National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

INTELLIGENCE PREPARATION OF THE OPERATING ENVIRONMENT: BUILDING TOWARDS A BETTER UNDERSTANDING OF CYBER OPERATIONS

Major Hans La Pierre

JCSP 46

Solo Flight

Disclaimer

PCEMI 46

Solo Flight

Avertissement

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 – PCEMI 46
2019 – 2020

SOLO FLIGHT

INTELLIGENCE PREPARATION OF THE OPERATING ENVIRONMENT: BUILDING TOWARDS A BETTER UNDERSTANDING OF CYBER OPERATIONS

Major Hans La Pierre

Word Count: 5237

Nombre de mots: 5237

INTELLIGENCE PREPARATION OF THE OPERATING ENVIRONMENT – BUILDING TOWARDS A BETTER UNDERSTANDING OF CYBER

In 1968, two American psychologists, J.C.R. Licklider and Robert W. Taylor, posited that computers would evolve beyond their mathematical equation solving purpose to form a globe spanning interconnected constellation focused on capturing and sharing information; the Intergalactic Computer Network.[1] It wasn't until a year later, on 29 October 1969, that the Internet's ancestor, the Advanced Research Projects Agency Network (ARPANET), would be born when a single computer at the University of California in Los Angeles successfully communicated with another one at Stanford University,[2] some five hundred kilometers away. It would take another two decades before the Internet as we currently know it would come to exist, with the invention of the World Wide Web in 1989.[3] Over the following years, the Internet would grow from 3 million users in 1990[4] to 4.13 billion users in 2019.[5] The launch of the Apple iPhone in 2007 further democratized Internet access by mainstreaming mobility.[6] As of 2019, there were over 6 billion mobile broadband subscriptions active worldwide.[7] Today, the Internet serves as the backbone for the world's corporate, industrial, government, public, private, and military networks, linking together an ever-expanding quantity of users and devices. It was estimated that approximately 9.5 billion Internet of Things devices were

---

[1] Peter Singer and Emerson Brooking, *LikeWar: The Weaponization of Social Media* (New York: Houghton Mifflin Harcourt Publishing, 2018), 25-26.

[2] Ibid, 27.

[3] Ibid, 38-39.

[4] Ibid.

[5] J. Clement, "Internet Usage Worldwide – Statistics & Facts", Statista, last modified 25 July 2019, https://www.statista.com/topics/1145/internet-usage-worldwide/.

[6] Singer and Brooking, *LikeWar*, 48.

[7] S. O'Dea, "Number of Active Mobile Broadband Subscriptions Worldwide from 2007 to 2019", Statista, last modified 28 February 2020, https://www.statista.com/statistics/273016/number-of-mobile-broadband-subscriptions-worldwide-since-2007/.

connected at the end of 2019.[8] As the author Peter W. Singer puts it, "[the Internet] has become woven into almost everything we do […]".[9] Indeed, the Internet, or the prophesized Intergalactic Computer Network, has effectively ushered in a new era, one in which the cyberspace – "the element of the operational environment that consists of the interdependent networks of information technology structures […] as well as the software and data that resides within them"[10] - has coalesced into its very own domain comprised of "all infrastructure, entities, users and activities related to or affecting, cyberspace."[11]

Thus, as the operational environment grows with the addition of the cyber domain, our understanding of the latter's implications on military operations must evolve. Indeed, events occurring in cyberspace can have tactical, operational and strategic consequences. For instance, a NATO catfishing[12] experiment conducted during one of its exercises in late 2018 resulted in NATO troops unknowingly disclosing manoeuvre units' locations and troop movements, and even led to desertions.[13] In 2008, the United States Department of Defense discovered its Central Command classified networks, on which detailed planning for its operations in Iraq, Afghanistan, and across the Middle East were being conducted, had been compromised, potentially revealing those plans to its adversaries.[14] Finally, in 2017, Russia's NotPetya malware, meant to target Ukrainian

---

[8] Knud Lueth, "IoT 2019 in Review – The 10 Most Relevant IoT Developments of the Year", IoT Analytics, last modified 7 January 2020, https://iot-analytics.com/iot-2019-in-review/.

[9] Singer and Brooking, *LikeWar*, 24.

[10] Government of Canada, *JDN 2017-02, Canadian Armed Forces Joint Doctrine Note – Cyber Operations* (Ottawa: Canadian Forces Warfare Center, 2017), Chapter 2, 1.

[11] Ibid.

[12] Catfishing is the act of luring someone into a relationship by means of a fictional online persona.

[13] Issie Lapowsky, "NATO Group Catfished Soldiers to Prove a Point About Privacy", Wired, last modified 18 February 2019, https://www.wired.com/story/nato-stratcom-catfished-soldiers-social-media/.

[14] Ellen Nakashima, "Cyber-Intruder Sparks Response, Debate", The Washington Post, last modified 8 December 2011, https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html.

governmental organizations and companies, went rogue and within hours crippled, amongst others, some of the world's biggest commercial shipping companies such as Maersk and TNT Express (FedEx's European subsidiary),[15] which are critical to the global supply chain and on which militaries across the world rely heavily to move troops, supplies and equipment. The impetus for commanders and their staff to understand how cyber affects the overall operating environment in order to employ it to attack an adversary, or to preclude a cyber threat or risk from jeopardizing their mission, has therefore never been higher.[16]

However, is the current Canadian Armed Forces (CAF) Intelligence Preparation of the Operating Environment (IPOE) doctrine, the processes by which a holistic analysis of the operating environment is provided to commanders and their staff, suited to properly analyze the implications of the cyber domain on operations? Moreover, what adaptations, if any, are necessary to properly analyze the cyber aspect of the operating environment? This essay contends that while the CAF IPOE process remains relevant to the analysis of the cyber environment, its outcome suffers from the application of conventional, informational and defensive filters to it, and therefore requires the adoption of a new cyber analytical model as well as the adaptation of current methods in order to properly assess the impacts of the cyber environment on operations.

