper.

Framing the Information Environment

The IE is not fundamentally different from the five domains characteristic wise, in fact, without information the OE would be a meaningless concept.[23] The IE is defined as "The aggregate of the individuals, organizations, and systems that collect, process, disseminate or act on information."[24] Described in the DoD's Joint Concept for Integrated Campaigning as "a heterogeneous global environment where humans and automated systems observe, orient, decide, and act on data, information, and knowledge."[25] Note that none of these definitions attempt to impose boundaries on the IE. In fact, US, FVEY and NATO are very explicit in that it is "unbounded [and] hyper-connected."[26] Most schools of thought describe the IE as having three layers (or

---

[22] Ibid., 42.
[23] Drohan, "Paper #38. What 'Talk-Fight' Ideologues Understand About Warfare," 13.
[24] Ehlers Jr. and Blannin, "Making Sense of the Information Environment | Small Wars Journal," 2.
[25] Joint Chiefs of Staff, "Joint Concept for Integrated Campaigning" (Department of Defense, March 16, 2018), 3, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257#:~:text=is%20Integrated%20Campaigning.-,The%20JCIC%20defines%20integrated%20campaigning%20as%20Joint%20Force%20and%20interorganizational,and%20duration%20across%20multiple%20domains.
[26] Ehlers Jr. and Blannin, "Making Sense of the Information Environment | Small Wars Journal," 1.

dimensions depending on the source): the cognitive, virtual (sometimes referred to as informational - another example of the tautological problem),[27][28] and physical. This paper will explore these layers/dimensions in reverse order. The physical dimension is all tangible elements in a given space and includes infrastructure and storage mediums.[29] The virtual/informational layer is where "we collect, process, store, disseminate, and protect information."[30] This layer is what links the physical to the cognitive. The cognitive is described as "composed of the attitudes, beliefs, and perceptions of those who transmit, receive, respond to, or act upon information."[31] As previously discussed, these layers are, in fact, the aggregate of the extant domains. The effects measured in the IE (also known as Measures of Effectiveness) will be created across all domains and OEs. "The IE directly affects and transcends all operating environments."[32] A hole in the ground created by a munition will have ripples across the IE extending past a specific OE. These ripples include the damage caused in the physical layer, but that is less important than the effects in the cognitive layer.[33]

The IE is Global

---

[27] Sara B. King, "Military Social Influence in the Global Information Environment: A Civilian Primer: Military Social Influence," *Analyses of Social Issues and Public Policy* 11, no. 1 (December 2011): 11, doi:10.1111/j.1530-2415.2010.01214.x.
[28] Tomasz Kacała, "Military Leadership in the Context of Challenges and Threats Existing in Information Environment," *Journal of Corporate Responsibility and Leadership* 2, no. 1 (March 9, 2016): 11, doi:10.12775/JCRL.2015.001.
[29] Ehlers Jr. and Blannin, "Making Sense of the Information Environment | Small Wars Journal," 1.
[30] Joint Chiefs of Staff, "Joint Concept for Operating in the Information Environment (JCOIE)," 3.
[31] United States Department of Defense, "STRATEGY FOR OPERATIONS IN THE INFORMATION ENVIRONMENT June 2016," June 2016, 3, https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.
[32] Theohary, "Defense Primer: Information Operations," 2.
[33] King, "Military Social Influence in the Global Information Environment," 5.

