National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

THE FUTURE OF INFORMATION OPERATIONS IN THE CANADIAN ARMED FORCES

Maj Richard Matheson

JCSP 43 DL

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 43 AD

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 43 DL – PCEMI 43 AD
2017 – 2018

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

THE FUTURE OF INFORMATION OPERATIONS IN THE CANADIAN ARMED FORCES

Maj Richard Matheson

Word Count: 2976

Compte de mots: 2976

THE FUTURE OF INFORMATION OPERATIONS IN THE CANADIAN ARMED FORCES

Introduction

Canadian Armed Forces (CAF) Joint Doctrine defines information operations as "actions taken in support of political and military objectives which influence decision makers by affecting other's information while exploiting (fully utilizing) and protecting one's own information."[1] In the Canadian Army's Land Operations information operations are defined as "coordinated actions to create desired effects on the will, understanding and capability of adversaries, potential adversaries and other approved parties in support of overall objectives by affecting their information, information-based processes and systems while exploiting and protecting one's own."[2] Since the end of the cold war Canada and their NATO allies, in particular the US, have reorganized their militaries to fight counter-terrorism (CT) and counterinsurgency (COIN) operations. While our potential adversaries, mainly Russia, China, and Iran, have continued to develop their information and political warfare capabilities. As a result, a significant information knowledge and capability gap now exists between NATO and these potential adversaries.[3] In particular, Russia has used extensive political warfare capabilities and theory, to include information operations, to great effect in recent conflicts such as the Crimea and eastern Ukraine. In order to effectively operate in today's operating environment, the CAF must update their IO capability and doctrine to be able to match those of our potential adversaries. The CAF must also

---

[1] Canada. Department of National Defence. B-GG-005-004/AF-010, CFJP 03.10 – Information Operations. Ottawa, ON: Chief of the Defence Staff, 1998-04, 1-2.

[2] Canada. Department of National Defence. B-GL-300-001/FP-001, Land Operations. Ottawa, ON: Chief of the Defence Staff, 2008-01, 5-44.

[3] Lauder, Matthew A., Masters of Chaos: The Application of Political Warfare by the Russian Federation in the Contemporary Operating Environment, Defence Research and Development Canada, 2018, 17.

work closely with other Canadian government departments and agencies to develop social media and cyber doctrine to effectively counter potential threats against Canadian targets, to include the civilian population. Information Operations (IO) are increasing in importance across all domain's in military, political, industrial, and social environments. This paper will prove that the Canadian Armed Forces must adapt their IO doctrine and capability to effectively operate in today's changing operating environment.

Increasing importance of information

The nature of warfare is changing. It is no longer just about who has the larger military but is also about who has the best information about the battlefield; to include all actors be they state or non-state, combatant or non-combatant, military or civilian.[4] To this end, information operations have become an important element of modern warfare. Battles and conflicts are now sometimes waged entirely in the information domain. The information domain and information conflict have blurred the boundaries between peace, conflict, and war.[5] The information domain has the ability to disrupt and erode the hierarchies around which our institutions are formed. It can also diffuse and redistribute power, often to the benefit of the weaker and smaller actors.[6] States such as Russia, China, and to a lesser extent Iran, are using this as a way to gain an asymmetric advantage over the much larger United States military. Information activities have become an engrained feature of modren warfare, not just for cyber-empowered militaries such as that of the United States and Russia, but also for low-tech forces. Insurgent groups benefit from

[4] Arquilla, John, and David Ronfeldt. "Cyberwar is Coming!" In Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica: RAND Corporation, 1997, 23.

[5] Ehrhart, Hans-Georg. "Postmodern warfare and the blurred boundaries between war and peace." Defense & Security Analysis 33, No. 3, (14 Jul 2017), 264.

[6] Arquilla, John, and David Ronfeldt. "Cyberwar is Coming!" In Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica: RAND Corporation, 1997, 26.

the use of the Internet to recruit fighters and to finance operations. Social media is exploited for purposes that range from passing targeting information to directing the deployment of forces, as well as recruiting and disinformation campaigns.[7]

The aim of information conflict or activities between nations and societies is to disrupt, damage, or modify what a target population knows or thinks it knows about itself and the world. Information activities is conducted throughout the spectrum of conflict and spans the political, economic, and social, as well as military forms of conflict. In contrast to economic wars that target the production and distribution of goods, and political wars that aim at the leadership and institutions of a government, information conflict can affect all these areas by the targeting of information and communications.

