National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

REMOTE WARFARE FORCE PROTECTION: ACCOUNTING FOR NON KINETIC THREATS AND RISKS

Lieutenant-Colonel Carl Gravel

JCSP 45

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 45

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 45 – PCEMI 45
MAY 2019 – MAI 2019

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

REMOTE WARFARE FORCE PROTECTION: ACCOUNTING FOR NON KINETIC THREATS AND RISKS

Lieutenant-Colonel Carl Gravel

Word Count: 5,000

Nombre de mots : 5,000

INTRODUCTION

The Canadian Armed Forces (CAF) last updated its joint publication on Force Protection in 2006; the height of its participation in the War in Afghanistan.[1] Since then, the threats and risks associated with operating in the new multi-domain environment have changed significantly. To ensure that the CAF maintains its freedom of action and operational effectiveness, its Force Protection doctrine needs to be reviewed. The current doctrine attempts to account for all sources of risks and asymmetric threats to "minimize risk to [the CAF's] forces so that they can accomplish their mission" but covers only risks on the physical plane.[2]

While kinetic threats and physical risks to CAF personnel have also evolved, Force Protection measures enshrined in its doctrine are still valid and effective. This paper will argue that CAF force protection doctrine should be reviewed to account for psychological threats to CAF personnel and non-kinetic risks associated with operating in the emerging multi-domain environment. To support this argument, it is important to first define the new environment in which CAF personnel will have to operate. Secondly, this paper will explore how Canadian soldiers, in the context of grey-zone conflicts, being both actors and recipient of hybrid warfare tactics, are exposed to asymmetric threats often targeting them directly. It will then demonstrate that the conduct of hybrid warfare, especially remote warfare tactics, have inherent psychological and moral risks that require mitigation above and beyond what is provided by health services and the chaplaincy. Finally, the current CAF Joint Force Protection doctrine will be compared against other pieces of doctrine and policy to identify potential recommendations to expand the scope of Force Protection to the psychological and moral plane.

---

[1] Canada. Dept. of National Defence. *CF Joint Force Protection Doctrine (English)*. Ottawa: Dept. of National Defence, 2006. cover.

[2] *Ibid*., i.

WHAT CHANGED?

Modern Force Protection

The development of the contemporary force protection doctrine has been directly influenced by the increasing ability of relatively small armed groups, such as terrorist organizations, to exploit vulnerabilities of modern and professional military forces. A defining event that sparked the refinement of the modern concepts and methods to protect the force and its ability to maintain operational effectiveness was the bombings of the Multinational Forces in Lebanon (MNF) barracks at the Beirut International Airport in 1983. This event was arguably the first major asymmetric attack against a modern multinational force where a small terrorist organization, which may have been backed by state actors, inflicted significant casualties to a much larger force. This killing of 350 United States (U.S.) and French personnel led to the identification of several lessons learned regarding protection of the force against asymmetric threats. For instance, the report of the U.S. Department of Defense commission on the Beirut International Airport Terrorist Act made some important conclusions that would help shape the conduct of operations for the following decades. The first key conclusion was that "international terrorist acts [...] poses an increasing threat to U.S. personnel and facilities" and concurrently that "state sponsored terrorism is an important part of the spectrum of warfare." [3]The other key conclusion was that in order to ensure military preparedness and ensure the ability to defend and counter terrorism, that doctrine should be developed and implemented throughout the force.[4]

---

[3] United States of America. Department of Defence. *Report of the DOD Commission on Beirut International Airport Terrorist Act, October 23, 1983*. 1983. p. 128-129; United Nations. "United Nations Security Council Resolution 1566 (2004)." United Nations Security Council. Adopted 8 October 2004. Terrorist acts as defined in paragraph 2 of the UNSCR.

[4] United States of America. Department of Defence. *Report of the DOD Commission on Beirut International Airport Terrorist Act, October 23, 1983*. 1983. 133.

Looking back 35 years, history has shown that defending against terrorist acts, state sponsored or not, would define the modus operandi of modern military forces engaged in conflict around the globe. In the post Cold War world, under the paradigms of the conduct of Operations Other Than War (OOTW) or Counter-Insurgency (COIN) operations, the concepts associated with the doctrine of force protection have been key in enabling military capabilities and maintaining operational effectiveness.[5] The predominance of asymmetric threats by non-state actors against modern military forces for the past few decades has been enabled both by its successes and by the advancement and availability of technological means. The Internet, cellular phones, and affordable commercial drones are but a few examples of new technologies that transformed the battlefields of the 21st century and further enabled the successes of asymmetric threats against conventional forces. Changes to the conduct of warfare in the Information Age are so significant that solutions devised to protect forces against asymmetric threats similar in nature as the Beirut barracks bombings might no longer be effective.

