National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Lieutenant-Colonel Marc Gallant

Informing Canadian Information Operations

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

Lieutenant-Colonel Marc Gallant

Informing Canadian Information Operations

INFORMING CANADIAN INFORMATION OPERATIONS

Introduction

Information Operations (Info Ops) is defined in Canadian doctrine as 'a military function that plans and coordinates military activities to create desired effects focused primarily in the cognitive domain' (CFJP 3.0 Operations 2011, 1-7). Less fulsome than the NATO definition[1] utilized by Info Ops practitioners in multinational settings, our definition serves well to inform the new initiate on the scope of Info Ops. The qualifier of this being that it is a military function pertaining to military activities shows the Canadian Armed Forces (CAF) has not kept pace with the changing reality of the global environment. Post Afghanistan conflicts introduced us to hybrid and grey zone activities, with adversaries utilizing all elements of DIME/JIMP[2] power to influence audiences. CAF doctrine and activities are moving on from the COIN focus of Afghanistan but have not yet fully coordinated themselves to address current global challenges.

To observe and to orient to the evolving adversarial information environment, this paper will examine Russian hybrid approach to conflict, including the strengths and weakness of their whole of government style of Info Ops. A review of Info Ops in the CAF will lay bare some challenges our current decision makers face when planning at the operational and strategic level. The evolution of current friendly capabilities should provide ample discussion for the remainder of the paper, the intent of which is to offer

---

[1] From AJP 3.0 Information operations is a military function to provide advice and coordinate military information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and other North Atlantic Council approved parties in support of Alliance mission objectives. Information activities are actions designed to affect information and or information systems and can be performed by any actor and include protective measures.

[2] DIME/JIMP – Diplomatic, Information, Military, Economic / Joint Interagency Multinational Public

suggestions to improve and match CAF capabilities with the current global information environment.

The ease of movement within the information environment shapes today's global conflicts. Geographic borders are no boundary to information. The CAF must transition away from Info Ops in a Task Force styled employment strategy focused at operational and tactical levels in an expeditionary context, consistent with their experience in Afghanistan, into a persistent Info Ops presence in all activities. That was our last war. Canada is obliged to engage in operational and strategic activities within the global environment and Info Ops is a vital component of such activities, particularly defensive activities to shield itself and allies from adversarial information campaigns. Instead of teaching an old dog new tricks, the CAF must follow the adage 'form follows function'. If the CAF wants to be a key player in the Government of Canada's comprehensive approach to global engagement, it must adopt a holistic approach to Information Operations that indoctrinates leaders early. The CAF must build and integrate a robust, permanent Info Ops into its structure and everyday operations, across the spectrum of conflict, if it is to be a meaningful contributor to Canadian sovereignty[3].

Gerasimov's New Warfare

Orienting CAF Info Ops demands understanding of one's adversaries, which in the case of Russia, is best observed in General Gerasimov's new focus on political warfare. Gerasimov wrote that 'the very rules of war have fundamentally changed. The role of nonmilitary means of achieving political and strategic goals has grown' (McKew

[3] While Strong Secure and Engaged acknowledges the challenges of Grey Zone and Hybrid Warfare (pg 53) it offers no direction or priority in addressing these issues.

2017). This is the merger of political, business, media, conventional and asymmetrical warfare with a heavy reliance on propaganda tools. Our understanding of conflict leans towards two norms. First, during our two world wars, the apparatus of the state was laser focused on the war effort, including the civilian population and all industry. Essential the mobilization of the entire nation. Conversely, in more conventional state on state conflicts, the populations and institutions of involved states move through their daily lives mostly independent of the conflict, typified in western expeditionary warfare in Afghanistan and Iraq. In Gerasimov's doctrine, we have a blurring of the traditional lines, with arguably civilian institutions coherently shaping the conflict environment as agents of the state, while the citizenry is an uninvolved audience. The Gerasimov doctrine assumes a perpetual state of conflict below the threshold of war, with 4:1 ratio of nonmilitary to military measures (Blagovest Tashev 2019, 133), suggesting a non-kinetic main effort.