This essay is separated in three sections. The first will provide a brief overview of the IPOE process. The second will describe how the current CAF doctrine approaches

---

[15] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", Wired, last modified 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[16] Craig Jones, "Demystifying Intelligence Support to Cyber Operations", *Military Intelligence* October-December (2015), 49.

cyber as part of the IPOE and highlight some of its shortcomings. Finally, the third will examine how foreign doctrine, academic and industry literature analyses cyber implications to plans and operations, and offer a way forward for the CAF with regards to the intelligence preparation of the cyber operating environment.

WHAT IS THE IPOE?

The IPOE or the Intelligence Preparation of the Battlefield (IPB), its Army equivalent, have long been the tool of choice to define the operating environment and the interdependencies existing between it, the enemy, friendly, and neutral forces. This section will explain why the IPOE terminology will be the one employed in this essay over its IPB counterpart, set some limitations on the scope of this essay and provide an overview of the IPOE process.

IPOE or IPB?

The IPOE and IPB overall processes are identical and serve the same purpose. The difference lies in the scope of their analysis. While the IPB does account for socio-economic and cultural factors, it focuses primarily on the geospatial analysis of the weather-terrain-enemy trifecta of the operating environment.[17] The IPB is the analytical tool typically adopted by component commanders and their staff.[18] The IPOE, on the other hand, achieves a joint geospatial and systems analysis of the operating environment by integrating all component perspectives, as well as those of multinational and other partners, and a complete Political, Economic, Military, Social, Information and

---

[17] Government of Canada, *B-GL-357-001/FP-001, Land Force Information Operations Field Manual – Intelligence* (Kingston: Canadian Army Doctrine and Training Center, 2001), 71-73.

[18] Government of Canada, *CFJP 2-1.1, Canadian Forces Joint Publication – Intelligence Preparation of the Operational Environment* (Ottawa: Canadian Forces Warfare Center, 2016), Chapter 1, 3-4.

Infrastructure (PEMSII) assessment.[19] Therefore, given the similarity of the processes, and since the IPOE process integrates individual IPBs into its analysis, can be applied throughout the spectrum of conflict and at all levels of warfare (tactical to strategic),[20] this essay will employ the IPOE terminology. However, it should be understood that arguments made herein are also relevant to the IPB process.

A Few Limitations

While the IPOE process both supports and feeds off of other processes, such as the operational planning process or the intelligence cycle, this essay will limit itself to the analysis of cyber considerations in the context of the IPOE process. Further, it won't delve into whether or not Cyber should be recognized as a domain; it is assumed it is one as per CAF doctrine.[21] Finally, it won't address any legal or ethical implications of cyber operations outside of any IPOE implication.

Overview of the IPOE Process

CAF doctrine defines the IPOE as "the analytical process used by intelligence organizations to produce intelligence assessments, estimates, and other intelligence products, in support of a commander's decision-making process."[22] Through the IPOE process, the operating environment – that is the "composite of conditions, circumstances, and influences that affect the employment of capabilities [of friendly, adversary and neutral actors,] and bear on the decisions of the commander"[23] – is continuously analyzed

[19] Ibid, 1.
[20] Government of Canada, *CFJP 2-1.1*, Chapter 1, 8.
[21] Government of Canada, *JDN 2017-02*, Chapter 2, 2.
[22] Government of Canada, *CFJP 2-1.1*, Chapter 1, 1.
[23] Ibid, 2.

following a four step cycle: defining the operating environment, describing its effects, evaluating the enemy, and defining his potential courses of actions.[24]

The first step, defining the operating environment, focuses on identifying the commander's area of operations, as well as analyzing the mission and intent of both the superior and higher commanders in order to ascertain all significant elements which may affect the commander's decisions, or friendly and enemy courses of action (COA).[25] Thereafter, a cursory analysis of all aspects of the operational environment (land, sea, air, space, information, human terrain, etc.[26]) would follow to identify those key elements which may impact the force and its mission, understanding that they will likely extend far beyond the boundaries of the area of operations.[27] Once completed, the areas of influence, intelligence responsibility and interest are established.[28] These are of particular importance as they help guide IPOE efforts by respectively setting the requirements to identify the factors influencing a commander's ability to reach out and touch an adversary outside of his assigned area of operations if required, to develop and share IPOE products, and to continuously monitor enemy, neutral and other activities well outside of the commander's areas of influence and intelligence responsibility.[29] This step culminates with an assessment of currently available intelligence and information, and its sufficiency to conduct the remainder of the IPOE process. Any shortfall is addressed by the development of initial priority information requirements (PIR) to steer intelligence collection efforts, or by the submission of requests for information.[30]

---

[24] Government of Canada, *CFJP 2-1.1*, Chapter 1, 1.
[25] Ibid, Chapter 2, 2-3.
[26] Ibid, Chapter 1, 1.
[27] Ibid, Chapter 2, 3.
[28] Ibid, 4-5.
[29] Ibid.
[30] Ibid, 6-7.