Another important aspect of the information environment is the melding of civil and military means, the relevance of civil means on operation is increasing. This is due to the nexus between security and development that has become the "norm" in the context of military interventions. The combination of security and development is meant to stabilize the host country while at the same time winning over the local population. Information activities play a large role in the melding of civilian and military efforts into "whole of government approach." [8]

Until now, information conflict does not know any real limits. The emerging cyber domain, combined with the rest of the information domain, are unregulated and are being exploited in a new form of conflict.[9] The physical fight can be won on the battlefield but lost in the court of public opinion, if one side has acted outside the law, or been made to appear to have

[7] Schmitt, Michael N. "The Law of Cyber Targeting." Naval War College Review 68, Iss. 2, (Spring 2015): 11-30, 11.

[8] Ehrhart, Hans-Georg. "Postmodern warfare and the blurred boundaries between war and peace." Defense & Security Analysis 33, No. 3, (14 Jul 2017), 265.

[9] Ibid., 270.

acted outside the law of armed conflict. Given the novelty of information and cyber operations any alleged misuse at the tactical level can even have the potential for strategic consequences.[10]

Cyber Operations, also known as Computer Network Operations (CNO), have been increasing in importance for Western governments. There have been a series of attacks against governmental computer systems originating from China and Russia, most notably a Russian cyber-assault on Estonia and Chinese attacks on American and Japanese military and economic targets.[11] Recently, the Russian hacking of Democratic National Committee computers during the 2016 US presidential elections also made headlines. Our potential adversaries have proven themselves to be adept at both the technical aspects of IO, such as CNO, as well as the psychological aspects such as social media disinformation campaigns.

Future capabilities

As technologies advance and the world becomes more interconnected the military will have to adapt how they operate. Dense populations, critical infrastructure, and the proliferation of technologies that operate within the electromagnetic spectrum pose many challenges and opportunities for future forces.[12] In order to effectively operate within cities, the army will need to understand the human terrain as well as the usual environment and physical terrain. Although the interconnected world offers more of a challenge by ensuring that every action done by the military is only one tweet or Facebook post away from the rest of the world, it also provides the military with an opportunity for information and intelligence from multiple sources. Through the

[10] Schmitt, Michael N. "The Law of Cyber Targeting." Naval War College Review 68, Iss. 2, (Spring 2015): 11-30, 12.

[11] Black, Jeremy. "Into the Future." Chapter 7 in War and Technology. Bloomington: Indiana University Press, 2013, 253.

[12] Lawton, Joel, Matthew Santaspirt, and Michael Crites. "Army Operations in Megacities and Dense Urban Areas: A Mad Scientist Perspective." Military Intelligence Professional Bulletin 42, Iss. 3, (July 2016), 12.

mapping of geo-located tweets, the military can determine were incidents are occurring, what areas are access denied, and where and what type of aid is needed. This information can then be added together with full motion video from networked traffic cameras that are already in place in many cities.[13] This will allow the militaries to monitor the pattern-of-life of many cities in real time, without the disrupting presence their patrols would have in the area. This information can also be reviewed after each incident and analyzed to reveal patterns that may indicate future attacks. The future operating environment will be filled with connected devices such as game consoles, baby monitors, and home automated systems, that militaries can access to gain more information about the human terrain. At the tactical level being able to access personal electronic devices of a buildings occupants, such as smart phones, will be able to give the soldier a better picture of what each room contains. The information obtained from each connected device, personal electronic devices, and unmanned systems could be used to render a real-time 3D model of the building, as well as show the location of the buildings occupants, to include adversaries and non-combatants. This detailed information, as well as information gained outside the buildings by the traffic and security cameras will enhance the commander's situational awareness, allowing them to make rapid decisions and increase the protection of their forces. In addition, counter-measures to deny the enemy access to this information will also need to be developed.[14] To properly access these abilities in real-time, so that they provide the commander with this information as quickly as possible, some sort of tactical cyber capability needs to be available to each commander.

[13] Ibid., 14.

[14] Sampaio, Antonio. "Before and after urban warfare: Conflict prevention and transitions in cities." International Review of the Red Cross 98, Iss. 1, (2016), 42.