Information Age Warfare: The Grey-Zone

The latter half of the 20th century saw the transition from conflicts waged between nations using their conventional military forces to multinational military forces engaged against international terrorist organizations or rogue states. In contrast, the beginning of the 21st century is seeing a transition back to conflicts between nation states but with two key differences: the focus on asymmetric engagements below the threshold of war and the emergence of new Information Age domains of warfare. The strategic importance of information, networks, and space capabilities and assets made the space and cyber / information domains join the traditional

[5] Canada. Dept. of National Defence. CFJP 3-14, *CF Joint Force Protection Doctrine (English)*. Ottawa: Dept. of National Defence, 2006. 1-1.

land, air, and sea domains as grounds to wage war and conflicts. This is a significant paradigm-shift: the causes, means, ways, and ends of conflicts have transformed into something that is almost unrecognizable for the conventional military forces. [6]Traditional attrition warfare died with the Industrial Age as "the days when wars could be won by sheer bravery and perseverance are gone."[7] Warfare in the Information Age is now about psychological attrition and strategic narratives. It will seemingly remain somewhere between peace and war; in the grey-zone. To be successful in this new context, military forces have to reshape their structure, ways of thinking, and their actions.

Conflicts in the grey-zone are incredibly complex, ill-defined, and engaged by all available instruments of national power as well as by non-state actors. They can be violent or not, and they may not even be militarized. However, when they are, the utilization of military power has not been so far to employ conventional forces meant to engage in a symmetrical way other conventional forces. Instead, it is as a mix of national military forces combined with non-state actors and employing asymmetric tactics. So far, there is no consensus on the naming and definition of this new way of waging war in the grey-zone. Some scholars, like Hans-Georg Ehrhart, label it postmodern warfare, others, like Jean-Christophe Boucher, call it hybrid warfare.[8] Labels aside, one of the defining characteristic of this type of warfare is the employment of irregular practices by nations to further their geopolitical interests while

---

[6] Carment, David and Belo, Dani. "War's Future: The Risks and reward of Grey-Zone Conflict and Hybrid Warfare." Canadian Global Affairs Institute. October 2018. 2.

[7] Barry R. Schneider and Lawrence E. Grinter. "Battlefield of the Future: 21st Century Warfare Issues." Honolulu, HI: University Press of the Pacific, 2002, 104.

[8] Boucher, Jean-Christophe. "Hybrid Warfare and Civil-Military Relations." Canadian Global Affairs Institute (CGAI). Policy Update. December 2017; Ehrhart, Hans-Georg. "Postmodern warfare and the blurred boundaries between war and peace." Institute for Peace Research and Security Policy, University of Hamburg, Defense & Security Analysis Vol. 33, No. 3, (2017).

mitigating risks and preventing crossing the threshold of war. What is important to keep in mind is that it is a mean to, as defined by political scientist Michael J. Mazarr, conduct

> sequences of gradual steps to secure strategic leverage. The efforts remain below thresholds that would generate a powerful [national]. or international response, but nonetheless are forceful and deliberate, calculated to gain measurable traction over time.[9]

Buffer as Shield: Remote Warfare

Focusing on mitigating risk is one of the unavoidable aspect of the evolution of warfare where the primary aim is to shield both the operators (individuals) and nations (collectives) to the consequences of warfare. In fact, it can be argued that "the history of modern weaponry involves the construction of the technological capacity to produce lethal results while exposing the operator to the least amount of risk of death or injury." [10] In addition to the actual tools of warfare, modern tactics are centred on producing an asymmetrical risk where "the overall strategy is to create a system that grants the operator total immunity from risk but still inflicts maximum damage to the enemy." [11] This system has been almost exclusively focused on physical risk, as it has been the most impactful to individuals and associated to political risks for nations. Where weapon systems would be developed to prevent physical harm to operators, strategies and tactics would evolve to prevent exposure to physical consequences of being a participant in a conflict.

Advances in technology have even enabled removing operators from the theatre of operations and having them conduct their war activities remotely. This is what has become

---

[9] Mazarr, Michael J. "Mastering the Gray Zone: Understanding a Changing Era of Conflict." Strategic Studies Institute, US Army War College, 2015. 1.

[10] Ohlin, Jens David. *Research Handbook on Remote Warfare*. Edward Elgar Publishing, Incorporated. 2017. 17.

[11] *Ibid*., 18.

known as "remote warfare." Utilizing weapons such as remotely piloted aircraft (i.e., drones), cyber-weapons, or autonomous weapon systems shields the operators from physical risk associated with the conduct of military operations in a given theatre. However, these capabilities are a double-edged sword and are also used by adversaries to maximize the asymmetry of risk between them and their target.[12]

The effects of utilizing these remote capabilities also have other impacts on the presence of risk when conducting operations. For example, these capabilities could have an effect of complementing an in-theatre force that would be smaller than required without those remotely operated capability, which reduces force protection requirements to mitigate risk within the theatre of operations.[13] The creation of a buffer between the physical effects of war and its operators by the utilization of remote weaponry, asymmetric tactics or strategies seemingly has a net benefit when looking at the balance of risk. However, these means also come with several second order effects that are not easily apparent and can themselves pose a risk to the CAF and its personnel.

PERSONAL NATURE OF ASYMMETRIC THREATS

The militarization of the information domain (space, cyber and electronic warfare) provides brand new avenues of attack both for state and non-state actors. These new avenues allow for new forms of direct threats both to Canada and members of the CAF. Adversaries can operate in this emerging domain, either jointly with the traditional domains, or not, to achieve specific goals. While targets can vary significantly depending on the objectives and methods of

[12] Knowles, Emily and Watson, Abigail. "No Such Thing as A Quick Fix - The Aspiration-Capabilities Gap in British Remote Warfare." Remote Warfare Program. Oxford Research Group. 2018. 2.

