



**CANADIAN GLOBAL AFFAIRS INSTITUTE**  
**INSTITUT CANADIEN DES AFFAIRES MONDIALES**

# **War's Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare**

by David Carment and Dani Belo  
October 2018

# POLICY PAPER

---

## **WAR'S FUTURE: THE RISKS AND REWARDS OF GREY-ZONE CONFLICT AND HYBRID WARFARE**

by David Carment, CGAI Fellow and Dani Belo

October 2018



CANADIAN GLOBAL AFFAIRS INSTITUTE  
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute  
1800, 421 – 7th Avenue S.W., Calgary, AB T2P 4K9  
[www.cgai.ca](http://www.cgai.ca)

©2018 Canadian Global Affairs Institute  
ISBN: 978-1-77397-043-1

This paper underwent a double-blind peer review.



## ► **Executive Summary**

---

Today's geopolitical conflicts, especially among great powers, involve a desire to fundamentally revise the order of alliances as well as solidify new norms of conduct. The purpose of our paper is to delineate two distinct phenomena in international affairs – hybrid warfare, which emphasizes the tactical level and grey-zone conflicts, which incorporates a long-term strategic dimension into international disputes. We argue that hybrid warfare can be a tactical subset of grey-zone conflict deployed under certain conditions and in varying degrees. We examine four case studies: China's application of 'unrestricted warfare', Russia's strategy of 'hybrid balancing', 'regional hybridism' practiced by Israel and 'restricted hybridism' applied by Canada/NATO globally. We conclude that the solution to challenges from Russia and China is not a military one but a political and collective one based on baseline requirements for building resilience. Israel, on the other hand, is largely uninterested in the revision of order of alliances and will continue to utilize its tactical advantage vis-à-vis regional neighbors to achieve victories in short conflicts. We conclude that NATO (and Canada) should work more closely with the Organization for Security and Co-operation in Europe and the European Union to effectively extend security guarantees to its members. In doing so Canada and likeminded countries will involve the costs of engaging in hybrid warfare and the subsequent erosion of democratic accountability.



**T**oday's geopolitical conflicts reflect a desire by some states to gradually, but fundamentally, revise the regional or global system of alliances and international norms to a degree not even seen during the Cold War. This process of conflict-induced change is known as grey-zone conflict, in which states conduct operations that only occasionally pass the threshold of war. Grey-zone conflict refers to those post-Cold War conflicts – not always violent – which are prolonged and frequently characterized by an ambiguous point of victory (Carment, Nikolko and Belo, 2018).

In this brief, we distinguish between the strategic goals of grey-zone conflict and the tactical operations of hybrid warfare. The two are not synonymous. Unlike hybrid warfare, grey-zone conflict participants rely on unconventional tactics that do not cross the threshold of formalized state-level aggression. Put another way, hybrid warfare can be a tactical subset of grey-zone conflict deployed under certain conditions and in varying degrees. In making this distinction we are better positioned to understand the spectrum of states that are engaged in grey-zone conflict while drawing on different kinds of hybrid tactics.

At one end of the spectrum consider China's concept of "unrestricted warfare" which closely approximates grey-zone strategic, revisionist thinking without hybrid warfare. Then there is Russia's involvement in the Baltics and Eastern Ukraine where we see mixed elements of grey-zone conflict and hybrid warfare or what we call "hybrid balancing". Israeli application of "regional hybridism", emphasizing tactical operations, is our third example. Finally, at the other end of the spectrum there is Canada/NATO's hybrid warfare in weak and fragile states and its use of "restricted hybridism" largely absent of an offensive strategic calculus embedded in grey-zone conflict.

## **Hybrid Warfare and Grey-Zone Conflict**

Hybrid warfare is most often understood in the context of antagonistic behaviour between Russia and the United States. In viewing, for example, the hot wars between these two states' proxies, it is assumed that hybrid warfare involves explicitly offensive and state-sanctioned violent tactics against "hybrid threats" as is the case in Ukraine and Syria (Hoffman, 2015, 25-36).