Russia

In the West the term "soft power" is used to describe a range of tools, including non-governmental ones, to co-opt – rather than coerce – others to achieve desired goals. The Russian understanding of this term is more in line with an information campaign or operation. The Russian foreign policy concept notes the 'illegal' use of soft power and human rights concepts to put pressure on sovereign states, intervene in their internal affairs, and destabilize them by manipulating public opinion.[15] As such, Russia considers the use of information campaigns against other nations as nothing more than an extension of their foreign policy. How Russia uses their variation of "soft power" can also be described as a form of political warfare. Political warfare is described as the employment of all the means at a nation's command, short of war, to achieve its national objectives. Political warfare is first-and-foremost an informational endeavor, using both state and non-state assets to dominate the information environment.[16] Russia has continued to invest in their political warfare capability by modernizing organizational structures, updating strategic policies and doctrine, developing new concepts and theories, as well as incorporating new technologies as they become available.[17] On the other hand, since the end of the Cold War the US and their NATO allies have mostly concentrated on building their counter-terrorism and counterinsurgency abilities, which has resulted in a deterioration of their political warfare capabilities.[18] As such, a large knowledge and capability gap now exists between Russia

[15] Monaghan, Andrew. The New Russian Foreign Policy Concept: Evolving Continuity. Chatham House, 2013, 6-7.

[16] Lauder, Matthew A., Masters of Chaos: The Application of Political Warfare by the Russian Federation in the Contemporary Operating Environment, Defence Research and Development Canada, 2018, 1.

[17] Ibid., 2.

[18] Ibid., 1.

and NATO. This capability gap, particularly in cyber and social media, has given Russia an asymmetric advantage in the space between peace and war.[19]

The Russian political warfare model has three phases; foment, seize, and consolidate. In the foment phase Russia uses information activities, conducted by Russian agents or proxies under the nominal control or guidance of Russian officials, to destabilize the target nation by rupturing existing fault-lines or creating a crisis to push the nation into a state of chaos. In the next phase, seize, Russia uses military and non-military measures by pro-Russian proxies to seize territory, dominate the information environment, and seize state power. When required, the seize phase may be augmented by Russian military assets. The final consolidate phase includes formalizing control over a territory, as well as maintaining information dominance and reestablishing a state of normalcy and stability. There are no set boundaries between the stages and operations can be conducted throughout each phase.[20] Russia used this model to great effect during operations in the Crimea and eastern Ukraine.

One of the ways Russia uses information activities to keep adversaries off balance is by the coordinated use of disinformation campaigns. Throughout the Ukrainian campaign there are multiple examples of Russia using disinformation to great effect. For example, one particular campaign involved a staged video posted to YouTube that purportedly showed Blackwater members attempting to suppress a non-violent pro-Russian demonstration in eastern Ukraine. Once the existence of the video was reported by the Daily Mail in the UK, Russian news sites then used the Daily Mail article as proof of the authenticity. The whole campaign became such a distraction to US and Ukrainian officials that it forced US authorities to officially deny the claims.

---

[19] Ibid., 23.
[20] Ibid., 36

Russia has also proved themselves adept at combining the technical aspects of IO with the psychological aspects. For example, in early 2015 a phone call between Victoria Nuland, the US Assistant Secretary of State, and the US Ambassador to the Ukraine was intercepted and recorded (technical) and then released on social media (psychological). During the phone call some very embarrassing comments were made by Nuland which damaged the US reputation in the region and forced the US into damage control.[21] Another example of a successful combination to technical and psychological aspects of IO is the hacking of Democratic National Committee (DNC) computers (technical) and then releasing their emails (psychological). As a result of the leaked emails the president of the DNC had to resign, and the Clinton campaign was significantly damaged.[22] As Canada is heavily involved in NATO's enhanced forward presence battlegroup in Latvia, and a training mission in the Ukraine, the Canadian Armed Forces (CAF) must be prepared to deal with these kinds of information activities directed at them, as well as a way to identify and counter these campaigns. We can expect the target-audiences for such campaigns to not only be the regional civilian population, but our domestic population as well.

Canadian Armed Forces current doctrine

The CAF's current IO doctrine is CF Joint Doctrine B-GG-005-004/AF-010 Information Operations, published on 15 April 1998.[23] In the twenty years since this doctrine was published information technology has advanced a long way. Since this doctrine was published the way the world communicates has changed. The use of cell phones is now a lot more common place in

[21] Lauder, Matthew A., When Lies Become Truth: A Brief Examination of Smear Campaigns as a Key Tactic of Russian Informational Conflict, Defence Research and Development Canada, 2016, 5.