[13] North Atlantic Treaty Organization. AJP 3-4, *Allied Joint doctrine for Force Protection*. NATO Standardization Office. Edition A Version 1 April 2015. 4-8.

the adversary, CAF personnel can find themselves being directly under threat under this domain. These threats are non-kinetic in nature and can either be direct or indirect. They are also not addressed by the CAF's current Force Protection doctrine.

Indirect: Influence Operations

The interconnectivity brought by Information Age technology has resulted in the creation of a virtual word that enables people from all over the world to connect and share thoughts and ideas. This relatively nascent virtual world already transcended the real world in many aspects, notably breaking the limits of time and distance. The apparatus of the information domain allows for the rapid propagation, storage and processing of a vast quantity of information in a short period of time. This massive amount of available information has shifted the paradigms surrounding the meaning of quality and value of data. [14] Significant portion of the value is now attributed to the potential operationalization of data. This is as true for corporations in support of their business model, or by other entities seeking to further their interests by manipulating the available data. In this space, adversaries are able to shape portions of the available data creating a narrative that will either influence specific actors or directly further their interests. [15]

For the CAF and its personnel, this translates into adversaries being able to effectively conduct influence operations, i.e., propaganda, to delegitimize CAF actions. This adversarial influence brings a negative psychological effect on CAF members and may impact their motivation and performance, which can result in decreased operational effectiveness. A recent example of this would be the "fake news" campaign by Russia against the CAF operating in

[14] Gasser, Urs. "What Makes Information Valuable? Information Quality, Revisited". *Berkman Klein Center for Internet & Society*. Harvard University.

[15] Maan, Ajit. "Narrative Warfare" CreateSpace Independent Publishing Platform, 03 April 2018.

Latvia as part of Operation Reassurance.[16] This campaign was a direct threat to the CAF's success as it sought to discredit and delegitimize its actions. Further than being a threat to the overall mission, these kinds of influence operations are a threat to CAF personnel as they can degrade understanding or support of the mission or even introduce bias shifting the way CAF personnel think and act in the theatre of operation. In Latvia, the countermeasure that the CAF employed to fend against the Russian "fake news" campaign was to propagate its own version of the narrative; a much more positive one. As CAF Chief of the Defence Staff, General Jonathan Vance, stated to *The Globe and Mail*: "the most effective tool to push back against efforts to discredit the battlegroup is its PR campaign."[17]

Direct: Deliberate Targeting

An even more serious threat than attempting to influence CAF personnel is targeting them directly within the information domain. Online information, especially social media, is becoming more than a simulacrum of reality; it is becoming the new reality. This *Hyperreality*, as coined by French sociologist Jean Baudrillard, is the blend of the real and the online representation of the real.[18] Where parts of people's lives now reside in the information domain, it is now being used by various malicious actors to interact nefariously with them. "On the Internet, nobody knows you're a dog" says the classic adage published in *The New Yorker* in 1993 about the nature of online interaction through avatars.[19] The real person behind the online mask may not be who they claim to be and their intent might also be masked.

---

[16] Blackwell, Tom. "Russian fake-news campaign against Canadian troops in Latvia includes propaganda about litter, luxury apartments." National Post. Last accessed on 05 May 2019.

[17] Ling, Justin. "In Latvia, Canadian and Italian forces stand on guard with NATO against Russian expansion." The Globe and Mail. 11 June 2018. Last accessed on 05 May 2019. https://www.theglobeandmail.com/world/article-in-latvia-nato-forces-stand-on-guard-against-russian-expansion/

[18] Baudrillard, Jean. "Simulacra and simulation". Ann Arbor: University of Michigan Press. 1994.

[19] Steiner, Peter. "On the Internet Nobody Knows You're a Dog." New Yorker. 5 July 1993. 61.

In that context, adversaries are able to target specific individuals and utilize the data found in their digital footprints as means of delivering an operational effect. Through the exploitation of various vulnerabilities, both technical and personal, the information domain is a vector that enables non-kinetic coercive actions. For the CAF, this means that adversaries are able, and incentivized, to target its personnel in an attempt to obtain a competitive advantage in every phase of a conflict. CAF personnel can be targeted by adversaries and their data can be used against them in order to gain intelligence through catfishing, phishing, blackmailing, or other scams. As the average Canadian is at risk of being victim to such actions, so are CAF personnel. The key difference being that CAF members can be more than simple victims of criminal fraud, they can be deliberate targets of an adversary attempting to gain a competitive advantage in a conflict or attempting to degrade the operational effectiveness of the CAF. These methods can be very effective at low cost. A research conducted during a NATO exercise illustrated this well. There, researchers used open source data, fake social media profiles and targeted advertisement to measure the operational impact of social engineering targeting actions. The results were that "by the end of the exercise, the researchers identified 150 soldiers, found
the locations of several battalions, tracked troop movements, and compelled service members to engage in "undesirable behavior," including leaving their positions against orders." [20]

