National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CHINA AND GRAY ZONE OPERATIONS: THE NEED FOR A MODERN CANADIAN NATIONAL SECURITY APPARATUS

Lieutenant-Commander Anonymous

JCSP 49

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 n° 49

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 49 - PCEMI n° 49
2022 - 2023

Exercise Solo Flight – Exercice Solo Flight

CHINA AND GRAY ZONE OPERATIONS: THE NEED FOR A MODERN CANADIAN NATIONAL SECURITY APPARATUS

Lieutenant-Commander Anonymous

CHINA AND GRAY ZONE OPERATIONS:
THE NEED FOR A MODERN CANADIAN NATIONAL SECURITY APPARATUS

INTRODUCTION

In his classic work *The Art of War,* the ancient Chinese strategist and philosopher Sun Tzu wrote, "subjugating the enemy's army without fighting is the true pinnacle of excellence."[1] Expanding on this tenet of Master Sun's philosophy in 1999, People's Liberation Army (PLA) Colonels Qiao Liang and Wang Xiangsui published *Unrestricted Warfare* which outlined how the PLA might reinvigorate the, "'most basic article' of ancient Chinese warfare, a technique they call the 'side principle.'"[2] This 'side principle' can essentially be interpreted to mean, "avoiding clashing with an enemy's powerful sword to cut into the warrior's exposed side."[3] For the PLA and the leadership of the People's Republic of China (PRC) (as manifested by the Chinese Communist Party [CCP]), Qiao and Wang's work reinvigorated the idea of, "multi-domain, whole-of-government engagement to achieve political objectives while avoiding conventional military confrontation."[4] Many of the ideas theorized by Qiao and Wang have since been implemented into CCP and PLA policy and doctrine and provide useful insight for understanding what is loosely understood to be China's 'gray zone' strategy.

In their study of gray zone warfare, researchers Azad, Haider and Sadiq argue that, "the terms 'hybrid warfare,' 'gray zone warfare,' and 'ambiguous warfare' have received unprecedented attention in recent years."[5] For them the, "changing nature of warfare has been defined and categorized in diverse ways leading to numerous perspectives revealing more confusion than clarity."[6] Indeed, Russian General, Makmut alluded to this challenge when he said, "If the employment of any non-military means is a war, then the whole of human history is war…"[7] For General Makmut, "conceptualizing non-military confrontations as wars is unhelpful … because most of the required actions and counter-actions *do not fall under the military's responsibility* (emphasis added)."[8]

It is the latter half of Makmut's statement that this paper seeks to address. As Azad notes, "many contemporary conflicts are neither black nor white; instead, they fall in the middle of the two: the gray zone."[9] If this statement is accepted as true (and there is

---

[1] Sun Tzu. *The Art of War* in *The Seven Military Classics of Ancient China.* Translated by Ralph Sawyer. Boulder, CO: Westview Press, 1993.
[2] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Panama City, Panama: Pan American Publishing Company, 1999), xvii.
[3] Qiao, *Unrestricted*, xiii.
[4] Matt Peterson, "Competition and Decision in the Gray Zone: A New National Security Strategy." *The Strategy Bridge*, 20 April 2021.
[5] Azad, T.M., M.W. Haider, and Sadiq, M. 'Understanding Gray Zone Warfare From Multiple Perspectives'. *World Affairs* 186, no. 1 (2023): 81–104. https://doi.org/10.1177/00438200221141101.
[6] Azad, Haider, and Sadiq, "Understanding," 81.
[7] Thompson, Jason. 'Hybrid Warfare: Redefining and Responding to Hostile Intent'. *Canadian Military Journal* 22, no. 3 (Summer 2022): 62–70.
[8] Thompson, "Hybrid," 64.
[9] Azad, Haider, and Sadiq, "Understanding," 81.

much evidence to support this claim, as this paper will show), then the question must be asked, what is the Canadian national security apparatus doing to counter and combat Chinese gray zone activities? In order to answer this question, this paper will examine: 1) Chinese activity in 'cyberspace'; 2) Chinese gray zone activity in the physical realm (primarily focusing on activity in the South and East China Seas); and 3) Chinese activity in the information environment. Subsequently this paper will examine the Canadian response to growing Chinese gray zone activities (or lack thereof) and the challenges associated with delegating responsibility for Canadian responses to gray zone warfare entirely to the Canadian Armed Forces. In so doing, this paper will argue that the Canadian national security apparatus is not appropriately configured to counter, compete or combat Chinese gray zone operations that aim to challenge the Rules-Based International Order (RBIO) which Canada seeks to uphold and defend.

THE GRAY ZONE AND CYBER OPERATIONS

In order to ensure clarity throughout this paper, it is first necessary to define some key terms. In 2016, Hoffman argued, "that the biggest challenge of our times is to identify war – as we do not know what war is and what war is not."[10] Azad et al. posited in 2023 that, "Hoffman's position remains solid because the boundaries between war and peace have been increasingly blurred."[11] This phenomenon among the academic community only strengthens the argument for working definitions for critical concepts.