The second step, describing the effects of the operating environment, consists of a detailed assessment of the impacts of the operational environment on enemy, friendly and neutral capabilities and COAs.[31] The conduct of both a geospatial and a systems analysis is necessary in order to properly define and understand the effects of the operating environment on operations.[32] The former allows for the evaluation of all physical, non-physical and locational aspects of the land, sea, air, space and information domains, as well as of other relevant facets of the operating environment such as the electromagnetic spectrum, time, and weather and climate.[33] The latter provides a thorough analysis of Political, Economic, Military, Social, Information and Infrastructure (PEMSII) systems that exist within the operating environment, and the relationships that connect nodes, sub-systems and systems together.[34] In both cases, relevant characteristics of the operating environment are identified along with their likely impact on military operations.[35] The final result of these analyses is a set of assessed and prioritized planning considerations (avenues of approach, key terrain, key system nodes, etc.), and initial enemy COAs necessary to support the planning and development of sound friendly COAs.[36] Various overlay and matrix products that help the commander and his staff understand the impacts of diverse operating environment factors or its makeup are typically developed during this step.[37]

The third step, evaluating the adversary, compares adversarial models, which combine enemy templates depicting doctrinal employment and disposition of forces with

---

[31] Government of Canada, *CFJP 2-1.1*, Chapter 2, 7.
[32] Ibid.
[33] Ibid, 7-36.
[34] Ibid, 36.
[35] Ibid, 7.
[36] Ibid, 44.
[37] Ibid, 7.

a description of preferred doctrinal or historical tactics and a list of high value targets necessary to the execution of the aforementioned templates, with the current adversary situation in order to determine which models are potentially unfolding. This assessment includes the full range of capabilities being brought to bear by the enemy, as well as all limitations to it stemming from previously identified environmental impacts.[38] This step concludes with the identification of the enemy's Centres of Gravity (CoG), which are "the characteristics, capabilities or localities from which [he] derives [his] freedom of action, physical strength or will to fight."[39] Analysis of a CoG's critical capabilities and critical requirements will reveal critical vulnerabilities which the enemy must protect, but which can be exploited with a high return on investment. The exploitation of those key enemy weaknesses become decisive points which friendly plans must achieve.[40]

The fourth and final step of the IPOE process, describing the adversary courses of action, develops a detailed understanding of the enemy's likely intent and strategy.[41] His intent is derived from a holistic evaluation of his current politico-military situation, strategic and operational capabilities, and socio-cultural features.[42] His strategy, on the other hand, is derived from adversarial models previously assessed as plausible and how well they achieve his predefined intent, that is the objectives and end states he pursues. To those should be added any realistic COA which would significantly hinder friendly COAs, regardless of the enemy's ability to deliver on it given current operating environment conditions, and all COAs recently executed by the enemy.[43] Once all

---

[38] Government of Canada, *CFJP 2-1.1*, Chapter 2, 45-52.
[39] Ibid, 53.
[40] Ibid, 56.
[41] Ibid.
[42] Ibid, 57.
[43] Ibid.

credible COAs have been identified, they are prioritized based on their likelihood of occurrence.[44] From this prioritized list are then selected at a minimum the most likely and the most dangerous enemy COAs,[45] which get developed in detail to include a full description of their concept of operations, a graphical illustration of the enemy's force disposition, and key timings, locations, objectives and high value targets.[46] Finally, unique PIRs are defined for each selected COA in order to allow intelligence collection efforts to accurately discriminate the COA being executed from the others.[47]

While gaining a complete understanding of the operating environment is utopic,[48] the J2, through the execution of iterative IPOE analyses and with the active collaboration of the remainder of the staff, subordinate elements, and national and international partners plays an important role in getting commanders as close to it as possible.[49] Understanding how the IPOE process functions is essential to the proper assessment and definition of how the cyber environment should be analysed.

CYBER IN THE CURRENT CAF IPOE DOCTRINE

While the overall CAF IPOE process is logical and comprehensive, it falls short of providing the means to conduct a thorough assessment of the cyber environment. First, it largely eschews the cyber environment, and, when it does consider it, it does so through the same analytical lens with which it approaches the more conventional and physical domains of land, sea, air and space. Second, it nests cyber under the broader information domain, therefore foregoing the fact that cyber can affect more than the will,

---

[44] Government of Canada, *CFJP 2-1.1*, Chapter 2, 58.
[45] Ibid, 58.
[46] Ibid, 59-63.
[47] Ibid, 64.
[48] Ibid, Chapter 1, 11.
[49] Ibid, 2.

understanding and command and control (C2) capabilities of the enemy.[50] Finally, when cyber considerations are broached, they largely revolve around defense and neglect the offensive aspects.

CAF IPOE Doctrine Underprivileges Cyber

In assessing the operating environment, the CAF IPOE doctrine largely glosses over the analysis of the cyber operating environment and offers little to no guidance in conducting it. For example, while it recognizes that the definition of the operating environment, as part of the first step of the IPOE process, is critical to its outcome and mandates that its geospatial elements conform to the World Geodetic System 1984 standard,[51] it offers no analytical model or equivalent output standard for cyber. Further, when defining the significant characteristics of the operating environment, it focuses predominantly on physical aspects of cyber, such as communication infrastructure and the general disposition, capabilities and objectives of the adversary's military and paramilitary forces.[52] While this is useful information, it provides only part of the broad cyber picture.[53] Indeed, much of what matters is not physical, but virtual. An incomplete general representation of the key cyber characteristics at this point will affect the definition of the commander's area of interest, as well as waste precious time in obtaining relevant intelligence to answer cyber PIRs[54] that would otherwise have been identified at