CAF personnel affected by these kinds of influence and targeting operations through the information domain have the potential to face serious psychological impacts. Similar to typical dating and relationship scams (i.e., Catfishing), victims will most likely be changed negatively by the experience. In an attempt to explore the psychological impacts of online fraud, Monica

[20] Lapowsky, Issie. "NATO Group catfished Soldiers to Prove a Point About Privacy." WIRED Magazine. 18 February 2019. Last accessed 05 May 2019.
https://www.wired.com/story/nato-stratcom-catfished-soldiers-social-media/

Whitty, professor of human factors in cyber security and Tom Buchanan, professor of psychology said of the experience that "for some, [it] led to a loss of trust in others. [...] They also severed ties with others and felt less inclined to be social. [It] lowered [their] sense of self-worth and confidence."[21] These negative experiences have a negative effect on the mental health of personnel and they should be provided measures to protect themselves against threats of that nature. In an operational context, these measures must be both doctrinal and systemic.

THE RISKS OF HOLDING THE REMOTE

The risks mentioned above were derived from actions by adversaries, but in the new multi-domain environment, there are also other risks to personnel inherent to the conduct of operations. Notably, the risks that come with the conduct of remote warfare activities. The addition of remote weaponry and the delivery of operational effects within the information domain have helped shield forces from kinetic threats. However, these new means of conducting war pose risks to the mental health of the force, which could jeopardize operational effectiveness.

Reciprocity is not the Aim

The CAF as a professional military force of a democratic nation prides itself on having the "highest ethical standards in all decisions and actions, whether at home or abroad." [22] Naturally, as a volunteer force, it is reasonable to expect that the majority of CAF personnel associate with this statement and embrace the values and ethics of the organization. Furthermore, it is also reasonable to claim that the CAF sees itself as an organization that is fair and just, wants

[21] Whitty, M. T., & Buchanan, T. "The online dating romance scam: The psychological impact on victims – both financial and non-financial". Criminology & Criminal Justice, 16(2). 2016. 182..

[22] Canada. Dept. of National Defence. *Code of Values and Ethics (English)*. Ottawa: Dept. Of National Defence, 2012. 7.

to do good, that follows domestic and international laws, and is a public institution that the Canadian population can look up to.[23] This context is important as it lays the basic assumptions and expectations of CAF personnel and Canadians toward the organization. The CAF is a military force that fights in justified war in accordance with international law and aims to improve peace and stability.

To be consequent with these expectations, the methods employed must also seem fair and just. Otherwise, this opens the door to problems where the justification for participating in a conflict might be obfuscated by an apparent unfairness caused by an asymmetry at the tactical level. The employment of certain methods or technologies might make the fight "intrinsically unfair and thus unjust."[24] Delivering operational effects from a distance, especially those having deadly effects, might make certain operators feel that they are fighting unfairly and could, in some cases, lead them to experience a moral dilemma that, if not addressed, could result in a moral injury. The National Center for Post Traumatic Stress Disorder (PTSD) of the U.S. Department of Veterans Affairs defines a moral injury as an event that "shatters moral and ethical expectations that are rooted in religious or spiritual beliefs, or culture-based, organizational, and group-based rules about fairness, the value of life, and so forth." [25] The utilization of technologies such as remotely piloted aircraft and cyber weapons that are aimed to maximize the asymmetry of risk make the fight de-facto unfair, which might play against the expectations of fairness in some cases. Pushed to extreme cases, this asymmetry attached to a

---

[23] Canada. Dept. of National Defence. *Summary of Duty with Honour - The Profession of Arms in Canada (English)*. Ottawa: Dept. Of National Defence, 2003. 6.

[24] Galliot, Jai C. "Uninhabited Aerial Vehicles and the Asymmetry Objection: A Response to Strawser". Journal of Military Ethics, 11:1. 2012. 59.

[25] United States of America. Department of Veterans Affairs. *Moral Injury in the Context of War*. National Center for PTSD. Last accessed on 05 May 2019. https://www.ptsd.va.gov/professional/treat/cooccurring/moral_injury.asp

large technological imbalance "may actually override any justification for war." [26] This situation would not only play against expectations of fairness, but also those of justness.

War as a 9 to 5 Job: The Confusing Line between War and Peace

Another risk of remote warfare beyond the potential risk of moral injury is that while it shields operators from the kinetic dangers, it does not shield them from being exposed to the horrors of war. A clear example of this would be drone operators and intelligence personnel, which operate remotely but have a direct view on the gruesome impacts of war. In the U.S. Air Force, there have been several reports of higher rates of occupational stress and suicide for those type of personnel. A showcase example would be the 480th Intelligence, Surveillance and Reconnaissance Wing, U.S. Air Force; a formation specialized in those types of activities. Due to the nature of their mission, the wing had to ramp up the medical, psychological and moral support to "to ease [the] burden by treating the trauma of remote warfare a little more like the effects of traditional combat."[27] Leading the team supporting the personnel of the 408th, Lieutenant-Colonel Cameron Thurman, the Wing's Surgeon, gives a clear diagnostic: "observing the horrors of war, over and over again — even from a distance — carries a heavy burden." [28]

Operating in the new environment of hybrid warfare and grey-zone conflict, especially remotely, also brings another set of psychological risks associated with the blurred lines between war and peace. According to Ehrhart, as "geographic and normative limits blur and erode," it brings into question the notion of what is actually considered war in the context of actions within

[26] Galliot, Jai C. "Uninhabited Aerial Vehicles and the Asymmetry Objection: A Response to Strawser". Journal of Military Ethics, 11:1. 2012. 62.