The following three paragraphs will explore the "why" it is not helpful to create a sixth domain (i.e., information as a domain). The reader should be convinced by now that domains are *discreet* spheres of influence which, by definition, are bounded. They are domains because military planners carve them out of their related physical environments to create an OE as a composite thereof. So why is there is no utility in carving out an "Information Domain" to overlay on the doctrinal domains as part of the OE? The answer is it would be an impediment to conducting operations and planning campaigns where understanding all the dynamics are essential for a commander to effectively employ capabilities and make decisions. Going back to the exploration of the term "environment" it is important to capture that it is the "the aggregate of social and cultural conditions that influence the life of an individual or community."[34] The IE is ubiquitous and activities in any region of the globe will have impacts across all domains.[35] "The IE is global in nature and cannot be contained. Effects create both intended and unintended consequences."[36] Ignoring influences halfway across the world may simplify the task of analysis, however, predicting change and measuring effectiveness become impossible. Further, the risk of unintended consequences expands as we ignore more and more inputs in a drive to parse out whole sections, indeed the greater part, of the IE into a discreet domain. So far this paper has only implied the existence of multiple OEs, yet even Canada, relatively small compared to the global campaigning of the US or NATO, conducts activities in multiple theaters. A myopic view of internal impacts could and do miss interconnectedness and perceptions by not

---

[34] Ehlers Jr. and Blannin, "Making Sense of the Information Environment | Small Wars Journal," 2.
[35] Ibid., 1.
[36] Emilio Iasiello, "What Is the Role of Cyber Operations in Information Warfare?," *Journal of Strategic Security* 14, no. 4 (January 2021): 74, doi:10.5038/1944-0472.14.4.1931.

only allies, or neutral parties, but competitors and threats.[37] Far better to be intentional in the creation of effects from one OE to another than being forces to assess and deal with unintended consequences later.[38]

OE vs IE

Only implied so far in this paper, but an OE presupposes a named operation which comes with legal frameworks that legitimise conducting activities within a bounded zone. Yet the current continuum ranges from peace, to competition, to conflict before armed conflict is reached. An OE is based on a legal framework, be it a Status of Forces Agreement (SOFA), Treaty, Law of Armed Conflict (LOAC) etc., but competition below the threshold of armed conflict does not have a neat delineation and the globally connected IE cannot functionally be contained. This leaves us with the problem of incorporating globalised activities on localised effects, not necessarily supported by LOAC. The replacement in the USG lexicon of the term PSYOPS with MISO is an explicit recognition of this fact.[39] So to is the CAF, and USMC experimentation with OIE superseding IO.[40] Informational activities occur throughout this continuum and importantly are critical to shaping circumstances in the prevention of armed conflict. These baseline activities need a framework as well and artificially limiting the scope and scale ties the CAF's hands whilst its adversaries and competitors have no compunction about targeting social audiences and influencing Canadian and Allied populations with means that do not warrant armed intervention. It is vital that the CAF acknowledge it must compete across the entire spectrum of operation for the "values, attitudes, beliefs,

[37] Joint Chiefs of Staff, "Joint Concept for Operating in the Information Environment (JCOIE)," 20.
[38] McGuffin and Mitchell, "On Domains," 401.
[39] King, "Military Social Influence in the Global Information Environment," 1.
[40] Reese, "Operations in the Information Environment," 36.

and perceptions"[41] of all audiences, both local and abroad.[42] Recommendations along these lines will be captured in the subsequent recommendations paragraph.

Effects Based Approach

"Effects in the physical and informational dimensions of the IE ultimately register an impact in the human cognitive dimension, making it the central object of operations in the IE."[43] The CAF has adopted an effects-based approach to campaign design and operational design.[44] This framework is how the Military instrument fits in with the wider strategic aims in a coherent fashion with the other instruments of national power. The primacy of objectives at the campaign and operational level cannot be overstated. Canadian campaign design builds from the framework of objectives-effects-tasks (OETs).[45] Effects are meaningless without objectives, much in the same way an OE is meaningless without information. With this facet in mind, one can see that the grouping of capabilities and conduct of activities in a domain must at all times be aimed towards a stated objective. Otherwise, the best the Joint Force can hope for is to waste resources in pointless action, at worst it is expending blood and treasure counter purpose to the State's goals and strategy. The previously discussed domains are the spaces that the tasks from the campaign framework take place. It would not make sense to measure the effectiveness of those activities within the same domain, that is the realm of performance measurement. The same, then, applies to information. Further to this, actions taken by actors, audiences, and adversaries in the IE both within and without the OE must be