[50] Government of Canada, *CFJP 3-10, Canadian Forces Joint Publication – Information Operations* (Ottawa: Canadian Forces Warfare Center, 2015), Chapter 1, 5-6.
[51] Government of Canada, *CFJP2-1.1*, Chapter 2, 2.
[52] Ibid, 4.
[53] Jones, 'Demystifying Intelligence', 49.
[54] Dennis Katolin, "Cyber in the Single Battle: Antiquated Operational Models Need to Change", *Marine Corps Gazette* February (2020), 52.

this stage instead of later or possibly too late. In war, time is seldom available in excess. Again, this highlights the need for an adapted analytical model for cyber.[55]

The second step of the IPOE, which concerns itself with the detailed definition and analysis of the characteristics of the operating environment and their effects on adversary, friendly and neutral capabilities and COAs, actually puts forth some explicit and relevant considerations concerning the cyber domain.[56] However, it also remains fraught with issues. While the remainder of these problems will be covered later in this section, it is sufficient at this point to highlight that the detailed analysis of cyber considerations and of their effects on military operations remains conditional to the application of a geospatial lens to the operating environment. Indeed, CAF IPOE doctrine calls for the application of a geospatial perspective, as it "supports all views of the operational environment",[57] with the analysis of the operations area taking precedence over that of the area of interest.[58] Such an analytical approach based on physical location associations[59] is ill suited to the analysis of a domain which is global, where the nature of terrain is transient, and where time is largely irrelevant in the sense that, if cyberspace was linear, an event occurring at one end of it can have a near-instantaneous effect at its opposite end.[60] This space-time compression is what has recently pushed some academics, such as Dr. Barney Warf, professor at Kansas University, who highlighted

---

[55] Antoine Lemay, Scott Knight and Jose Fernandez, "Intelligence Preparation of the Cyber Environment (IPCE): Finding the High Ground in Cyberspace", *Journal of Information Warfare* 13, no. 3 (2014), 142.

[56] Government of Canada, *CFJP2-1.1*, Chapter 2, 22-27.

[57] Ibid, 7.

[58] Ibid, 8.

[59] "Meaning of Geospatial in English", Lexico, last accessed 6 May 2020, https://www.lexico.com/en/definition/geospatial.

[60] Government of Canada, *JDN 2017-02*, Chapter 2, 5.

that in the age of cyber "the friction of distance […] has diminished greatly"[61] and that "cyberwar generates new geographies of conflict that defy conventional Westphalian understandings"[62], to stress the development and application of alternate analytical models for cyber.

Finally, steps three and four of the CAF IPOE, respectively focused on evaluating the adversary and developing his COAs, while requiring some adaptions to account for cyber specificities which the document ignores (to be covered in the next section), remain conceptually sound and applicable to the assessment of cyber threats and the development of cyber, or general, enemy COAs.[63]

A Case of Subordination?

As previously stated, there are multiple issues with CAF IPOE cyber analysis methodologies, specifically within the second step of the process. The first one concerned the lack of an appropriate analytical model to identify and study the impacts of the cyber domain on adversary, friendly and neutral military operations. The second one is the subordination of cyber environment considerations under the broader umbrella of the information domain.[64] The information domain is defined as "the information itself, the individuals, organisations and systems that receive, process, and convey the information and the cognitive, virtual and physical space in which this occurs"[65] and is interdependent with cyberspace and the cyber domain.[66] The concern here is not whether cyber

---

[61] Barney Warf and Emily Fekete, "Relational Geographies of Cyberterrorism and Cyberwar", *Space and Polity* 20, no. 2 (2016), 154.
[62] Ibid, 145.
[63] Lemay, Knight and Fernandez, 'Intelligence Preparation of the Cyber Environment', 143.
[64] Government of Canada, *CFJP2-1.1*, Chapter 2, 22-27.
[65] Government of Canada, *CFJP 3-10*, Chapter 1, 1.
[66] Government of Canada, *JDN 2017-02*, Chapter 2, 1.

environment characteristics should be included in the impact analysis of the information environment on, information or otherwise, operations; they absolutely must be.[67] Rather, it is that by defining and evaluating cyber characteristics solely through the prism of the information environment and information operations, one risks inadvertently overlooking other relevant aspects of the cyber environment. This particular issue of subordination has also been noted as problematic by Jeffrey Caton, president of Kepler Strategies, a think tank focused on national security and cyberspace theory, in his analysis of NATO cyber strategy and policy.[68] Indeed, while information operations seek to affect the adversary's ability to make decisions,[69] cyber operations can be used for more than influencing the enemy's will, understanding or capability required to do so. For example, the analysis of key cyber environment characteristics and of their impacts could lead to deductions concerning opportunities for the enemy to spy on us, or for us to hijack some of his weapons platforms.[70] Neither, in and of itself, has much to do with one's ability to make decisions. Therefore, while the CAF IPOE doctrine includes relevant considerations pertaining to physical (computer hardware and networks) and informational (computer software, data, procedures and human operators) characteristics of the cyber environment,[71] it should not negate the requirement for a comprehensive analysis of the cyber environment's characteristics beyond its intersectionality with its information counterpart.

---

[67] Ibid, Chapter 4, 1.

[68] Jeffrey Caton, *NATO Cyberspace Capability: A Strategic and Operational Evolution* (n.p.: Strategic Studies Institute, U.S. Army War College, 2016), 18-19.

[69] Government of Canada, *CFJP 3-10*, Chapter 1, 5-6.

[70] Government of Canada, *JDN 2017-02*, Chapter 4, 1.