[27] McCammon, Sarah. "The Warfare May be Remote but the Trauma is Real." National Public Radio. Last accessed 05 May 2019. https://www.npr.org/2017/04/24/525413427/for-drone-pilots-warfare-may-be-remote-but-the-trauma-is-real

[28] *Ibid*.

the grey-zone.[29] This challenge to the traditional notions and paradigms of warfare not only has implications at the political level, but also at the personal level. Traditionally, soldiers going into war had to leave their home to conduct war and would only come back once their duty was done. Even the personnel supporting from the home front had an easier time understanding what the limits of war were: the enemy, the theatre of war and the methods and tactics were well defined. Nowadays, the blurred lines of grey-zone conflicts and the nature of the conduct of remote warfare makes it tremendously hard for personnel to have clear mental boundaries separating themselves at war and themselves at home, at peace. Looking back at the case of 408th Wing, the intelligence and drone operators have to live with through these blurred lines as they transition between their work, which unlike most people is the conduct of war, and ordinary life everyday. As U.S. Air Force psychologist, Lieutenant-Colonel Alan Ogle puts it: "Ten minutes, 15 minutes, [they] drive home. They've gone from being eyes, head in the fight, and making critical life and death decisions, to then being involved in all the normal ... responsibilities that we have, where they're a spouse, they're a parent."[30] This reality further brings psychological risks to military personnel engaged in remote warfare scenarios. These are risks that needs to be addressed at all level and both in planning and execution phases.

Another dimension to the blurred lines of conflict, especially within the information domain, is the increased ambiguity of the status of participants in a grey-zone conflict. For example, it is increasingly hard to perfectly identify the sources of a cyber attack and even harder

[29] Ehrhart, Hans-Georg. "Postmodern warfare and the blurred boundaries between war and peace." Institute for Peace Research and Security Policy, University of Hamburg, Defense & Security Analysis Vol. 33, No. 3, (2017). 271.

[30] McCammon, Sarah. "The Warfare May be Remote but the Trauma is Real." National Public Radio. Last accessed 05 May 2019. https://www.npr.org/2017/04/24/525413427/for-drone-pilots-warfare-may-be-remote-but-the-trauma-is-real

to determine if civilians engaged in such actions are to be considered Direct Participants in Hostilities.[31] This uncertainty will always come with some level of doubt for some military operators when they have to conduct operations against a target of that nature. *Is this a legitimate target?* is a question that will linger in one's mind as the blurred lines of grey-zone conflict makes it hard to clearly answer for certain. This question has a strong potential for the development of moral injuries and the chain of command must ensure that all possible actions are taken to provide personnel with clear targeting mechanisms and ways to voice and address concerns.

FIXING THE DOCTRINAL GAP

A Holistic Multi-Domain Doctrine

Having defined what are arguably the most significant threats and risks to personnel, it is now important to look at avenues to adapt the CAF's force protection doctrine to this new context of grey-zone conflicts and hybrid warfare. Even the CAF's primary guidance document, Canada's new Defence Policy: Strong, Secure, Engaged (SSE), highlights the fact that the "characteristics of conflict have changed significantly over the last 10 years." [32] It also clearly states that the CAF will need to account for and adapt to the grey-zone and hybrid warfare, as well as develop capabilities to operate in the space and cyber domains. [33] Concurrently, the new defence policy aims to improve significantly the support provided to CAF personnel, especially regarding health and resilience.[34] With the defence policy as a baseline framework, the emphasis

---

[31] Melzer, Nils. *Interpretative Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*. International Committee of the Red Cross. Geneva, Switzerland. May 2009. 38.

[32] Canada. Dept. of National Defence. *Strong, Secure, Engaged - Canada's defence policy*. Ottawa: Dept. of National Defence, 2017. 52

[33] *Ibid*., 53.

[34] *Ibid*., 26.

on psychological support to CAF personnel can and should be incorporated throughout existing doctrine. In this case, while SSE advocates for stronger support measures by the CAF Health System, its directing principles should be applied at large throughout doctrine. Psychological protection should be incorporated into the CAF's doctrine of Force Protection as it would make it more holistic and a better fit to the current context of multi-domain operations. This would allow for the harmonization of concepts and for the organic incorporation of psychological protection measures as part of planning and risk management. It would also serve to highlight the importance of psychological protection in the new operating environment as a function of command at all levels.