---

[41] Joint Chiefs of Staff, "Joint Concept for Integrated Campaigning," 4.
[42] Theohary, "Defense Primer: Information Operations," 2.
[43] Joint Chiefs of Staff, "Joint Concept for Integrated Campaigning," 3.
[44] *Canadian Forces Doctrine*, 6–5.
[45] *CFJP 5.0 - The Canadian Forces Operational Planning Process (OPP) Change 2*, B-GJ-005-500/FP-000, 2008, 2–1.

accounted for as well. A global IE, overlaid with one or more OEs ensures that the impacts of interrelated inputs and outputs are not missed.

Recommendations

The previous work has highlighted some needed changes to the CAF perspective on the IE, as well as some issues requiring clarification in doctrine. First, as first brought up in paragraph four, the CAF definition for domain is both incomplete and overly broad. The CAF, through the Joint Terminology panel should adopt a Canadianised version of the NATO definition: "discrete spheres of military capabilities and activities that are applied within the [operating environment] and provide a framework for organizing the military instrument."[46] If this proposal is accepted, then the CAF should also consider codifying and differentiating the following prefixes to domain: pan/all-domain (interchangeable): "Orchestration of military activities, across all domains and environments, synchronised with non-military activities, to enable the [CAF] to deliver converging effects at the speed of relevance. [Note: NATO refers to pan/all-Domain as Multi Domain]"[47] Doctrinally information should remain an environment since information permeates all domains, is unbounded, and cannot be considered discreet. Canada should also consider amending its definition of OE to: "The composite of all military domains within a defined space where military power is exercised, and operations are conducted to achieve objectives." This would solve the tautological problem that makes the current definition so circular. The CAF should also consider onboarding the IE as part of its official lexicon, though remove the "informational layer"

---

[46] *Allied Joint Publication 01, Allied Joint Doctrine Ratification Draft 1 (Edition F Version 1)*, 104.
[47] Ibid., 3.

found in USG sources of the IE with the IE solely consisting of the physical and cognitive. This approach mirrors the direction of the ongoing CFJP 3-10 rewrite at the time this paper was written.[48] Finally, the CAF, in concert with DND, needs to build procedures and recommend policies that respect rule of law and international norms for operating in the IE. This would be the first step in normalising CAF activities that do not fit neatly into LOAC.

Conclusion

In conclusion, it has been demonstrated that information is not an appropriate construct for a domain. Domains are, by definition, bounded constructs that aggregate to form an OE. The OE, being the space that military activities take place in order to achieve objectives needs some kind of construct to analyse and assess its impacts. Add to this, actions taken outside the OE will still have consequences inside of it. Information cannot be bounded, nor would it be helpful to place an artificial boundary to it. Indeed, this paper has demonstrated that the OE is a meaningless concept without the IE tying everything together. The IE then becomes the perfect framework for placing a localised OE inside the global IE. This framework forces military professionals to view the IE holistically which in turn alleviates the tendency to stovepipe capabilities. A globalised IE also provides a convenient medium to measure effects. At all times the application of military power must be toward specific objectives. Without a means to analyse the effects of the inputs and outputs of military actions, as well as those of outside agents, generating true understanding of the OE would be impossible. Canada, its allies, and coalition partners are all working, to one degree or another, on the concept of OIE. There

---

[48] *CFJP3-10 Operations in the Information Environment (OIE) Working Draft 1*.

are challenges both academic and military; and this paper has made some recommendations to improve the study and foster thinking towards a fulsome concept that Canada can apply to meeting the demands of the current security environment.

BIBLIOGRAPHY

Allied Joint Publication 01, Allied Joint Doctrine Ratification Draft 1 (Edition F Version 1). F. Allied Joint Doctrine, AJP-01. NATO STANDARDIZATION OFFICE (NSO), 2020.