[71] Government of Canada, *CFJP2-1.1*, Chapter 2, 22-24.

What About Cyber Offense?

The third and final issue lies with the fact that CAF IPOE cyber considerations seem to cater disproportionately to cyber defense concerns (i.e. what the enemy can do to us). Indeed, much of the language surrounding the analysis of cyber considerations in step two of the CAF IPOE process is specific to the risk of the enemy leveraging certain characteristics against friendly forces,[72] going so far as proposing mitigating solutions.[73] This issue is not new, nor specific to CAF IPOE doctrine. Dr. Aaron Brantly, assistant professor of political science at Virginia Tech, notes that the much of the literature surrounding cyber vulnerabilities tends to focus more on safeguarding against them than understanding them, thus overshadowing offensive opportunities with defensive considerations.[74] That is not to say that no consideration is given to the impacts of the cyber environment on adversarial and neutral parties. The CAF IPOE doctrine does mention that " the effects of the [cyber] environment should be analyzed to consider how significant characteristics affect friendly, neutral and adversary capabilities and broad COAs."[75] However, the application of this statement seems to be lost on much of the discourse and the provided examples in this section. An impartial analysis of the characteristics of the cyber environment and of their potential effects on the operations of

[72] Government of Canada, *CFJP2-1.1*, Chapter 2, 22-27.
[73] Ibid, 24.
[74] Aaron Brantly, "Defining the Role of Intelligence in Cyber: A Hybrid Push and Pull", in *Studies in Intelligence: Understanding the Intelligence Cycle*, ed. Mark Phythian (New York: Routledge, 2013), 89.
[75] Government of Canada, *CFJP2-1.1*, Chapter 2, 25.

all is required in order to illuminate both defensive requirements and offensive opportunities which could be leveraged by adversary and friendly forces.

Thou Shall be Forgiven… Not

The CAF IPOE doctrine might be forgiven its previously described shortcomings, given that it would typically integrate component IPB products,[76] to include cyber, into its analysis of the operating environment. Unfortunately, component IPB doctrine is even less evocative on the subject. An investigation of Canadian Army doctrine, to include the Intelligence Field Manual,[77] Signals in Support of Land Operations - Principles and Fundamentals,[78] Command Support in Land Operations[79] and Staff Duties for Land Operations[80] doctrines has failed to reveal anything relevant about the analysis of the cyber environment. Perhaps understandably so, as they date back from 2001, 2009 and 2008 (last two documents) respectively, and are therefore wholly outdated from a cyber perspective. Much more concerning though is the fact that the CAF Joint Doctrine Note on Cyber Operations does not offer any cogent explanation as to what the IPOE for cyber should entail, simply stating that it is to "be developed".[81]

In summary, CAF IPOE doctrine approaches the analysis of the cyber environment in a limited manner and applies to it a conventional, informational and defensive perspective which would likely result in the inadequate assessment of its

---

[76] Government of Canada, *CFJP2-1.1*, Chapter 1, 4.
[77] Government of Canada, *B-GL-357-001/FP-001*, n.p.
[78] Government of Canada, *B-GL-351-001/FP-001, Signals in Support of Land Operations - Principles and Fundamentals* (Kingston: Canadian Army Doctrine and Training Center, 2009), n.p.
[79] Government of Canada, *B-GL-331-001/FP-001, Land Force - Command Support in Land Operations* (Kingston: Canadian Army Doctrine and Training Center, 2008), n.p.
[80] Government of Canada, B-GL-331-002/FP-001, Staff Duties for Land Operations (Kingston: Canadian Army Doctrine and Training Center, 2008), n.p.
[81] Government of Canada, *JDN 2017-02*, Chapter 4, 21.

impact on operations. Therefore, a holistic assessment of the cyber environment's characteristics, conducted through the application of a relevant analytical model and encompassing both offensive and defensive considerations, is necessary in order to ensure their impacts on adversary, friendly and neutral operations are fully identified and understood. Further, given the scarcity of information available from supporting doctrine pertaining to what a cyber IPOE should entail, we must look elsewhere to find answers as to how to properly analyze the cyber environment.

A WAY FORWARD

From what has been covered so far in the previous sections, we can make the following observations. First, it is clear that a new analytical model adapted to cyber's unique nature is required to properly represent and evaluate considerations stemming from this newer environment's key characteristics. Second, the IPOE process consists of two interdependent, yet distinctive, sub-processes. The first, comprised of the first two steps, seeks to define the operating environment and assess its potential impacts on adversary, friendly and neutral operations. The second, comprised of the last two steps, focuses on defining the adversary and developing his plausible COAs. Each of these sub-processes therefore requires different considerations. This section will seek to define, through foreign doctrine, academic and industry literature, what such an alternate analytical model could be and what those considerations are, in order to propose a more comprehensive way forward for the analysis of the Cyber operating environment.

Alternative Cyber Analytical Models

In seeking an alternative to the purely geospatial analysis model promulgated by the CAF IPOE doctrine, one can look to the U.S. Army's Operational Framework.[82] Through the application of this model, the analysis of the various operating environments (to include cyber) is not only framed within their physical and temporal aspects (e.g. weapons ranges and effects in time and space), but also within their cognitive and virtual aspects (e.g. decision making processes, cyber posture, etc.). However, by its own admission, the execution of the IPOE within this framework, although providing for a more holistic assessment of the characteristics and effects of each operating environment on overall military operations, remains "[…] both geographically and temporarily specific."[83] Another plausible option can perhaps be found in the relatively nascent field of relational geography.