The current joint doctrine, despite being past its normal in-service life of five years as it was last updated in 2006, still have most of it right.[35] Stating that most "CAF operations are joint." has been both validated over time and reinforced by the new multi-domain warfare environment, which has furthered the necessity of 'jointness'. [36] One of the leading military organization with this view, the U.S. military, has embraced the concept of multi-domain operations and is now devoting significant resources to develop doctrine and capabilities to better operate in a joint fashion. The crux of this transition, according to Lieutenant-General Eric Wesley, director of the U.S. Army Capabilities Integration Center (now the U.S. Army Futures Command), is solving the problem of the "Multi-Domain Command & Control." [37] Consequent to this point of view, is that joint doctrine needs to be elevated to the level of an unified

---

[35] Canada. Dept. of National Defence. CFJP A1, *Doctrine Development Manual 3rd Edition (English)*. Ottawa: Dept. of National Defence, 2010. 1-2.

[36] Canada. Dept. of National Defence. CFJP 3-14, *CF Joint Force Protection Doctrine (English)*. Ottawa: Dept. of National Defence, 2006. i.

[37] Freedberg JR., Sydney J. "Services Wargaming Multi-Domain Consensus: Army 3-Star Futurist." Breaking Defense, 10 January 2019. Last accessed on 05 May 2019. https://breakingdefense.com/2019/01/services-wargaming-multi-domain-consensus-army-3-star-futurist/

multi-domain doctrine where it acts as the core reference that is supported by the individual environmental doctrine, and not the other way around. [38] Thus, the CAF Joint Force Protection Doctrine Manual should become the doctrinal core for Force Protection in the Multi-Domain environment.

From Mental Health to Psychological Protection

Currently, the psychological protection of CAF personnel is assured by various mental health programs and services provided by the CAF Chaplaincy, the CAF Health Services Group and other support organizations.[39] That said, it is important to highlight that while the effectiveness of the delivery of those programs and services is an important item to evaluate, that the aim here is only to look at the doctrine and policy surrounding those services. When looking at the current CAF policies surrounding mental and moral health, only a handful of Queen's Regulations and Orders (QR&O) and Defence Administrative Orders and Directives (DAOD) can be found. This very meek framework only establishes mental health as an administrative function where the practitioners are responsible to develop and implement its strategy. [40] It is not integrated with joint doctrine, which would allow for proper consideration of psychological protection during the planning and conduct of operations.

One area of existing CAF doctrine that touches on psychological protection is the Joint Doctrine Manual for Psychological Operations. However, this piece of doctrine is also past its

---

[38] Canada. Dept. of National Defence. CFJP 3-14, *CF Joint Force Protection Doctrine (English)*. Ottawa: Dept. of National Defence, 2006. i.

[39] Canada. Dept. of National Defence. "Mental Health Programs and Services." National Morale & Welfare Services. Last accessed on 05 May 2019. https://www.cafconnection.ca/National/Programs-Services/Mental-Health/Mental-Health-Programs-and-Services.aspx

[40] Canada. Dept. of National Defence. DAOD 5017-0, *Mental Health (English)*. Ottawa: Dept. of National Defence, Issued 2000-04-24.

in-service life with its last revision of January 2004.[41] It also only covers broad planning and conduct considerations related to countering enemy psychological operations, not actual psychological protection.[42] Its interpretation of psychological operations is also limited to traditional propaganda and information operations and does not account for the emerging tactics and strategies of the multi-domain environment. While this manual would also benefit from a significant overhaul, the aspects of psychological protections should not be isolated in a manual dedicated to the conduct of psychological operations. This updated manual should still cover doctrinal elements of Counter-Psyops but the overall concept of psychological protection would be ill-served being separated from the other fundamental aspects of Force Protection. The principal idea is that psychological protection needs to be part of a holistic Force Protection model aimed at considering all threats and risks to personnel. This view is already consequent with the current definition of Force Protection within the joint doctrine. [43]

Looking Outward

The concept of psychological protection, sometimes labeled psychological defence, has already been adopted by some countries at the collective level as part of their defence policy. Two notable examples are Sweden and Singapore. Under the context of grey-zone conflicts and Russian hybrid warfare operations, Sweden recently moved to reinvigorate its defence apparatus.[44] As part of this effort, Sweden coined a new concept as part of its new defence

---

[41] Canada. Dept. of National Defence. CFJP A1, *Doctrine Development Manual 3rd Edition (English)*. Ottawa: Dept. of National Defence, 2010. 1-2.

[42] Canada. Dept. of National Defence. CFJP 3-10.1, *Psychological Operations (English)*. Ottawa: Dept. of National Defence, 2004. 1-5.

[43] Canada. Dept. of National Defence. CFJP 3-14, *CF Joint Force Protection Doctrine (English)*. Ottawa: Dept. of National Defence, 2006. 1-1.