The term 'gray zone' was first used in 2010 and, "broadly depicts multi-dimensional activities aimed to alter adversary behavior while remaining below the threshold of conventional military employment." Azad et al. posit that, "'little green men,' cyber exploitation and disinformation, are the common themes in the gray zone."[12] As such, and to ensure maximum inclusivity with respect to possible gray zone activities, this paper will define 'gray zone warfare' and its strategies as the US Special Operations Command does:

> Competitive interaction among and within state and non-state actors that fall between the traditional war and peace duality. They are characterized by ambiguity about the nature of the conflict, the opacity of the parties involved, or uncertainty about the relevant policy and legal frameworks.[13]

A common misconception that frequently occurs is that the terms 'gray zone warfare' and 'hybrid warfare' are interchangeable.[14] They are not. The difference is that kinetic means belong solely to the realm of 'hybrid warfare' whereas, "gray zone warfare is limited to non-kinetic means."[15]

---

[10] Azad, Haider, and Sadiq, "Understanding," 84.
[11] Azad, Haider, and Sadiq, "Understanding," 84.
[12] Azad, Haider, and Sadiq, "Understanding," 84.
[13] Azad, Haider, and Sadiq, "Understanding," 87.
[14] Azad, Haider, and Sadiq, "Understanding," 93.
[15] Azad, Haider, and Sadiq, "Understanding," 93.

The term 'cyberwar' was originally coined by John Arquilla in 1993 and, at the time was, "characterized as the disruption or destruction of information and communication systems at the military level."[16] This definition has been expanded and clarified since its inception and today the US Joint Publication for Cyberspace Operations refers to cyberspace as:

> the domain within the information environment that consists of the interdependent network of information technology (IT) infrastructures and resident data. It includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace operations (CO) is the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.[17]

The necessarily all-encompassing definition above provides a framework wherein just about anything and everything used in modern military operations has some element of 'cyber' associated with it. This is not necessarily a negative and the remainder of this section aims to highlight how China can be seen to be embracing the all-encompassing nature of cyberspace for its own benefit.

Much of the modern literature surrounding cyber operations highlights some of the more extraordinary potentials of cyber operations. Indeed in Arquilla's own latest book, *Bitskrieg,* he outlines a scenario that sees, "a war in the waters off east Asia."[18] In such a scenario one could expect to see, "American aircraft carrier strike groups being struck by smart, often automated weapons . . . all while the sophisticated battle management systems upon which the U.S. Navy relies are hacked, crippling the operational tempo of the fleet."[19] While this scenario *may* one day come to fruition, it is argued by researchers Harknett and Smeets that this extraordinary scenario (and others like it) may not be the most beneficial for providing insight into the far more prevalent cyber operations that are being routinely conducted by China and other state and non-state actors.[20]

For Harknett and Smeets, it is important (especially with respect to China) to differentiate between a 'cyber operation' and a 'cyber campaign.'[21] For them, a cyber operation, "refers to a series of coordinated actions directed towards a computer or network in order to achieve a certain operational objective."[22] They argue that cyber operations can have a myriad of objectives from espionage or "to cause disruption, denial, degradation, or destruction," in military systems or civilian infrastructure alike, for example. On the other hand, a cyber campaign, "refers to a series of coordinated

---

[16] Arquilla, John, and David Ronfeldt. *Cyberwar Is Coming!* Web Only: RAND Corporation, 1993.
[17] JP 3-12 pg 1-1
[18] Tiezzi, Shannon. 'John Arquilla on the New Challenge of Cyberwarfare'. *The Diplomat*, 14 September 2021.
[19] Tiezzi, "John," 1.
[20] Harknett, Richard J., and Max Smeets. 'Cyber Campaigns and Strategic Outcomes'. *Journal of Strategic Studies* 45, no. 4 (2022): 534–67
[21] Harknett, and Smeets, "Cyber Campaigns," 541.
[22] Harknett, and Smeets, "Cyber Campaigns," 541.

cyber operations, which take place over time, to achieve a cumulative outcome leading to strategic advantage."[23] They argue that a cyber campaign can vary greatly in terms of the number and affiliation of threat groups conducting a single campaign as well as their duration and finally that the result of a cyber campaign may noy yield an, "immediate strategic outcome."[24]

Harknett and Smeets posit that there is an ever-growing body of evidence to, "uncover Chinese cyber activity as campaigns."[25] Indeed, they highlight recent findings that, "have been able to track various espionage activity directly back to units… of the PLA's General Staff department."[26] While some scholars argue that China's ability to conduct espionage and theft (including of highly classified US stealth aircraft technology) is great; their ability to turn it into a competitive advantage is lacking.[27] While, it is true that China has not reached parity with the US in terms of stealth technology, Harkneet and Smeets argue, China is still likely far ahead of the next nearest competitors and, critically, have situational awareness of weaknesses in US designs. This, they argue, is but one example of a long duration cyber campaign.[28]

Fundamentally, Harknett and Smeet conclude that, "we should study cyber means not as enablers of war, although they can be, but more critically as the strategic alternative to it."[29] Their conclusions call for new research that, "starts with the premise that strategic cyber competition could be pursued with the same intent and overall objective traditionally associated with war, but achieve those ends through other means."