Exposure to the media's oversimplification of cyber operations, in a bid to render their concept accessible to their target audiences, has led us to perceive them as simply attacking or defending networks.[84] This view is however limited. Cyber-attacks, by virtue of dissolving boundaries separating civil and military affairs, state and non-state actors, foreign and domestic issues, and war and peace,[85] embody the "[…] ongoing collision between Cartesian space and the emerging relational topologies […]."[86] Relational geographies are constantly built and re-built, unevenly interconnecting people, things and

[82] Department of the Army, *ATP 2-01.3, Army Techniques Publication – Intelligence Preparation of the* Battlefield (Washington, DC: Army Publishing Directorate, 2019), Chapter 1, 14.
[83] Ibid.
[84] Jones, 'Demystifying intelligence', 49.
[85] Warf and Fekete, 'Relational Geographies of Cyberterrorism', 146.
[86] Ibid.

spaces[87] in times, influenced by ever changing dynamics and patterns.[88] Space, or geography, in this case is not only an objective or tangible location, surface or container, but a set of relations that are in constant flux and which frame where activities occur.[89] In this context, cyber exhibits a "[…] capillary character that is never captured by the notions of levels, layers, territories, spheres, categories, structures, or systems."[90] This highlights the fact that, although not addressed so far, the conduct of a systems analysis of PEMSII factors, which CAF[91] and US Army[92] IPOE doctrine both call for, would, even when combined with the results of its geospatial counterpart, fail to provide a truly comprehensive understanding of the cyber domain.

Knowing where cyber actors are physically may have no bearing on knowing where they are in cyberspace, and knowing where they may be in cyberspace at any given time does not preclude them from being elsewhere simultaneously, or by virtue of what they are doing being somewhere entirely different the very next second. New concepts of cyber spatiality, so that their analysis through careful "juxtapositions, comparisons and sequences [may] highlight key spatial and temporal processes", are therefore required.[93] Such a relational geography approach to the analysis of the cyber environment would not only serve to address the preponderant tendency of the IPOE process to focus on objective geography, but also help reveal new cyber threats and opportunities.[94]

---

[87] Warf and Fekete, 'Relational Geographies of Cyberterrorism', 146.

[88] Allison Hui and Gordon Walker, "Concepts and Methodologies for a New Relational Geography of Energy Demand: Social Practices, Doing-Places and Settings", *Energy Research & Social Science* 36 (2018), 28.

[89] Ibid, 21-22 & 28.

[90] Warf and Fekete, 'Relational Geographies of Cyberterrorism', 146.

[91] Government of Canada, *CFJP2-1.1*, Chapter 2, 36-44.

[92] Department of the Army, *ATP 2-01.3*, Chapter 4, 22-29 & Annex D, 5-9.

[93] Warf and Fekete, 'Relational Geographies of Cyberterrorism', 147.

[94] Hui and Walker, 'Concepts and Methodologies for a New Relational Geography of Energy Demand', 28.

However, contrary to how we ought to look at things in cyberspace, what we ought to look at has been fairly well defined. Thus, let us consider the cyber environment's key characteristics, and aspects thereof, which should be analyzed as part of the CAF IPOE process.

Defining Key Cyber Characteristics and Considerations

In defining the key adversary, friendly and neutral features of the cyber environment, part of steps one and two of the IPOE process, U.S. Army doctrine leverages the three layers of cyberspace, namely its physical, logical and personae layers.[95] The physical layer is comprised of the hardware, infrastructure and connecting equipment, as well as their related policies and procedures.[96] To this should be added essential elements relating to the Electromagnetic Spectrum (EMS)[97] and the power generation necessary to the operation of this equipment.[98] The logical layer, for its part, includes those elements, such as websites, logical network topologies and configurations, etc.,[99] which are abstractedly related to one another and may bear little to no relation to the network's physical structure.[100] Finally, the personae layer focuses on virtual actors and how they relate to real individuals or organisations,[101] as well as how they interact with each another, and with the network.[102] Such an approach allows for a thorough definition of the key characteristics of the cyber environment, and is coherent with

---

[95] Department of the Army, *ATP 2-01.3*, Annex D, 2.
[96] Ibid.
[97] Danish Defence, *Joint Doctrine for Military Cyberspace Operations* (Copenhagen: Royal Danish Defence College, 2019), 7.
[98] Katolin, 'Cyber in the Single Battle', 53.
[99] Department of the Army, *ATP 2-01.3*, Annex D, 2-3.
[100] Jones, 'Demystifying intelligence', 50.
[101] Department of the Army, *ATP 2-01.3*, Annex D, 3.
[102] Jones, 'Demystifying intelligence', 50.

numerous other doctrines, such as Denmark's Cyber Operations doctrine.[103] Most important, however, is that it matches how Canada's own Cyber Operations doctrine divides cyberspace.[104]

In step two of the IPOE process, U.S. Army doctrine calls for the adaptation of the traditional Weather-Enemy-Terrain (WET) method in order to draw relevant considerations from the cyber characteristics.[105] *Weather* considers the impact of events such as solar storms and blizzards on the components of the physical layer and the EMS.[106] *Enemy* provides a general description of the various cyber threat actors, to include their composition, location(s) and capabilities.[107] Finally, *terrain* provides an assessment of those factors which may help or hinder one's freedom of manoeuvre and situational awareness, enemy or friendly, in cyber space. Such considerations may include the use of encryption, the presence of intrusion detection and protection systems, physical and logical chokepoints, etc.[108] An alternative to the WET method is the cyber specific Traffic-Adversary-Network (TAN) technique put forward by Antoine Lemay, chief scientific officer of Cyber Defence Corporation, et al.[109] While *adversary* and *network* respectively refer to the *enemy* and *terrain* components of the WET procedure, *traffic* more closely resembles virtual weather and focuses on changes in network traffic compositions, volumes and patterns in order to assess potential abnormal activity,