Drawing on NATO sources, Boucher (2017) argues hybrid warfare is broadly characterized by a wide range of overt and covert military, paramilitary and civilian measures employed in a highly integrated design. According to Boucher, it is the civilian element that distinguishes hybrid from regular warfare to the extent that non-military actors and stakeholders are explicitly involved in the political, informational and economic components of war. The degree of reliance on civilians and non-state actors makes hybrid warfare distinctly modern. Hybrid warfare is no longer just about partisans such as the French resistance or Soviet civil brigades in Karelia during the Second World War. Hybrid warfare is now societal in scope in terms of intended targets and those states that engage in it.



The modern idea of hybrid warfare originated partly from American war studies influenced by the realization that since 9/11, international conflict has become increasingly complex with regard to the number and kind of belligerents and the tools available to them. Furthermore, hybrid warfare has meaning for those states and alliances engaged with weaker yet more tactically flexible sub-state actors – principally threat-based and focused on the idea of irregular warfare to counter those threats (Carment, Nikolko and Belo 2018a, 2018b). The lethality of this threat-based approach to hybrid warfare emanates from the combination of high-tech capabilities and the pursuit of unconventional (and often unrestricted) tactics.

One reason for this dual approach is the circumvention of, and asymmetric adherence to, international law. Simply put, international legal structures act as restraints on what democratic states can do in the international arena. Hybridism offers a way out to avoid exploitation by states that do not uphold such laws.

Permissive and advantageous conditions are created for non-democratic states to conduct operations against their democratic adversaries. Highly centralized, and thus procedurally flexible, states such as Russia and China can use propaganda, domestic legal structures, economic pressure and support for non-state proxies more readily, compared to democracies. This relatively unregulated environment enables authoritarian states to normalize and internalize new practices for engagement against opponents. In contrast, there are clear limits to what democratic states can do with hybrid warfare.

This is because states such as Canada and the U.S are constrained by their decentralized decision-making, domestic laws and complex bureaucracies. All this renders democracies sensitive to the principal-agent problem in which lack of oversight may generate unintended and potentially undesirable outcomes. As Boucher (2017) points out, hybrid warfare by democratic states is a double-edged sword: without proper oversight, democracies risk unrestrained actions by their militaries. There is thus a fundamental problem of information asymmetries creating moral hazard. Moral hazard occurs under a type of information asymmetry where the risk-taking party to a transaction knows more about its intentions than the party paying the consequences of the risk (Rowlands and Carment, 1998).

The problem of moral hazard became readily apparent in Afghanistan in two glaring instances. The first involved Pakistan's support for the Taliban and the Canadian government's failure both to acknowledge its negative impact on the Canadian mission and to derive an effective solution to cross-border incursions and safe havens. In fact, the so-called 2008 Manley Report, which essentially green-lighted Canada's ongoing war in Afghanistan, mentioned the border problem just briefly. This leads to the conclusion that parliamentarians and bureaucrats in Ottawa were not properly informed of the situation despite significant Canadian presence and representation in Kandahar and Kabul. The report recommended among other things more frequent communications to Canadians regarding Canada's engagement in Afghanistan and integrated planning, though it provided no meaningful solution to the Pakistan problem. Another example of moral hazard occurred in relation to the so-called Afghan detainee scandal which only came to



light after FSO Richard Colvin revealed human rights abuses despite the Conservative government's continued denial.

The difficulty in acquiring information about a military's motives, tactics and capabilities is the common factor in that a democracy may be unwilling (for political reasons) or incapable (for institutional reasons) of holding its military accountable as a whole. Therefore, it has to function with incomplete information or become reliant on defence staff who may reveal only partial or false information. The unwillingness of defence staff to share information is partly motivated by a desire to disguise their true goals in order to avoid the label of an enabler to conflict or to ensure that opponents are not given that information.