GRAY ZONE TACTICS IN THE SOUTH CHINA SEA

This paper will now seek to highlight Chinese gray zone tactics, as they pertain to their physical environment. In order to do so, it will use the People's Armed Forces Maritime Militia (PAFMM) as a case study to outline the thinking and strategies employed by the CCP to reject the tenets of the RBIO and further its strategic goals. While the PAFMM is certainly not the sole Chinese institution that operates outside of established international norms as a means of Chinese influence (the Belt and Road Initiative [BRI] or Confucius Institutes could provide similar insight), this author finds the PAFMM's activities sufficiently egregious as to warrant close examination.

Luo and Panter succinctly articulate that the PAFMM (and similar institutions like China's Deep Water Fishing Fleets), "help China rewrite the rules of freedom of navigation, buttress its maritime claims, secure vital resources, and extend its economic reach across globe,"[30] while remaining below the threshold of open conflict. Further, they

---

[23] Harknett, and Smeets, "Cyber Campaigns," 541.
[24] Harknett, and Smeets, "Cyber Campaigns," 542.
[25] Harknett, and Smeets, "Cyber Campaigns," 550.
[26] Harknett, and Smeets, "Cyber Campaigns," 553.
[27] Harknett, and Smeets, "Cyber Campaigns," 553.
[28] Harknett, and Smeets, "Cyber Campaigns," 553.
[29] Harknett, and Smeets, "Cyber Campaigns," 558.
[30] Suxian Luo, and Jonathan Panter, "China's Maritime Militia and Fishing Fleets A Primer for Operational Staffs and Tactical Leaders." *Military Review China Reader Special Edition*, (September 2021): 7

postulate that, "the strength of the maritime militia is its deniability, which allows its vessels to harass and intimidate foreign civilian craft and warships while leaving the PRC room to deescalate by denying its affiliation with these activities."[31]

According to official Chinese policy, the PAFMM exists to complement the China Coast Guard (CCG)[32] and is positioned to support a, "people's war at sea," in any future conflict.[33] A 2013 Chinese White Paper stated the PAFMM would, "serve as an assistant and a backup force of the PLA in . . . defending China from external threats."[34] According to legal experts James Kraska and Michael Monti, "this strategy exploits a seam in the law of naval warfare, which protects coastal fishing vessels from capture or attack unless they are integrated into the enemy's naval force."[35]

According to Chinese doctrine, the PAFMM is defined as, "an armed mass organization composed of civilians retaining their regular jobs . . . and an auxiliary and reserve force of the PLA."[36] It, "consists of citizens working in the marine economy who receive training from the PLA and CCG."[37] If called upon, PAFMM vessels and personnel could be employed by the Chinese state to conduct, "border patrol, surveillance and reconnaissance, maritime transportation, search and rescue, and auxiliary tasks in support of naval operations in wartime."[38]

In 2015, researcher Michael Mazarr described China's national, overarching strategy as one in pursuit of, "regional hegemony to gain control of specific resources and counterbalance, and eventually replace, U.S. geopolitical preeminence in Asia."[39] In order to achieve this aim, the PAFMM, as a gray zone institution, operates in contravention to several international rules and norms. First and foremost, is the principle of 'distinction.' Distinction falls under international humanitarian law and is designed to, "protect civilians and ameliorate the effects upon them in warfare."[40] Given that PAFMM personnel operate primarily as a non-uniformed force in non-state-identified vessels, it is virtually impossible to satisfy the principle of distinction when they are carrying out military duties on behalf of the Chinese state. In times of peace, this is problematic; in times of conflict, it has the potential for catastrophic consequences with respect to discerning a valid military target vessel from an innocent fishing vessel.

---

[31] Luo, "Maritime Militia," 16.
[32] Alessio Patalano, "When Strategy is 'hybrid' and not 'grey': reviewing Chinese military and constabulary coercion at sea," *The Pacific Review* 31, no. 6 (Jan 2019): 822.
[33] Alexander Huang, *The PLA Navy at War: 1949–1999*, *in* Mark A. Ryan, David Michael Finkelstein & Michael A. McDevitt, *Chinese Warfighting: the PLA Experience Since* 1949, (2003): 266.
[34] Patalano, "Strategy," 822.
[35] James Kraska and Michael Monti, "The Law of Naval Warfare and China's Maritime Militia," *International Law Studies US Naval War College* 91 (2015): 451.
[36] "Zhonghua renmin gongheguo minbing gongzuo tiaoli" [Decree of the PRC on militia work], Central Military Commission of the People's Republic of China, December 1990, accessed 20 November 2020.
[37] Luo, "Maritime Militia," 12.
[38] Luo, "Maritime Militia," 12.
[39] Michael Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (U.S. Army War College Press, 2015), 81.
[40] Kraska, "Law," 458.