[22] Ibid., 6.

[23] Canada. Department of National Defence. B-GG-005-004/AF-010, CFJP 03.10 – Information Operations. Ottawa, ON: Chief of the Defence Staff, 1998-04.

most parts of the world. In 1998 social media to a large extent did not exist, and now it is quickly becoming the most common way that information is transmitted. The internet has grown and connected the world in ways that were not seen in 1998. In this doctrine it states, "While it is realized the CF currently does not possess a formal PSYOP capability, many potential allied partners do possess this capability, therefore, PSYOP must be considered for the effective integration of all IO capabilities."[24] This statement markedly dates this publication as the Canadian Army has had a growing PSYOPS capability for many years now and in June 2013 formalized the integration of PSYOPS in the Army Reserve with the signing of the Canadian Army Influence Activities Interim Implementation Directive (CA IA IID). The CA IA IID established a PSYOPS platoon within an Influence Activities Company in each Canadian Brigade Group.[25] Also noticeably missing from CF Joint Doctrine B-GG-005-004/AF-010 Information Operations due to its age is any reference to social media and cyber operations.

CF Joint Doctrine B-GJ-005-313/FP-001 Psychological Operations is another reference that needs to be updated, as it was published on 15 January 2004. PSYOPS is defined as "Planned psychological activities using methods of communications and other means directed to approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives."[26] In the doctrine it identifies that the three most common types of media to communicate with the target audience is audiovisual, visual, and audio.[27] Once again, this publication overlooks the importance of social media to communicate with the target audience. Although audiovisual, visual, and audio can all be used to communicate

---

[24] Ibid., 2-3.

[25] Canada. Department of National Defence. Canadian Army Influence Activities Interim Implementation Directive. Ottawa, ON: Commander Canadian Army, 2013-06.

[26] Canada. Department of National Defence. B-GJ-005-313/FP-010, CFJP 03.10.1 – Psychological Operations. Ottawa, ON: Chief of the Defence Staff, 2004-01, 1-1.

[27] Ibid., E1-1.

messages via social media, more detail should be provided for the use of social media in communicating with a target audience. Social media has become such a prevalent part of modern communication to should be classified as its own means of dissemination.

Canadian Army B-GL-300-001/FP-001 Land Operations, published 01 January 2008, contains a very good section dedicated to Information Operations. Chapter 5 Section 9 is dedicated to the use of information operations in land operations. Most notably, even though CF Joint Doctrine Information Operations does not mention cyber operations, Land Operations mentions Computer Network Operations (CNO) as an integral part of IO. Land Operations lists three types of CNO; Computer Network Attack, Computer Network Exploitation, and Computer Network Defence.[28] Although, Land Operations includes CNO as part of IO it does not provide any detail on how to conduct this type of operation.

Recently, the Chief of Defence Staff (CDS) has issued the Department of National Defence and Canadian Armed Forces Policy on Joint Information Operations, dated 3 April 2018. In it the CDS notes that "Adversaries are using the information environment to create an arena where disinformation, misinformation, and propaganda are mixed to obscure the truth, so that those adversaries can achieve their goals and objectives to the detriment of Canada and its allies."[29] Fortunately, the CAF has concluded that IO is playing a greater part in modern operations and are working to improve thier IO capability. Of note, this new policy allows for the CAF to conduct IO in Canada for two reasons; in the Defence of Canada, and Assistance to other Government Entities. While assisting other government entities CAF assistance must be at the

[28] Canada. Department of National Defence. B-GL-300-001/FP-001, Land Operations. Ottawa, ON: Chief of the Defence Staff, 2008-01, 5-50.

[29] Canada. Department of National Defence. Department of National Defence and Canadian Armed Forces Policy on Joint Information Operations. Ottawa, ON: Chief of the Defence Staff, 2018-04, 1.

request of the other entity and will be subject to the same legal constraints as said entity.[30] This is important because the CAF must be prepared to work with other government departments to counter adversary IO directed at our populace, as the interconnected nature of IO means that IO directed at the CAF can be from the same source as IO directed at some other aspect of Canada be it political, industrial, or social.

With the new focus on IO, the CAF must ensure that all IO doctrine is updated to include CNO and social media. In order for Canada to maintain a proper level of deterrence in the information domain, it must develop a robust IO capability, to include a strong offensive capability. This capability must be an intergovernmental effort, that includes the CAF, and is well coordinated from the top down. IO is a significant force multiplier that can allow a small force, such as the CAF, to build an asymmetric advantage and work as a balance of power.