[44] Defense News. "Sweden Adopts Tougher Military Strategy Doctrine." Sightline Media Group. Last modified 17 March 2016. https://www.defensenews.com/global/europe/2016/03/17/sweden-adopts-tougher-military-strategy-doctrine/

policy: Total Defence. This concept includes both civil and military defence, and is aimed at ensuring a holistic and seamless barrier to protect against hostile activities in the grey-zone and against hybrid warfare threats.[45] This concept of total defence includes psychological defence at the collective level with the aim of maintaining "open and democratic society with freedom of expression even during extraordinary conditions."[46] Similarly, and with inspiration from Scandinavian countries, Singapore also adopted a similar concept of Total Defence, which includes psychological defence as one of its five pillars.[47]

While Canada does not have a similar concept for its defence policy, it has the same key components. However, both Singapore and Sweden highlight the importance of psychological protection in the current context right within their core policy. That said, psychological protection as a pillar of the Total Defence concept is not the same as psychological protection as a subset of Force Protection. One is aimed at protecting the society versus protecting individuals and groups of military personnel. However, the identified importance of psychological defence both at the societal and the individual level is the same in the context of grey-zone conflict and hybrid warfare.[48] It needs to be in place to mitigate the emerging threats and risks of that new context. While highly unlikely that Canada would see significant amendments to its defence policy in the short term, there is an opportunity to build up the concepts of psychological protection in the CAF doctrine and over time establish it as a core concept of Canada's Defence Policy.

---

[45] Sweden. Ministry of Defence. "Sweden's Defence Policy 2016 to 2020." Published 02 June 2015. 3.

[46] *Ibid*., 5.

[47] Singapore. Ministry of Defence. "The 5 Pillars of total Defence." Last accessed on 05 May 2019. https://www.mindef.gov.sg/oms/imindef/mindef_websites/topics/totaldefence/about_us/5_Pillars.html

[48] Carment, David and Belo, Dani. "War's Future: The Risks and reward of Grey-Zone Conflict and Hybrid Warfare." Canadian Global Affairs Institute. October 2018.

CONCLUSION

The CAF's ability to protect its forces against asymmetric threats remains relevant in the age of hybrid warfare and grey-zone conflict. The transition from the Industrial Age and to Information Age did not make attrition warfare disappear, it simply morphed toward psychological attrition vice physical losses. This changed nature brings a need to change the way the CAF value assets, capabilities, methods and tactics. Colonel Jason Brown, Commander 408th Wing, U.S. Air Force said that "In the 21st century, in the information age, war fighting is no longer a matter of geography; it's a mentality." [49] While there will seemingly always be a need for kinetic actions in the conduct of war, there is now an increased importance of actions on the psychological plane. It is the emerging psychological risks and threats that are defining hybrid warfare and grey-zone conflicts, not simply the technological advances in weaponry.

In that context, the presence of potent asymmetric threats to CAF personnel is more valid than ever, albeit aimed at their minds rather than their body. These threats need to be mitigated in the same way that traditional physical threats have been. Furthermore, operating in this new context comes with intrinsic risks to CAF personnel. New emerging technologies have given the ability to the CAF to conduct operations remotely and minimize the potential for casualties. However, these new technologies have not provided an effective shield against psychological harm. The new remote warfare capabilities also come with significant psychological risks as seen by the experience of the 408th Wing.

The CAF Force Protection doctrine is way past its in-service life. It requires a serious rewrite to account for the new intricacies of the current operating environment, and also to

[49] McCammon, Sarah. "The Warfare May be Remote but the Trauma is Real." National Public Radio. Last accessed 05 May 2019. https://www.npr.org/2017/04/24/525413427/for-drone-pilots-warfare-may-be-remote-but-the-trauma-is-real

integrate psychological protection to its Force Protection model. This addition would serve to provide commanders and staff at all level a holistic framework to protect CAF personnel when planning and conducting operations. Psychological protection is not solely a question of mental health addressed by healthcare professionals, but part of a unified doctrine aimed at preserving the freedom of action and operational effectiveness by countering all threats to all its elements, including its personnel.[50]

[50] Canada. Dept. of National Defence. CFJP 3-14, *CF Joint Force Protection Doctrine (English)*. Ottawa: Dept. of National Defence, 2006. 1-1.

BIBLIOGRAPHY

Barry R. Schneider and Lawrence E. Grinter. “Battlefield of the Future: 21st Century Warfare Issues”. Honolulu, HI: University Press of the Pacific, 2002.

Baudrillard, Jean. “Simulacra and simulation”. Ann Arbor: University of Michigan Press. 1994.

Blackwell, Tom. “Russian fake-news campaign against Canadian troops in Latvia includes propaganda about litter, luxury apartments.” National Post. Last accessed on 05 May 2019. https://nationalpost.com/news/canada/russian-fake-news-campaign-against-canadian-troops-in-latvia-includes-propaganda-about-litter-luxury-apartments

Boucher, Jean-Christophe. “Hybrid Warfare and Civil-Military Relations.” Canadian Global Affairs Institute (CGAI). Policy Update. December 2017.

Canada. Dept. of National Defence. CFJP A1, *Doctrine Development Manual 3rd Edition (English)*. Ottawa: Dept. of National Defence, 2010.

Canada. Dept. of National Defence. CFJP 3-14, *CF Joint Force Protection Doctrine (English)*. Ottawa: Dept. of National Defence, 2006.

Canada. Dept. of National Defence. CFJP 3-10.1, *Psychological Operations (English)*. Ottawa: Dept. of National Defence, 2004.

Canada. Dept. of National Defence. *Code of Values and Ethics (English)*. Ottawa: Dept. Of National Defence, 2012.