Secondly, the PAFMM (and similar Chinese institutions) aim to exploit the international interpretation of maritime borders within the South China Sea. Although a signatory of the 1982 United Nations Convention on the Law of the Sea (UNCLOS), China's ambitions to claim, and if necessary, build, land masses from which to extend its influence is clearly a task ideally suited to the PAMFF. By maintaining a large number of non-descript, pseudo-state acting vessels near strategically sensitive features in the South China Sea, the Chinese government has a seemingly infinite number of ISR platforms that can rapidly be called upon to take state-sponsored action to support national (illegal) interests.

As was noted at the outset of this section, the PAMFF is not the only Chinese institution to operate in the gray zone in the physical world. There are equally nefarious operations being conducted under the umbrella of the BRI. Confucius Institutes exist on post-secondary campuses across Canada. A 2022 Canadian news article reported that Canada's federal police force was investigating Chinese 'police' stations operating in Canadian cities. The result of these gray zone operations (and others) as perpetrated by the Chinese government is greater than the sum of its parts. Fundamentally they aim to normalize behaviour that is inconsistent with international laws, rules, by playing the long game and never crossing the thresholds that might elicit a forceful response from the community of nations.

THE GRAY ZONE AND INFORMATION OPERATIONS

This section aims to highlight China's use of the Information Domain as a means of operating in the gray zone and advancing national strategic objectives. As with section pertaining to cyber operations, this paper will first endeavour to outline some foundational concepts and definitions.

Much like with cyber operations, there are a myriad of terms that are often used interchangeably within the Information environment but have different and distinct meanings. An example of this is the use of the terms 'misinformation' and 'disinformation.' Bachmann et al. provide a credible breakdown of how these terms differ:

> We define disinformation, as a subset of misinformation, as false or misleading information that is spread deliberately to deceive. It entails three components to unpack. First, agency as a part of a strategy. Disinformation is intentional where misinformation can be incidental or unwitting. Second, disinformation requires mechanisms to propagate. Intentionally designed disruptive narratives cannot achieve intended effects unless they reach larger audiences. Simply put, disinformation must spread to work. Third, unlike misinformation, disinformation has

discernable objectives. These objectives range from obfuscation to distrust, disruption, and destabilization.[41]

A second piece of foundational background concerning China in the Information environment is the concept of the, 'Three Warfares.' Approved in 2003 by the CCP Central Committee and the Central Military Commission, the three warfares consist of "Public Opinion; Psychological Warfare; and Legal Warfare,"[42] (sometimes these are referred to as "political warfare; public opinion warfare; and Legal Warfare"[43]).

Most contemporary scholarly literature is in agreement that the world is witnessing a return to great power competition unlike anything seen since the end of the Cold War. "Great power competition entails the distribution of relative gains with no finite terminal objectives."[44] In this context, Bachmann et al. posit that,

"it is not hard to see how information warfare plays a critical role in shaping how the great powers are competing in key issue areas."[45] They continue that, "major powers use weaponized narratives to sow internal discord and distrust, rendering their adversaries unable to focus on external threats."[46]

Complementary to Bachmann et al.'s assessments above, information and cyber experts, Ronfeldt and Arquilla, "urge strategists to consider a new concept for adapting U.S. grand strategy to the information age — noopolitik, which favors the use of 'soft power'— as a successor to realpolitik, with its emphasis on 'hard power.'"[47] The concept of the 'noosphere' was originally proposed in 1999 and described, "a global 'thinking circuit' and 'realm of the mind' upheld by the digital information revolution."[48] They argue that as the noosphere expands, "the conditions for traditional realpolitik strategies will erode, and the prospects for noopolitik strategies will grow. Thus, the decisive factor in today's and tomorrow's wars of ideas is bound to be "whose story wins"—the essence of noopolitik."[49]

Incorporating these theoretical frameworks into the realm of the practical; observers note that Beijing (as well as Moscow), "use digital media platforms and other information warfare capabilities not only to consolidate their authoritarian rule, but also to undermine and disrupt the liberal international order that the United States and its

---

[41] Bachmann, Sascha-Dominik Dov, Doowan Lee, and Andrew Dowse. 'COVID Information Warfare and the Future of Great Power Competition'. *The Fletcher Forum of World Affairs* 44, no. 2 (Summer 2020): 11–18.

[42] Bachmann, Doowan, and Dowse, "COVID," 14.