CFJP 01 - Canadian Military Doctrine. First. B-GJ-005-000/FP-001. Ottawa, Ontario: Colonel Steven P. Noonan, MSC, CD, 2011. http://www.cfd-cdf.forces.gc.ca/sites/page-eng.asp?page=3391.

CFJP 5.0 - The Canadian Forces Operational Planning Process (OPP) Change 2. B-GJ-005-500/FP-000, 2008.

CFJP3-10 Operations in the Information Environment (OIE) Working Draft 1. CFJP 3-10 2022-xx, 2022. http://collaboration-cjoc.forces.mil.ca/sites/JDoc/SitePages/Home.aspx.

Crimm, Maj Mark. "Can We Please Stop Talking about Domains?" *Defense News*, February 18, 2022. https://www.defensenews.com/opinion/commentary/2022/02/18/can-we-please-stop-talking-about-domains/.

Department of Defense, United States. "STRATEGY FOR OPERATIONS IN THE INFORMATION ENVIRONMENT June 2016," June 2016. https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.

Drohan, Thomas A. "Paper #38. What 'Talk-Fight' Ideologues Understand About Warfare: All-Domain, All-Effects in the Information Environment." *International Center for Security and Leadership*, April 19, 2021. https://securityandleadership.com/paper-38-what-vietnamese-nationalists-understood-taliban-fundamentalists-understand-and-we-do-not-all-domain-all-effects-warfare/.

Ehlers Jr., Robert S., and Patrick Blannin. "Making Sense of the Information Environment | Small Wars Journal," March 3, 2020. https://smallwarsjournal.com/jrnl/art/making-sense-information-environment.

Iasiello, Emilio. "What Is the Role of Cyber Operations in Information Warfare?" *Journal of Strategic Security* 14, no. 4 (January 2021): 72–86. doi:10.5038/1944-0472.14.4.1931.

Joint Chiefs of Staff. "Joint Concept for Integrated Campaigning." Department of Defense, March 16, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257#:~:text=is%20Integrated%20Campaigning.-,The%20JCIC%20defines%20integrated%20campaigning%20as%20Joint%20Force%20and%20interorganizational,and%20duration%20across%20multiple%20domains.

Joint Chiefs of Staff. "Joint Concept for Operating in the Information Environment (JCOIE)." Department of Defense, July 25, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf.

King, Sara B. "Military Social Influence in the Global Information Environment: A Civilian Primer: Military Social Influence." *Analyses of Social Issues and Public Policy* 11, no. 1 (December 2011): 1–26. doi:10.1111/j.1530-2415.2010.01214.x.

Kirschbaum, Joseph W. Information Environment: DOD Operations Need Enhanced Leadership and Integration of Capabilities, § Subcommittee on Cyber, Innovative Technologies, and Information Systems, Committee on Armed Services, House of Representatives. Accessed April 9, 2022. https://www.gao.gov/products/gao-21-525t.

McGuffin, Chris, and Paul Mitchell. "On Domains: Cyber and the Practice of Warfare." *International Journal: Canada's Journal of Global Policy Analysis* 69, no. 3 (September 2014): 394–412. doi:10.1177/0020702014540618.

Porche, Isaac R., Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy Y. Min, and Bruce J. Held. "The Information Environment and Information Warfare." In *Redefining Information Warfare Boundaries for an Army in a Wireless World*, 11–18. RAND Corporation, 2013. https://www.jstor.org/stable/10.7249/j.ctt3fh1qp.10.

Reese, LtCol C Travis. "Operations in the Information Environment." *Marine Corps Gazette*, Ideas and Issues, 104, no. 8 (August 2020): 9.

Strong Secure Engaged - Canada's Defence Policy. Department of National Defence, 2017. https://www.canada.ca/content/dam/dnd-mdn/documents/reports/2018/strong-secure-engaged/canada-defence-policy-report.pdf.

Theohary, Catherine A. "Defense Primer: Information Operations." Primer. Congressional Research Service, December 1, 2021. https://crsreports.congress.gov/product/details?prodcode=IF10771.