We are not suggesting that by itself hybrid warfare necessarily makes states less democratic, but there is the potential for civilian oversight to be compromised, leading to an erosion of democratic structures and norms. For example, a democratic state may be unable, for reasons related to capacity, politics or influence, to prevent military actions because it cannot discriminate between enablers and the more disengaged.

In our view, preferences for using hybrid warfare emerge when military decision-makers are able to largely circumvent the weak international legal regimes governing unconventional warfare tactics.<sup>1</sup> Cyber-warfare, for example, which both democratic and authoritarian states use, has been a grey area for international law. Cyber-operations can seldom be considered an armed attack that warrants an immediate military response by the target as deaths and infrastructure destruction are rarely immediate, reliably measurable or directly attributable to state actors (Roberts, 2014).

How does hybrid warfare relate to grey-zone conflict? Grey-zone conflict may incorporate conventional and non-conventional techniques or rely entirely on non-conventional tactics. Complete reliance on unconventional tools is likely to be less effective at fully and rapidly compelling relatively strong opponent(s) into specific avenues of desired action. Thus states engaged in grey-zone conflicts are likely to use hybrid techniques, and more of their conventional resources, when there is a perception that the use of unconventional techniques will not fully achieve a desired outcome. The incorporation of conventional force against an opponent would be more likely in cases of asymmetric conflict in which the cost of applying conventional techniques against a weaker opponent is much lower. However, in cases where opponents are in a symmetric conflict, states are likely to rely heavily on unconventional tools and covert operations.

The table below provides a comparison of grey-zone and hybrid warfare characteristics. Our cases relate to situations where asymmetry predominates.

---

<sup>1</sup> Hybrid warfare may use elements from four methods and categories of warfare; namely, irregular warfare (such as terrorism and counter-insurgency), asymmetric warfare (unconventional warfare such as partisan warfare), and compound warfare (where irregular forces are used simultaneously against an opponent). State actors can use hybrid warfare to augment their otherwise conventional warfare approach and non-state actors can use it to gain an advantage over a conventional warfare opponent.



Table 1. Comparison between Grey-Zone and Hybrid Warfare Characteristics

Characteristic	Grey-Zone Conflict	Hybrid Warfare
Level	Tactical, operational, strategic	Tactical and operational
Use of conventional military operations	Used alongside non-conventional operations.	Used alongside non-conventional operations. Usually the dominant element.
Use of non-conventional military operations	May be used standalone or alongside conventional operations.	Used alongside conventional operations as auxiliary tactics.
Protracted engagement	One of the dominant characteristics.	May be protracted or short.
Global and/or regional revisionist ambitions	One of the dominant characteristics.	Out of scope as the concept pertains to operational and tactical levels.
Symmetry between opponents	Used under both symmetric and asymmetric conditions.	Largely used under asymmetric conditions.

### China's Engagement in Grey-Zone Conflict

Turning to our first case, we see that China's growing global influence has become a considerable concern in the West because the country has been increasingly engaged in unconventional operations to dilute American hegemony. We argue for the label of "unrestricted" to characterize China's actions, as the unconventional strategies employed fall mostly outside the purview of treaties, international laws and norms, thus placing few restrictions on their use. We argue that China's actions fall short of engagement in hybrid conflict, while meeting the criteria of grey-zone conflict.

In the late 1990s, China's political, economic and military tacticians understood that to successfully promote the country's interests globally, direct military engagement vis-à-vis the U.S and its allies would not be an option. Moreover, any direct confrontation may trigger a nuclear response, which would yield no positive outcomes for any of the parties. In reviewing the PLA's *Unrestricted Warfare* publication, we note that China's strategic interests are other great powers. Activities targeting weaker opponents are largely meant to undermine the strength and unity of alliance structures surrounding other powerful states. Thus, even though the development of a conventional force remains a priority for China, the country would largely forgo its use in favour of unconventional tactics that would remain between the thresholds of open war and peace. In 1999, two Chinese military (PLA) officers reflected on this in *Unrestricted Warfare*, in which they



advance the concept of combining unconventional and covert tactics against the U.S. (Liang and Wang, 1999).