Russian information warfare works in two ways, information-technical and information-psychological (Thomas 2020, 7). We will focus on information-psychological, those actions designed to influence target audiences in the cognitive dimension. In the Russian model, construction of fake news, disinformation and propaganda are not military activities only. In this case, whole of government is better termed a whole of society approach. Consider Internet Research Agency, a company organized by Russian oligarch and associate of Putin, Yevgeniy Progozhin, also the owner of the Wagner Group. Ostensibly a private company, Internet Research Agency, is a well-known bot farm responsible for creating and distributing social media propaganda. It is this 'civilian' company that has a history of propaganda in the Baltics (Bills 2020) as

well as contributing to interfering with the US 2016 election (National Intelligence Council 2017, 4) resulting in their indictment in 2018 (United States of America 2018).

Within a whole of society approach, Russian information operations tactics include the 'big lie', reflexive control, and simply saturating targets with disinformation. Activities are aimed not just at military targets, but civilian populations of adversarial nations. The common theme amongst these techniques is to sow confusion among your adversaries. The big lie is typified in the Ukraine, examples including the Russian denial of association with the shooting down of Malaysian Airways Flight 17, or the non-affiliation of the 'little green men' during annexation of Crimea (Thomas 2020, 25). This is frequently followed by an alternate explanation, that attempts to shift responsibility, often only an allegation without accompanying substance. Reflexive control is a more deliberate process that causes an adversary to voluntarily choose the actions most advantageous to Russia, by shape an adversary perception of the situation decisively (Snecovaya 2015, 7). The Russian technique of saturating the information environment with multiple disinformation statements, then follow up on those that find purchase with target audiences appears quite prevalent. Having been referred to as the 'Firehose of Falsehood' (Matthews 2016, 1) this method is rapid, continuous, potentially entertains, with an intent of overwhelming an adversary looking for truth in a sea of fictions. Russia's 2014 annexation of the Crimea has made full use of these grey zone warfare techniques, both militarily and from their civilian sources. Prominent was the narrative of the uprising of the diaspora as a justification for annexation. The presence of a variety of sources for the same propaganda helps create an optic of credibility (Matthews 2016, 3).

Russia would have the world believe the West is to blame for all ills and pushes its 'complex approach/new generation war' as a defensive response to Western aggression. This current Ukraine conflicts shows faults with the Russian Information Warfare process. In 2014 reflexive control and a lack of attribution provided the West with an attractive noninterference option to avoid responding to the annexation of the Crimea. Today's Ukraine conflict is filled with direct refutation of Russian disinformation by the West. A fast intelligence cycle and public revelations of Russian information activities including proposed false flag activities (Alba 2022) is stripping the anonymity which Russia has long relied upon. The tactics and techniques working for the West in their support of Ukraine is the policy analyst's adage of 'speaking truth to power'. Here power lies in public opinion and the West is tearing through the Russian firehose of disinformation.

Information Operations: A Brief Primer

Ironically, the realm of Info Ops is filled with misinformation for the non-practitioner. A review of Info Ops is essential to orient ourselves to the information environment. Canadian Info Ops is not a command activity, in that the Information Operations Officer has no subordinates under their authority. Info Ops can be visualized as a planning and synchronization activity between kinetic and non-kinetic military actions. The Info Ops Officer layers and integrates the Information Related Capabilities (IRC) into the Commanders plan, preventing information fratricide and utilizing information activities to create desired effects in support of CAF objectives. The Info Ops Officer must be well versed in the Operational Planning Process, contribute to the

targeting cycle, and be prepared to translate the non-kinetic StratCom messaging into recommendations for operational level tasks.

See EMAILED copy of paper for submission with diagram for figure 1.

Figure 1: Information Operations Diagram as provided to candidates on the CAF Information Operations Officer Course showing how the Planner integrates IRCs into the Comd Msn in support of GoC Strategic Objectives. Source CAF Info Ops Course.