Conclusion

The importance of IO has increased in modern warfare due to advancements in technology. Canada's potential adversaries have built a large capability and knowledge gap that Canada must now work to close. In recent conflicts Russia has proven itself to be adept at using disinformation and misinformation, as well as combining the technical and psychological aspects of IO, to advance their political aims. The CAF must adapt their IO doctrine and capability to effectively operate in today's changing operating environment, to effectively protect Canada's interests at home and abroad. Cyber and social media are important aspects in today's IO and CAF doctrine must be updated to include this fact. The CAF must also be prepared to assist and work with other government agencies in a combined effort to protect Canada in the information

[30] Ibid., 5.

environment. Unless Canada closes the gap in ability with their potential adversaries they will remain vulnerable due to lacking an effective deterrence.

BIBLIOGRAPHY

Canada. Department of National Defence. B-GG-005-004/AF-010, CFJP 03.10 – Information Operations. Ottawa, ON: Chief of the Defence Staff, 1998-04.

Canada. Department of National Defence. B-BJ-005-900/FP-000, CFJP 9 – Civil Military Cooperation in Peace, Crisis, Emergency and War. Ottawa, ON: Chief of the Defence Staff, 1999-01.

Canada. Department of National Defence. B-GJ-005-313/FP-010, CFJP 03.10.1 – Psychological Operations. Ottawa, ON: Chief of the Defence Staff, 2004-01.

Canada. Department of National Defence. B-GL-300-001/FP-001, Land Operations. Ottawa, ON: Chief of the Defence Staff, 2008-01.

Canada. Department of National Defence. B-GL-300-005/FP-001, Land Information Operations. Ottawa, ON: Chief of the Defence Staff, 1999-01.

Canada. Department of National Defence. B-GL-331-002/FP-001, Staff Duties for Land Operations. Ottawa, ON: Chief of the Defence Staff, 2008-08.

Canada. Department of National Defence. B-GL-354-003/FP-001, Deception. Ottawa, ON: Chief of the Defence Staff, 1998-07.

Canada. Department of National Defence. B-GA-403-000, Aerospace Shape. Ottawa, ON: Chief of the Defence Staff, 2014-03.

Canada. Department of National Defence. Department of National Defence and Canadian Armed Forces Policy on Joint Information Operations. Ottawa, ON: Chief of the Defence Staff, 2018-04.

Canada. Department of National Defence. Canadian Army Influence Activities Interim Implementation Directive. Ottawa, ON: Commander Canadian Army, 2013-06.

North Atlantic Treaty Organization. AJP 3-10, Information Operations, 2009-11.

North Atlantic Treaty Organization. AJP 3.2, Land Operations, 2009-10.

Lauder, Matthew A., When Lies Become Truth: A Brief Examination of Smear Campaigns as a Key Tactic of Russian Informational Conflict, Defence Research and Development Canada, 2016.

Lauder, Matthew A., An Iron Fist in a Velvet Glove: A brief examination of the Russian military operation to annex Crimea in 2014, Defence Research and Development Canada, 2016.

Arquilla, John, and David Ronfeldt. "Cyberwar is Coming!" In Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica: RAND Corporation, 1997.

Denning, Dorothy. "A Theory of Information Warfare." Chapter 2 in Information Warfare and Security. New York: ACM Press, Addison Wesley, 1999.

Ehrhart, Hans-Georg. "Postmodern warfare and the blurred boundaries between war and peace." Defense & Security Analysis 33, No. 3, (14 Jul 2017).

Lauder, Matthew A., Masters of Chaos: The Application of Political Warfare by the Russian Federation in the Contemporary Operating Environment, Defence Research and Development Canada, 2018.

Sampaio, Antonio. "Before and after urban warfare: Conflict prevention and transitions in cities." International Review of the Red Cross 98, Iss. 1, (2016).

Lawton, Joel, Matthew Santaspirt, and Michael Crites. "Army Operations in Megacities and Dense Urban Areas: A Mad Scientist Perspective." Military Intelligence Professional Bulletin 42, Iss. 3, (July 2016).

Black, Jeremy. "Into the Future." Chapter 7 in War and Technology. Bloomington: Indiana University Press, 2013.

Monaghan, Andrew. The New Russian Foreign Policy Concept: Evolving Continuity. Chatham House, 2013.