[43] Martin, Garrett. 'China's Strategic Devaluing of American Social Capital'. *Journal of Strategic Security* 16, no. 1 (2023): 1–18.

[44] Bachmann, Doowan, and Dowse, "COVID," 12.

[45] Bachmann, Doowan, and Dowse, "COVID," 13.

[46] Bachmann, Doowan, and Dowse, "COVID," 13.

[47] Ronfeldt, David, and John Arquilla. *Whose Story Wins: Rise of the Noosphere, Noopolitik, and Information-Age Statecraft*. Santa Monica, Calif.: RAND Corporation, 2020.

[48] Ronfeldt and Arquilla, *Whose Story Wins,* iii.

[49] Ronfeldt and Arquilla, *Whose Story Wins,* iii.

allies have buttressed."[50] In recent history, for example, "the CCP has aggressively promoted patently false narratives about the origin of the coronavirus."[51] Additionally, "it has actively promoted the Party's public health 'leadership' using automated accounts, bots, and trolls, despite numerous frauds and defects noticed in several countries."[52] Furthermore, the CCP continues to focus, "on the 'cognitive' domain of information operations and aims to precondition the political, strategic, operational, and tactical arenas in the short and long run."[53] In sum, Bachmann et al. conclude that, "Beijing's information warfare is becoming increasingly sophisticated, powered by the use of artificial intelligence and aimed at overall 'thought management.'"[54]

The effectiveness of China's information activities fundamentally stems from the tight control the CCP over all elements of national power. At the heart of the issue (from a western perspective) is that China and the CCP are situated in a perfect position to play the long game strategically. With power so centrally located within the single party framework – and at the top of the party apparatus at that – control is extremely centralized and can be efficiently coordinated, sequenced, and phased to meet strategic aims. The reason China has been so successful with its gray zone strategies is that they are all controlled from the party's centre and are therefore complementary in nature. A hiccup in the cyber domain can be overcome by actions in the information or physical domains or vice versa. The agility with which China is moving about in the gray zone to achieve its intent has seemingly caught the West and Canada off guard. Examples of China's gray zone activities are plentiful and ongoing. They include the extended incarceration of Michael Spavor and Michael Kovrig in retaliation for the lawful arrest of Meng Wanzhou; the spy balloon incident of 2023; recent allegations that Canadian Conservative member of parliament, Michael Chong and his family were the subjects of Chinese intimidation tactics; and even as this paper is being written, there is an investigation being conducted by a former Governor General concerning Chinese interference in the last Canadian federal election. In order to remain competitive and promote and defend the RBIO that China aims to upset; a coordinated effort is needed.

CANADA AND GRAY ZONE WARFARE

This paper will now turn inward to examine Canada's response to increasing PRC gray zone activities. This section aims to highlight the challenges Canada is facing with respect to countering Chinese gray zone activities and ultimately demonstrate that the CAF alone, is not a sufficient resource to counter Chinese gray zone activities.

It is both important and necessary to examine Canada's response to increased Chinese gray zone activities in the context of history. Since the end of the Second World War (at least), Canada has enjoyed the benefits of being physically isolated from the world's major conflict zones. It has large oceans on three sides and a friendly, global hegemon as its neighbour to the south with whom it shares a robust continental defence

[50] Bachmann, Doowan, and Dowse, "COVID," 13.
[51] Bachmann, Doowan, and Dowse, "COVID," 13.
[52] Bachmann, Doowan, and Dowse, "COVID," 13.
[53] Bachmann, Doowan, and Dowse, "COVID," 13.
[54] Bachmann, Doowan, and Dowse, "COVID," 13.

arrangement. Canada had not been the target of an attack and, as such, participated largely in wars of choice (binded by international partnerships and agreements) vice wars based on defence of its territorial sovereignty. Given this reality, the CAF was (rightly) seen as the main, if not only, institution to deal with matters of national defence and/or military conflict and Canadian citizens (justifiably) largely grew complacent about threats to Canada.

In a more recent context, the CAF has largely been marred by a number of arisings that has caused attention to be shifted, both within and external to the CAF, away from its primary mandates. A sexual misconduct and professional conduct crisis rose to the fore in 2015 and continues to occupy the minds of senior institutional leadership; the 'politics' of Canadian military procurement led to, and continues to cause, delays to the delivery of new equipment; the numbers of personnel across the entire force began to attrit at an alarming rate which often put missions, training, and exercises in jeopardy; and finally the global COVID-19 pandemic exacerbated the aforementioned problems and created a host of new ones. This is the Canadian context in which China has been continuing to develop, resource, and enable gray zone activity in support of its interests – including activities aimed at Canada.