Often the uninitiated conflate Info Ops solely with cyber warfare or PSYOPS, as these are mentioned most prevalently in mainstream media. CAF Info Ops Information Related Capabilities (IRC) are show in figure 1, and include Cyber, PSYOPS, CIMIC, Public Affairs, EW as well as Deception, PPP[4], Engagements and Physical Destruction. Info Ops works within an effects framework, where strategic level objectives are met through operation level effects achieved by tactical level tasks. Mutually supporting effects are key and are achieved through synchronizing activities among the IRC. As an example, Info Ops conducted in OP REASSURANCE creates changes in the will, understanding and capability of the approved targets, as part of the NATO narrative of unity and 'demonstrating the strength of the transatlantic bond' (North Atlantic Treaty Organization 2022). This is done by layering IRC activities. Joint exercises in Latvia display NATO skills in physical destruction, but also make strategic PPP statements which are reinforced through PA. Concurrently, NATO OPSEC training and CIMIC outreach mitigates Russian propaganda directed at Enhanced Forward Presence members (Brewster 2020).

[4] PPP- Presence Posture Profile

The CAF model of Info Ops appears to be well aligned with a comprehensive approach and easy integration into GoC global strategy. If the CAF is already accustomed to synchronizing their military activities at the operational level, then integrating CAF activities with OGD and Allies at the strategic level, to counter Russian activities, would seem to be simply a matter of scaling and coordination. Certainly, this is how business in conducted on expeditionary operations such as Op IMPACT / NATO Mission Iraq / US OP INHERENT RESOLVE (OIR). CAF activities within the Directorate of Strategic Communications include KLE, StratCom, and the OIR narrative implementation. Combined with PA and the CJ39 Info Ops cell to coordinate activities within the coalition and host nation (Government of Canada 2021). If the CAF can work seamlessly with allies and host nations abroad, it should be simple to integrate at home.

Canadian Info Ops: Can it Work at Home?

Having reviewed what Info Ops are, we now need to ask if the CAF is ready to be a part of the GoC response to global information warfare. While our review of Info Ops doctrine and expeditionary operations says yes, our domestic organization is not so robust and certainly misaligned with GoC need. Ideally, security at home would see the CAF as simply one agency, similar to an IRC, responsible for some elements of the GoC response, working in conjunction with CSIS, CSE, RCMP, Public Safety, GAC etc. But we may not yet be as fulsome a stakeholder as the GoC requires. The permanent CAF establishment has inconsistent Info Ops capability and has done little to create a professional culture of delivering non-kinetic effects in the operating environment. A

long-neglected capability in the CAF, Info Ops and its IRCs only receive attention when presented in the media spotlight, often adversely (Pugliese 2015).

Training in Info Ops is in the periphery for most developmental periods for officers and NCOs. Few senior officers in the Regular Force have any formal info ops training, beyond brief orientations to the concepts during staff college. The intro to Info Ops provided during the Basic Intelligence Officers Course, is limited to a two-period guest lecture from a Peace Support Training Centre (PSTC) representative. This is more than any combat arms officers receive at a similar developmental period. Although, CIMIC, PSYOPS, PA and Info Ops are introduced during the Army Operations Course, the focus is understandably aimed at steel-on-steel conflict, with non-kinetic activities often absent or at best sprinkled on as an afterthought. Training has been described as 'Ad Hoc' for the Army by writers of the recent PDNA for Info Ops (Canadian Joint Warfare Centre 2021, 3). With Info Ops touted as a joint activity, the training situation is worse for those in the RCAF or RCN who receive less 'staff' training at the junior officer level with even more limited Info Ops orientation. It is not that good training is not available, the PSTC, responsible for delivering CIMIC, PSYOPS and Info Ops is world renown[5], but attendance on these courses has not been 'normalized' for any outside of the influence activities realm, mostly reservists, or those with a pending deployment.