Canada. Dept. of National Defence. DAOD 5017-0, *Mental Health (English)*. Ottawa: Dept. of National Defence, Issued 2000-04-24.

Canada. Dept. of National Defence. “Mental Health Programs and Services.” National Morale & Welfare Services. Last accessed on 05 May 2019. https://www.cafconnection.ca/National/Programs-Services/Mental-Health/Mental-Health-Programs-and-Services.aspx

Canada. Dept. of National Defence. *Summary of Duty with Honour - The Profession of Arms in Canada (English)*. Ottawa: Dept. Of National Defence, 2003.

Canada. Dept. of National Defence. *Strong, secure, engaged - Canada's defence policy*. Ottawa: Dept. of National Defence, 2017.

Carment, David and Belo, Dani. *War's Future: The Risks and reward of Grey-Zone Conflict and Hybrid Warfare*. Canadian Global Affairs Institute. October 2018.

Defense News. "Sweden Adopts Tougher Military Strategy Doctrine." Sightline Media Group. Last modified 17 March 2016. https://www.defensenews.com/global/europe/2016/03/17/sweden-adopts-tougher-military-strategy-doctrine/

Ehrhart, Hans-Georg. "Postmodern warfare and the blurred boundaries between war and peace." Institute for Peace Research and Security Policy, University of Hamburg, Defense & Security Analysis Vol. 33, No. 3, (2017).

Freedberg JR., Sydney J. "Services Wargaming Multi-Domain Consensus: Army 3-Star Futurist." Breaking Defense, 10 January 2019. Last accessed on 05 May 2019. https://breakingdefense.com/2019/01/services-wargaming-multi-domain-consensus-army-3-star-futurist/

Galliot, Jai C. "Uninhabited Aerial Vehicles and the Asymmetry Objection: A Response to Strawser". Journal of Military Ethics, 11:1. 2012. 58-66.

Gasser, Urs. "What Makes Information Valuable? Information Quality, Revisited". *Berkman Klein Center for Internet & Society*. Harvard University. Retrieved at: https://medium.com/berkman-klein-center/what-makes-information-valuable-information-quality-revisited-4ceb5ee11048 on 24 April 2019.

Knowles, Emily and Watson, Abigail. "No Such Thing as A Quick Fix - The Aspiration-Capabilities Gap in British Remote Warfare." *Remote Warfare Program*. Oxford Research Group. 2018.

Lapowsky, Issie. "NATO Group catfished Soldiers to Prove a Point About Privacy." WIRED Magazine. 18 February 2019. Last accessed 05 May 2019. https://www.wired.com/story/nato-stratcom-catfished-soldiers-social-media/

Ling, Justin. "In Latvia, Canadian and Italian forces stand on guard with NATO against Russian expansion." The Globe and Mail. 11 June 2018. Last accessed on 05 May 2019. https://www.theglobeandmail.com/world/article-in-latvia-nato-forces-stand-on-guard-against-russian-expansion/

Maan, Ajit. "Narrative Warfare" CreateSpace Independent Publishing Platform, 03 April 2018.

Mazarr, Michael J. "Mastering the Gray Zone: Understanding a Changing Era of Conflict." Strategic Studies Institute, US Army War College, 2015.

McCammon, Sarah. "The Warfare May be Remote but the Trauma is Real." National Public Radio. Last accessed 05 May 2019. https://www.npr.org/2017/04/24/525413427/for-drone-pilots-warfare-may-be-remote-but-the-trauma-is-real

Melzer, Nils. Interpretative Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law. International Committee of the Red Cross. Geneva, Switzerland. May 2009.

North Atlantic Treaty Organization. AJP 3-4, *Allied Joint doctrine for Force Protection*. NATO Standardization Office. Edition A Version 1 April 2015.

Ohlin, Jens David. *Research Handbook on Remote Warfare*. Edward Elgar Publishing, Incorporated. 2017.

Singapore. Ministry of Defence. "The 5 Pillars of total Defence." Last accessed on 05 May 2019. https://www.mindef.gov.sg/oms/imindef/mindef_websites/topics/totaldefence/about_us/5_Pillars.html

Steiner, Peter. "On the Internet Nobody Knows You're a Dog." *New Yorker*. 5 July 1993.

Sweden. Ministry of Defence. "Sweden's Defence Policy 2016 to 2020." Published 02 June 2015. Accessed at https://www.government.se/49c007/globalassets/government/dokument/forsvarsdepartementet/sweden_defence_policy_2016_to_2020

United Nations. "United Nations Security Council Resolution 1566 (2004)." United Nations Security Council. Adopted 8 October 2004.

United States of America. Department of Defence. *Report of the DOD Commission on Beirut International Airport Terrorist Act, October 23, 1983*. 1983. Retrieved at https://fas.org/irp/threat/beirut-1983.pdf

United States of America. Department of Veterans Affairs. *Moral Injury in the Context of War*. National Center for PTSD. Last accessed on 05 May 2019. https://www.ptsd.va.gov/professional/treat/cooccurring/moral_injury.asp

Whitty, M. T., & Buchanan, T. "The online dating romance scam: The psychological impact on victims – both financial and non-financial". *Criminology & Criminal Justice*, 16(2). 2016. 176–194.