Beginning from a purely CAF perspective, the most noteworthy aspect of Canadian military doctrine pertaining to countering any form of gray, hybrid, cyber, or information warfare is its deafening silence on the topics. The Canadian Forces Joint Publication (CFJP 01) – the CAF's capstone doctrinal document – makes absolutely no mention of gray, hybrid, or cyber warfare. It alludes (relevantly) to the Information domain only once stating that military forces are instruments of national power of last resort and are normally deployed, "when the diplomatic, *informational* (emphasis added), and economic instruments are not sufficient to realize the strategic goals."[55] This statement, as it is written, seemingly considers (incorrectly) that the *informational* environment to be something that military forces play no part in. Here again, context is important, in that CFJP 01 was published in 2009 and there have not been any updates since. In 2009, the CAF was engaged in conflict in Afghanistan against an enemy force that looked nothing like the modern PLA and employed strategies and tactics that were equally dissimilar.

Moving up the hierarchy of defence-related publications, Canada's 2017 Defence Policy, *Strong, Secure, Engaged* (SSE) at least makes mention of gray and hybrid warfare. Indeed it allocates one paragraph to the subject, acknowledging that, "State and non-state actors are increasingly pursuing their agendas using hybrid methods in the "grey zone" that exists just below the threshold of armed conflict."[56] It later indicates that such methods, "involve the coordinated application of diplomatic, informational, cyber, military and economic instruments to achieve strategic or operational objectives. They often rely on the deliberate spread of misinformation to sow confusion . . . and maintain deniability."[57] Nonetheless, in other sections of the document, SSE does accurately

---

[55] Government of Canada. "Canadian Forces Joint Publication 01: Canadian Military Doctrine." Issued April 2009, 0204.

[56] "Strong, Secure, Engaged: Canada's Defence Policy," 53.

[57] "Strong, Secure, Engaged: Canada's Defence Policy," 53.

articulate that "as a trading nation and influential member of the G7, G20, NATO and United Nations, Canada benefits from global stability underpinned by a rules-based international order."[58] Finally (and encouragingly), SSE stipulates, "activities in the South China Sea highlight the need for all states in the region to peacefully manage and resolve disputes in accordance with international law, and avoid coercion and other actions that could escalate tension."[59]

At the National Strategic level, Canada's 2022 Indo-Pacific Strategy is unusually direct in stating that, "China is an increasingly disruptive global power."[60] This national strategy document places great emphasis on strengthening allies and partnerships within the Indo-Pacific region in order to secure and enforce the RBIO from which China has benefitted in its rise as a global power. It states, "China is looking to shape the international order into a more permissive environment for interests and values that increasingly depart from ours."[61] Furthermore it stipulates that, "in areas of profound disagreement, we will challenge China, including when it engages in coercive behaviour—economic or otherwise—ignores human rights obligations or *undermines our national security interests* and those of partners in the region,"[62] (emphasis added).

The final Canadian policy document that this section will address is the CAF-generated (draft) *Pan-Domain Force Employment Concept* (PFEC). This document is by far the most relevant, all-encompassing, and forward-looking outline for the Canadian national security community in terms of how to deal with modern security threats including gray zone actors. On the premise that Canada is in an ongoing state of, "competition, confrontation, and potentially, conflict,"[63] it states that Canada, "can no longer base our thinking and planning on a simplistic binary conception of war and peace."[64] It acknowledges and indeed highlights that, "our adversaries are challenging us in the cyber, space, and information domains,"[65] in addition to the conventional domains and argues that, "we must meet this challenge across all domains."[66] Perhaps most importantly, it declares that CAF, "cannot deter or defeat the aggression of these powers alone."[67] Ultimately, the PFEC succinctly articulates, "overall, our environment demands new perspectives and a tailored set of military capabilities, integrated across domains, and applied in concert with other instruments of national power. We must adapt."[68]

As a foundational or capstone document to bring the Canadian national security apparatus into the twenty-first century, the PFEC is what Canada needs. It is clear that China is operating across all the domains available to it and has been for some time.

---

[58] "Strong, Secure, Engaged: Canada's Defence Policy," 50.
[59] "Strong, Secure, Engaged: Canada's Defence Policy," 50.
[60] "Canada's Indo-Pacific Strategy," 7.
[61] "Canada's Indo-Pacific Strategy," 7.
[62] "Canada's Indo-Pacific Strategy," 7.
[63] Government of Canada. "Pan-Domain Force Employment Concept: Prevailing in a Dangerous World." Current Approval AY 22/23, 4.
[64] "Pan-Domain Force Employment Concept," 4.
[65] "Pan-Domain Force Employment Concept," 4.
[66] "Pan-Domain Force Employment Concept," 4.
[67] "Pan-Domain Force Employment Concept," 4.
[68] "Pan-Domain Force Employment Concept," 4.

Admittedly, in many ways, the CCP's autocratic rule enables a level of political manoeuvre that is often unavailable to democracies such as Canada, however if Canada is to defend the RBIO and continue to reap the benefits it provides, implementation of a governance strategy like the PFEC is required and overdue.