The two main IRC's, referred to as 'influence activities' CIMIC and PSYOPS have long been a Primary Reserve capability (Government of Canada 2017, 69). This was appropriate when generating these capabilities for Afghanistan. It made sense to draw skills from the Primary Reserve, who are part time soldiers and civilian

[5] The Peace Support Training Centre is the CAF Centre of Excellence for CIMIC, PSYOPS and Info Ops training. Similar training is only otherwise available through NATO institutions or other international sources.

professionals, when the duties were related to engaging or influencing the civilian environment. However, it has created a 'break glass in case of war' attitude towards CIMIC, PSYOPS, and Info Ops, without having a strong permanent infrastructure or presence within the existing CAF establishment. Beyond the Regular Force component of the Influence Activities Task Force (IATF), elements of CJOC and SJS, there is no significant permanent Info Ops presence in the CAF, and these positions are often filled by reservists on contract. More worrisome for many was that CIMIC and PSYOPS, two very different military capabilities, were lumped together organizational into reserve Influence Activities (IA) Companies. The integration of these two IRC presents a perceptional problem, as the employment models were vastly different, but were expected of the same subunit.

The reliance upon the Primary Reserve for IA and Info Ops includes filling our missions. Appointments for KLE, CIMIC, Info Ops etc are often sought from members of the Primary Reserve, including augmentation for Technical Assistance Visits. The recent support to CTAT Lebanon to assist in the development of their own CIMIC training was almost exclusively made of Primary Reserve members. Regular Force members deployed to these positions rarely have this training prior to selection, and normally obtain Info Ops or similar training immediately prior to deployment. This creates a training expectation that is like a just in time service delivery, where training is provided only as absolutely needed, or as a surge capacity from the reserve. What this does not do is institutionalize the capacity into everyday operations within the CAF itself.

So, if skills are resident primarily in the reserve force, training is limited to secondary professional development or in support of deployment, what does the CAF

actually look like from Info Ops perspective. The simple answer to that is it depends where you are. Info Ops and key IRC, such as CIMIC and PA, can be very prevalent. Certainly, each base has a PAO, formations having the same, and this capability stretching into all elements, with even units having a Public Affairs representative. CIMIC elements exist only within the Army Reserve formations. At Div and higher, there is little consistency in portfolios. 4 Div stood down their G9 cell (CIMIC) and integrated the function into the G39 portfolio, yet 2 Div maintains their G9 cell. One would expect it would be synchronous across the Army at that level, but it is not. It is suspected that this is an artifact of deployed operation experience of commanders. Some expeditionary missions have a S9, where others hold those responsibilities within the S39 shop, perhaps individual Divs commanders simply mirror their deployed experiences.

If it seems like the CAF has their Info Ops and IRC misaligned with current need, it need not be perceived as so doom and gloom. Change is progressing incrementally. Not unlike the US SOF community, which integrates CIMIC and PSYOPS[6] into their command, CAF SOF has recognized that Info Ops is 'informing' many of the threat environments and they have sought training for their some of operators. Naval and Airforce elements are now actively seeking positions at the PSTC on Info Ops courses; indeed, the demographics of candidates are now also more evenly split among reservist and regular force members. The PSTC is actively looking to mitigate perceived training deltas in Info Ops in all developmental periods by creating a stand alone DLN Info Ops 101 introductory course, sufficient to orient the reader to Info Ops, much like the

[6] US Special Operations Command has an integrated PSYOPS group and a Civil Affairs (CIMIC) Bde.

preceding portion of this paper. This supports the Comd CA direction that Info Ops familiarization be included early in developmental period training (Comd CA 2021).