[103] Danish Defence, *Joint Doctrine for Military Cyberspace Operations*, 7.
[104] Government of Canada, *JDN 2017-02*, Chapter 2, 2-4.
[105] Department of the Army, *ATP 2-01.3*, Annex D, 4-5.
[106] Ibid, 9.
[107] Ibid, Chapter 4, 2-4.
[108] Ibid, Annex D, 5.
[109] Lemay, Knight and Fernandez, 'Intelligence Preparation of the Cyber Environment', 142-143.

concealment opportunities, etc.[110] TAN therefore calls for the systematic baselining[111] of key networks as initial requests for information.[112] Thus, by adapting the conventional WET method, which is well established within CAF doctrine,[113] to the cyber environment, and adding to it an additional component of *traffic* (WET2), a comprehensive assessment of the key cyber characteristics and their related considerations can be achieved.

Developing Cyber Adversarial Models

Evaluating the enemy, the third step of the IPOE process, is complicated by the fact that knowledge of the adversary's cyber doctrine may be limited, inaccurate, or simply non-existent, for most cyber threat actors.[114] This makes developing relevant adversarial models and adversary templates, which are crucial to developing plausible opponent COAs, challenging. In order to overcome this issue, the U.S. Army doctrine employs the Cyber Kill Chain (CKC) process.[115] By comparing each of the seven steps of the process[116] with an attributed and documented incident report,[117] or by simply wargaming it against one's own systems, it is possible to gain a generalized understanding of how a given cyber threat actors would proceed to achieve a given offensive objective.[118] An analysis of documented incident reports may also reveal

---

[110] Ibid.

[111] A baseline is the precise measurement of a network's operating parameters, including traffic levels and patterns, at a precise moment in time, and against which future measurements can be compared to detect variations and guide analysis to explain them.

[112] Steven Winterfeld, *Cyber IPB* (n.p.: SANS Institute, 2001), 5.

[113] Government of Canada, *CFJP2-1.1*, Chapter 2, 7-12.

[114] Lemay, Knight and Fernandez, 'Intelligence Preparation of the Cyber Environment', 143.

[115] Department of the Army, *ATP 2-01.3*, Annex D, 11.

[116] The seven steps of the Cyber Kill Chain are; reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objective.

[117] Lemay, Knight and Fernandez, 'Intelligence Preparation of the Cyber Environment', 143.

[118] Department of the Army, *ATP 2-01.3*, Annex D, 11.

specific or trends in enemy cyber Techniques, Tactics and Procedures (TTP), and capabilities. Finally, once the enemy most likely and most dangerous COAs have been fully developed, as part of step four of the IPOE process, previously measured friendly and neutral networks baselines can be used to create COA specific PIRs.[119] By doing so, discrepancies between baseline and current networks operating parameters measurements can help determine which COA the enemy is actively pursuing.[120]

Thus, by adapting conventional techniques and adopting new ones it is possible to better integrate the analysis of the cyber environment within the CAF IPOE process and bring value added to its overall outcome. Analyzing the cyber environment's key characteristics, determined through its physical, logical and personae layers, and relevant considerations, stemming from the application of the WET2 technique, through an appropriate cyber analytical model, such as the Operational Framework or one based on relational geography, allows for both the proper definition of the cyber operating environment and evaluating its effects on enemy, friendly and neutral operations. Moreover, applying the CKC process and leveraging the output of the WET2 method enables both the development of enemy COAs and the creation of COA specific indicators. While in no way *the* solution, the aforementioned proposals offer *a* way forward in ensuring a comprehensive analysis of the cyber environment in support of the CAF IPOE process.

[119] Lemay, Knight and Fernandez, 'Intelligence Preparation of the Cyber Environment', 145.
[120] Lemay, Knight and Fernandez, 'Intelligence Preparation of the Cyber Environment', 147.

CONCLUSION

Doctrine should never become so prescriptive that it prohibits commanders and their staff to think critically and creatively. War, after all, remains an art.[121] But, neither should it be devoid of purpose and utility in guiding and shaping their analytical thought process in support of intelligence collection, operations planning and decision making. Thus, in an era characterized more than ever by the compression of time and space, and the emergence of abstract geographies, a new perspective framing the CAF's IPOE analysis of the cyber environment is required. While the current CAF IPOE doctrine largely pays lip service to the cyber environment by seeing it as an adjunct element to the more conventional domains of land, sea, air and space, and to the information environment, as well as considering it almost entirely from a defensive vantage point, this state of affairs can be rectified. Analytical models, such as the Operational Framework or one based on relational geography, and various methods, such as WET2 and CKC, can provide a more relevant perspective and be harnessed within the existing CAF IPOE process framework. In doing so, a comprehensive analysis of the cyber environment can be achieved in order to ascertain its effects on enemy, friendly and neutral operations, both offensive and defensive. Moreover, better integrating the analysis of the cyber environment into the CAF IPOE process would enhance its overall outcome and serve to make it greater than the sum of its parts. Indeed, one who knows both his enemy and his self needs not fear the outcome of a hundred battles.[122] In parting, the application of relational geography to the analysis of the cyber environment, specifically in the

---

[121] Sunzi and Lionel Giles, *The Art of War* (Mineola: Dover Publications, 2002), 59.