There is reason however to be optimistic. A national security apparatus such as the one the PFEC outlines has proven to be achievable in other democracies. In a 2022 article in the *Canadian Military Journal*, Jason Thompson (a CAF Major) articulates how, in recent years, the UK has, "taken an innovative and forward-looking approach to its national security and national defence requirements."[69] At the core of the British model, is the *National Security Strategy and Strategic Defence and Security Review.* This is a, "capstone document that is updated and reviewed every 12 to 18 months."[70] Articulated within it is, "a pledge to exploit the full spectrum of available capabilities to respond to state-based threats, a promise to develop tough and innovative cyber security measures, and a commitment to . . . increase innovation and collaboration."[71] The real strength of the British model however lies in its 'fusion' approach across national security lines and its understanding that, "collaboration without specific authorities and responsibilities is ineffective.[72] To counter ineffective implementation of national assets and resources, the British government again came up with an appropriate solution: the Strategic Defence and Security Review Implementation Sub-Committee.[73] This sub-committee, "is chaired by the Chancellor of the Exchequer (Minister of Finance) and is empowered to address structural, policy and legal barriers to effective "Fusion." Furthermore, it is tasked to, "hold committee chairs and members accountable for their actions and reallocate resources and capabilities between departments to ensure that threats are addressed quickly and effectively."[74]

The British model outlined above demonstrates what a democratically-elected government is capable of achieving, in terms of national security apparatus and governance, when motivated to do so. However, as researcher and former Special Advisor (Policy) at Canada's Maritime Forces Pacific Headquarters James Boutilier states, "we (Canada) want to be at the table, but we are not prepared to do what the Australians call 'the hard yards.'"[75] Concerning the Indo-Pacific region, as a whole, Boutilier believes, "Ottawa has failed abjectly to understand the new security dynamic and to articulate clear foreign policy statements which adequately capture the new realities." For him, "Chinese influence operations in Canada and like-minded countries

[69] Thompson, "Hybrid," 67.
[70] Thompson, "Hybrid," 68.
[71] Thompson, "Hybrid," 68.
[72] Thompson, "Hybrid," 68.
[73] Thompson, "Hybrid," 68.
[74] Thompson, "Hybrid," 68.
[75] Boutilier, James. 'Canada Is a Nation Adrift in the Indo-Pacific, and That Needs to Change: James Boutilier for Inside Policy'. *MacDonald-Laurier Institute*, 30 June 2022.

like Australia and New Zealand have served as a wake-up call."[76] He concludes, "China isn't necessarily keen to start a war, but it will achieve its objectives by other means."

CONCLUSION

This research paper set about the challenge of answering the question: what is the Canadian national security apparatus doing to counter and combat Chinese gray zone activities? In order to address this question, it examined 1) Chinese activity in 'cyberspace'; 2) Chinese gray zone activity in the physical realm (primarily focusing on activity in the South and East China Seas); and 3) Chinese activity in the information environment. Subsequently, this paper endeavoured to situate the Canadian response to growing Chinese gray zone activities (or lack thereof) and the challenges associated with delegating responsibility for Canadian responses to gray zone warfare entirely to the Canadian Armed Forces. Furthermore, it offered that the British national security apparatus could provide a useful model for Canada given the relative similarities in governance structures.

The ultimate conclusion to be drawn from this paper is that the Canadian national security apparatus is currently not appropriately configured to counter, compete or combat Chinese gray zone operations that aim to challenge the Rules-Based International Order (RBIO) which Canada seeks to uphold and defend. In order to remain an active, responsible and relevant actor in the global community (commensurate with its status as a G7 country), Canada and the Canadian national security community must learn to follow through on their enduring international commitments and *actually* implement the policies and strategies that its governments announce and release. Canada has long been a beneficiary of the RBIO and has largely had the luxury of isolation from attack from beyond its borders. Through Chinese gray zone activities, these luxuries are no longer necessarily the case and the sooner the Canadian national security community gets serious about countering Chinese gray zone activities; the better.

[76] Witthoeft, Brett. 'Interview with Dr. James Boutilier'. *Canadian Naval Review* 15, no. 3 (3 November 2020): 35–39.

BIBLIOGRAPHY

Arquilla, John, and David Ronfeldt. *Cyberwar Is Coming!* Web Only: RAND Corporation, 1993.

Azad, T.M., M.W. Haider, and Sadiq, M. 'Understanding Gray Zone Warfare From Multiple Perspectives'. *World Affairs* 186, no. 1 (2023): 81–104. https://doi.org/10.1177/00438200221141101.

Bachmann, Sascha-Dominik Dov, Doowan Lee, and Andrew Dowse. 'COVID Information Warfare and the Future of Great Power Competition'. *The Fletcher Forum of World Affairs* 44, no. 2 (Summer 2020): 11–18. https://www.proquest.com/openview/f57132f70fe702f26446e052a6fa6211/1.