Additional recent realignments of Info Ops will support the CAF in conducting domestic activities and supporting the GoC across the spectrum of conflict, including DOMOPS or defense against foreign Information Operations. CDS Guidance on Info Ops and Influence Activities demanded a clear delineation of policies and doctrine for information operations and domestic operations (CDS 2021). This included direction on PSYOPS, CIMIC, Military Public Affairs and intelligence collection. It should be quite reassuring to the Canadian public and our OGD stakeholders that CAF members can professionally engage in their activities, within strict policy boundaries, in support of aid to civil powers or defence activities at home. The separation of CIMIC and PSYOPS from their composite IA companies leaves CIMIC elements affiliated to the Army Reserve Bde and PSYOPS linked to the IATF. The sharp delineation of tasks, responsibility, chains of command and authorities will ensure a more transparent use of the capabilities in any operation. While the elements and even army divisions and still have variation on Info Ops and IRC priorities within their respective HQ, the alignment of underlying skills and abilities is underway and with many of the IRCs well established, and the traditionally reserve capabilities migrating into the regular force domain. While the CAF has a stellar reputation for conducting exceptional Info Ops in expeditionary theatres, the pieces are all aligned for the organization to work with our other governmental stakeholder to defend at home from a persistent grey zone threat.

Conclusion

If we accept the Gerasimov doctrine of being at a constant state of war, then Canada is at war, albeit a hybrid one or a grey zone conflict. Unlike the world conflicts of the past where Canada went to war as an entire nation, our recent experience has been exclusively in expeditionary operations. Countering the Russian, or other adversarial, threats of grey zone conflict means that Canada must be ready to defend, on its home territory. Working with our OGD stakeholders also means accepting we may not be the lead in defending against grey zone conflict. The paradigm shift is understanding the CAF is being asked to package up a tailored task force such as deploying to Europe or the Middle East but contribute to a 'come as you are fight'. Cultivating a sense of at home readiness is something Canada has limited experience with, and that experience includes such dated activities as the Fenian Raids.

But form does follow function. The CAF has the capacity to be a valuable player in a GoC response to a hostile information environment and help shield the Canadian population and institutions from hostile influence activities. Aligning many of the Info Ops and non-kinetic activities into the permanent structure of the 'at home' force will create a culture within the CAF that believes that defending Canada at home is about more than simply steel on steel warfighting. While the CAF may not be the lead in a whole of government approach to a national information warfare protection policy, it must recognize that it does have a place. That means well trained and available pool of experienced professional talent. The Primary Reserve can support a quantum of that capacity but normalizing this within the permanent CAF establishments will codify the importance of information operations for the organization. The CAF must continue its recent evolution so that Info Ops is an established capability within the everyday

structure and integrated into all operations, expeditionary and domestic, across the spectrum of conflict, if we are to provide meaningful contributions to a synchronized Canadian strategy for global engagement, defence and sovereignty.

References

Canadian Joint Warfare Centre. 2021. *Operations in the Information Environment.* Professional Development Needs Analysis, Ottawa: National Defence.

Alba, Davey. 2022. *Russia has been laying groundwork online for a 'false flag' operation misinformation researchers say.* Feb 19. Accessed May 27, 2022. https://www.nytimes.com/2022/02/19/business/russia-has-been-laying-groundwork-online-for-a-false-flag-operation-misinformation-researchers-say.html.

Bills, Christian. 2020. *The Internet Research Agency: Spreading Disinformation.* Oct 30. Accessed May 26, 2022. https://smallwarsjournal.com/jrnl/art/internet-research-agency-spreading-disinformation.

Blagovest Tashev, LtCol Michael Purcell, Maj Brian McLaughlin. 2019. "Russia's Information Warfare Exploring the Cognative Dimension." *Marine Corps University Journal* 10 (2): 129-147.

Brewster, Murray. 2020. "Canadian-led NATO battlegroup in Latvia targeted by pandemic disinformation campaign." *CBC.* May 24. Accessed May 25, 2022. https://www.cbc.ca/news/politics/nato-latvia-battle-group-pandemic-covid-coronavirus-disinformation-russia-1.5581248.

CDS. 2021. *CDS/DM Directive - Resonse to Reviews of Information Operations and Influnence Activities.* CDS Direction, Ottawa: National Defence.