[122] Sunzi and Giles, *The Art of War,* 51.

development of methodologies which could be leveraged within the CAF IPOE process, is an area which likely merits further research.

BIBLIOGRAPHY

Brantly, Aaron. 2013. "Defining the Role of Intelligence in Cyber: A Hybrid Push and Pull." In *Studies in Intelligence: Understanding the Intelligence Cycle*, by Mark Phythian, 90-112. New York: Routledge.

Caton, Jeffrey L. 2016. *NATO Cyberspace Capability: A Strategic and Operational Evolution.* Strategic Studies Institute, U.S. Army War College.

Clement, J. 2019. *Internet Usage Worldwide - Statistics & Facts.* July 25. Accessed May 6, 2020. https://www.statista.com/topics/1145/internet-usage-worldwide/.

Coviello, Katherine R. 2019. "The History of Intelligence Preparation of the Battlefield as We Consider Multi-Domain Operations and Cyberspace." *Military Intelligence* (October-December): 33-36.

Danish Defence. 2019. *Joint Doctrine for Military Cyberspace Operations.* Copenhagen: Royal Danish Defence College.

Department of the Army. 2019. *ATP 2-01.3, Army Techniques Publication - Intelligence Preparation of the Battlefield.* Washington, DC: Army Publishing Directorate.

Government of Canada. 2008. *B-GL-331-001/FP-001, Land Force - Command Support in Land Operations.* Kingston: Canadian Army Doctrine and Training Center.

—. 2008. *B-GL-331-002/FP-001, Staff Duties for Land Operations.* Kingston: Canadian Army Doctrine and Training Center.

—. 2009. *B-GL-351-001/FP-001, Signals in Support of Land Operations - Principles and Fundamentals.* Vol. 1. Kingston: Canadian Army Doctrine and Training Center.

—. 2001. *B-GL-357-001/FP-001, Land Force Information Operations Field Manual - Intelligence.* Kingston: Canadian Army Doctrine and Training Center.

—. 2016. *CFJP 2-1.1, Canadian Forces Joint Publication - Intelligence Preparation of the Operational Environment.* Ottawa: Canadian Forces Warfare Center.

—. 2015. *CFJP 3-10, Canadian Forces Joint Publication - Information Operations.* Ottawa: Canadian Forces Warfare Center.

—. 2017. *JDN 2017-02, Canadian Armed Forces Joint Doctrine Note - Cyber Operations.* Ottawa: Canadian Forces Warfare Center.

Greenberg, Andy. 2018. *The Untold Story of NotPetya, the Most Devastating Cyberattack in History.* August 22. Accessed May 6, 2020. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Hui, Allison, and Gordon Walker. 2018. "Concepts and Methodologies for a New Relational Geography of Energy Demand: Social Practices, Doing-Places and Settings." *Energy Research & Social Science* 36: 21-29.

Jones, Craig. 2015. "Demystifying Intelligence Support to Cyber Operations." *Military Intelligence* (October-December): 49-51.

Katolin, Dennis W. 2020. "Cyber in the Single Battle: Antiquated Operational Models Need to Change." *Marine Corps Gazette* (February): 51-55.

Lapowsky, Issie. 2019. *NATO Group Catfished Soldiers to Prove a Point About Privacy.* February 18. Accessed February 3, 2020. https://www.wired.com/story/nato-stratcom-catfished-soldiers-social-media/.

Lemay, Antoine, Scott Knight, and Jose Fernandez. 2014. "Intelligence Preparation of the Cyber Environment (IPCE): Finding the High Ground in Cyberspace." *Journal of Information Warfare* 13 (3): 46-56.

Lobdell, Terri M. 2019. "Aligning Intelligence Preparation of the Battlefield Doctrine with Current Threat." *Military Intelligence* (July-September): 26-28.

Lueth, Knud L. 2020. *IoT 2019 in Review - The 10 Most Relevant IoT Developments of the Year.* January 7. Accessed May 6, 2020. https://iot-analytics.com/iot-2019-in-review/.

Malpas, Jeff. 2012. "Putting Space in Place: Philosophical Topography and Relational Geography." *Environment and Planning D: Society and Space* 30 (2): 226-242.

Morris, Victor R. 2017. "Complex Intelligence Preparation of the Battlefield in Ukrainian Antiterrorism Operations." *Military Review* (January-February): 58-65.

Nakashima, Ellen. 2011. *Cyber-Intruder Sparks Response, Debate.* December 8. Accessed February 11, 2020. https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html.

O'Dea, S. 2020. *Number of Active Mobile Broadband Subscriptions Worldwide from 2007 to 2019.* February 28. Accessed May 6, 2020. https://www.statista.com/statistics/273016/number-of-mobile-broadband-subscriptions-worldwide-since-2007/.

Oxford Dictionary. n.d. *"Meaning of Geospatial in English".* Accessed May 6, 2020. https://www.lexico.com/definition/geospatial.

Singer, P.W., and Emerson T. Brooking. 2018. *LikeWar: The Weaponization of Social Media.* New York: Houghton Mifflin Harcourt Publishing.

Sunzi, and Lionel Giles. 2002. *The Art of War.* Mineola: Dover Publications.

Warf, Barney, and Emily Fekete. 2016. "Relational Geographies of Cyberterrorism and Cyberwar." *Space and Polity* (Routledge) 20 (2): 143-157.

Winterfeld, Steven P. 2001. *Cyber IPB.* Global Information Assurance Certification Paper, SANS Institute.