Boutilier, James. 'Canada Is a Nation Adrift in the Indo-Pacific, and That Needs to Change: James Boutilier for Inside Policy'. *MacDonald-Laurier Institute*, 30 June 2022. https://macdonaldlaurier.ca/canada-is-a-nation-adrift-in-the-indo-pacific-and-that-needs-to-change-james-boutilier-for-inside-policy/.

Brands, Hal. "Paradoxes of the Gray Zone." *Foreign Policy Research Institute* (5 February 2016). https://www.fpri.org/article/2016/02/paradoxes-gray-zone/

Col. Qiao Liang and Col. Wang Xiangsui (People's Liberation Army). *Unrestricted Warfare China's Plan to Destroy America.* Panama City, Panama: Pan American Publishing Company, 2002.

Government of Canada. "Canada's Indo-Pacific Strategy." Last modified, 30 November, 2022. https://www.international.gc.ca/transparency-transparence/indo-pacific-indo-pacifique/index.aspx?lang=eng

Government of Canada. "Canadian Forces Joint Publication 01: Canadian Military Doctrine." Issued April 2009.

Government of Canada. "Pan-Domain Force Employment Concept: Prevailing in a Dangerous World." Current Approval AY 22/23.

Government of Canada. "Strong, Secure, Engaged: Canada's Defence Policy." Last modified, 31 May, 2019. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html

Harknett, Richard J., and Max Smeets. 'Cyber Campaigns and Strategic Outcomes'. *Journal of Strategic Studies* 45, no. 4 (2022): 534–67. https://doi.org/10.1080/01402390.2020.1732354.

Huang, Alexander, *The PLA Navy at War: 1949–1999*, *in* Mark A. Ryan, David Michael Finkelstein & Michael A. McDevitt, *Chinese Warfighting: the PLA Experience Since* 1949, (2003): 266.

Kraska, James, and Michael Monti. "The Law of Naval Warfare and China's Maritime Militia." *International Law Studies U.S. Naval War College* 91 (2015): 450-467. https://digital-commons.usnwc.edu/ils/vol91/iss1/13/

Luo, Shuxian, and Jonathan G. Panter. "China's Maritime Militia and Fishing Fleets A Primer for Operational Staffs and Tactical Leaders." *Military Review China Reader Special Edition*, September 2021. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/China-Reader-Special-Edition-September-2021/Luo-Panter-Maritime-Militia/

Martin, Garrett. 'China's Strategic Devaluing of American Social Capital'. *Journal of Strategic Security* 16, no. 1 (2023): 1–18. https://digitalcommons.usf.edu/jss/vol16/iss1/1.

Mazarr, Michael. *Mastering the Gray Zone: Understanding a Changing Era of Conflict.* U.S. Army War College Press, 2015. https://press.armywarcollege.edu/monographs/428.

Morris, Lyle J., Michael J. Mazarr, and Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe. *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War.* Santa Monica, California: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR2942.html

Nye, Joseph. "How not to deal with a rising China: a US perspective." *International Affairs* 98, no. 5 (September 2022): 1635-1651. https://doi.org/10.1093/ia/iiac117

Patalano, Alessio. "When strategy is 'hybrid' and not 'grey': reviewing Chinese military and constabulary coercion at sea." *The Pacific Review* 31, no. 6 (2018): 811-839. https://doi.org/10.1080/09512748.2018.1513546

Peterson, Matt. "Competition and Decision in the Gray Zone: A New National Security Strategy." *The Strategy Bridge*, 20 April 2021. https://thestrategybridge.org/the-bridge/2021/4/20/competition-and-decision-in-the-gray-zone-a-new-national-security-strategy.

Ronfeldt, David, and John Arquilla. *Whose Story Wins: Rise of the Noosphere, Noopolitik, and Information-Age Statecraft*. Santa Monica, Calif.: RAND Corporation, 2020. https://www.rand.org/pubs/perspectives/PEA237-1.html.

Sun Tzu. *The Art of War* in *The Seven Military Classics of Ancient China.* Translated by Ralph Sawyer. Boulder, CO: Westview Press, 1993.

Thompson, Jason. 'Hybrid Warfare: Redefining and Responding to Hostile Intent'. *Canadian Military Journal* 22, no. 3 (Summer 2022): 62–70.

Tiezzi, Shannon. 'John Arquilla on the New Challenge of Cyberwarfare'. *The Diplomat*, 14 September 2021. https://journals.sagepub.com/doi/abs/10.1177/00208817221117700.

United Nations Convention on the Law of the Sea. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

Witthoeft, Brett. 'Interview with Dr. James Boutilier'. *Canadian Naval Review* 15, no. 3 (3 November 2020): 35–39.

中华人民共和国民兵工作条例 [Decree of the PRC on militia work], Central Military Commission of the People's Republic of China, December 1990, accessed 20 November 2020. [URL]