Comd CA. 2021. *Initiating Directive - Resetting the CIMIC and PSYOPS Capabilities in the Canadian Army.* Commander Directive, Ottawa: Canadian Army.

Cunningham, Conor. 2020. "A Russian Federation Information Warfare Primer." *University of Washington.* Nov 12. Accessed March 02, 2022. https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/.

Government of Canada. 2021. "Operation IMPACT." *National efence.* 06 30. Accessed 05 26, 2022. https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-impact.html.

Government of Canada. 2017. "Strong Secure Engaged." Defence Policy, Ottawa.

Kramer, Andrew E. 2019. "Russian General Pitches 'Information' Operations as a Form of War." *The New York Times.* March 2. Accessed 04 10, 2022.

https://www.nytimes.com/2019/03/02/world/europe/russia-hybrid-war-gerasimov.html.

Matthews, Miriam and Christopher Paul. 2016. *The Russian "Firehose of Falsehood" Propaganda Model.* Perspective, Rand Corporation.

McKew, Molly. 2017. "The Gerasimov Doctrine." *The Politico.* Occt. Accessed 04 05, 2022. https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/.

Morris, Victor. 2015. "Grading Gerasimov: Evaluating Russian Non Linear War Through Modern Chinese Doctrine." *Small Wars Journal.* Sept 09. Accessed 05 16, 2022. https://smallwarsjournal.com/jrnl/art/grading-gerasimov-evaluating-russian-nonlinear-war-through-modern-chinese-doctrine.

National Defence. 2011. *CFJP 3.0 Operations.* Vols. B-GJ-005-300/FP-001. Ottawa.

National Defence. 2018. *Department of National Defence and Canadian Armed Forces Policy on Joint Information Operations.* Policy Direction, Ottawa: National Defene.

National Intelligence Council. 2017. *Assessing Russian Activities and Intentions in the Recent US Elections.* Intelligence Community Assessment, Office of the Diretcor of National Intelligene.

NATO. 2009. *Allied Joint Doctrine for Information Operations.* Nato Standardization Agency.

—. 2019. *Allied Joint Doctrine for the Conduct of Operations Edition C Ver 1.0.* NATO Standardization Office.

North Atlantic Treaty Organization. 2022. "NATO's Enhanced Forward Presence." *NATO.* Public Diplomacy Division. Feb. Accessed May 23, 2022. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/2/pdf/2202-factsheet_efp_en.pdf.

Pugliese, David. 2015. "Chief of Defence Staff Gen. Jon Vance and the "weaponization of public affairs'." *The Ottawa Citizen.* Sept 21. Accessed 04 15, 2022. https://ottawacitizen.com/news/national/defence-watch/chief-of-the-defence-staff-gen-jon-vance-and-the-weaponization-of-public-affairs.

—. 2021. "Miltary Leaders saw pandemic as unique opportunity to test propaganda techniques on Canadians, Forces report says." *The Ottawa Citizen.* Sept 27. Accessed 04 12, 2022. https://ottawacitizen.com/news/national/defence-

watch/military-leaders-saw-pandemic-as-unique-opportunity-to-test-propaganda-techniques-on-canadians-forces-report-says.

Snecovaya, Maria. 2015. *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare.* Report, www.understandingwar.org, Washington: Institute for the Study of War.

Snegovaya, Maria. 2015. *Putin's Information Warfare in Ukraine.* Policy Research Report, Washington DC: Institute for the Study of War.

Thomas, Timothy. 2020. *Three Discussion of Russian concepts: Russian Information Weapons, Baltic Defences against Russian Propoganda and Russias Development of Non Lethal Weapons.* Consultant Report USEUCOM, McClean: MITRE.

United States of America. 2018. *Unitedd States of America v. Internet Research Agency et al.* Federal Indictment 1:18-cr-00032-DLF, Washington DC: United States District Court for the District of Columbia. Accessed May 26, 2022. https://www.justice.gov/file/1035477/download.