They generally identify four alternatives to traditional military engagement: 1) Political action to promote favourable global change in policy and international norms; 2) Increasing economic pressure on allies and opponents. China's ability to promote its interests on a global scale, and even change partnership priorities of individual countries, would stem from its considerable influence in the world economy; 3) Engagement in cyber and network warfare; and 4) Incorporation of non-state actors into conflicts. Over the past decade, China's actions largely adhered to these principles.

As we highlighted earlier, cyber-space remains mostly ungoverned by international laws and treaties, leaving significant flexibility for China to exploit as a platform of warfare. In January 2010, China launched cyber-attacks against 34 U.S. companies, including military contractors.<sup>2</sup> Another instance was the breach of Australia's Security Intelligence Organisation in 2013.<sup>3</sup> Even though both the U.S. and Australia attributed the attacks to the Chinese state, no sanctions were applied against the country. Although cyber-space has been an important domain for China, the country's targeted economic investment has been a central strategy to revise orders of alliances.

China's exponentially increasing investment in developing African states over the past decade has significantly challenged U.S. hegemony. For example, a historic meeting between Chinese leaders and representatives of 48 governments in Africa took place in the Chinese capital in November 2006 while the U.S. was preoccupied with the war in Iraq. This meeting paved the way for future investment in traditional U.S. allied states such as Angola and Nigeria, where China initiated long-term infrastructure and communications projects (Campbell, 2008). This trend has created economies entirely dependent on Chinese investment. Regardless of these countries' ambivalence to such investments, they are a de facto challenge to U.S. hegemony and will continue to grow with time.

## **Russia and Hybrid Balancing**

In 2007, at the Munich Security Conference, Vladimir Putin presented a number of principles that not only highlighted Russia's rejection of U.S. global hegemony, he instilled doubt that international law is a reliable framework for inter-state conduct and defending Russia. This position, which some analysts incorrectly diagnosed as revisionist, was adopted following the NATO alliance's eastward expansion into Russia's self-declared spheres of influence (Carment and Belo, 2017). The tactical, operational and strategic dimensions of Russia's "hybrid balancing" are encapsulated in what is commonly labelled the Gerasimov Doctrine. Akin to the American framework on the Adaptive Approach for the Use of Military Force (AAUMF), the doctrine

---

<sup>2</sup> "Google China Cyberattack Part of Vast Espionage Campaign, Experts Say." <http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html?noredirect=on>

<sup>3</sup> "Australian Spy HQ Plans Stolen by Chinese Hackers." <https://www.reuters.com/article/us-australia-hacking/australian-spy-hq-plans-stolen-by-chinese-hackers-report-idUSBRE94R02A20130528>



emphasizes the necessity of using military and non-military means against opponents (Bartles, 2016).

More concretely, we see Russia's involvement in the Baltics, Crimea and Eastern Ukraine as a mix of grey-zone and hybrid warfare. Against NATO states directly, Russia has relied entirely on unconventional tools such as economic pressure, propaganda, formation of special bilateral relations with EU members and the use of cyber-warfare to challenge the military alliance in places such as the Baltic states. These are characteristic of grey-zone conflicts. In Eastern Ukraine and Crimea, Russia has engaged in hybrid warfare using non-state proxies to supplement a deficit in trained soldiers and war material (Carment, Nikolko and Belo, 2018a, 2018b).

Contrary to the view of many Western academics and journalists, Gerasimov (2016) emphasizes that there is no model or formula for warfare, but rather each scenario is markedly unique and requires a tailored approach. In his view, however, war in the 21st century is conducted at a roughly four-to-one ratio of non-military and traditional military tools and tactics (Bartles, 2016, 20). This emphasis on covert operations and non-military tactics is evident in Russia's actions in the Baltics, better characterized as engagement in grey-zone conflict, and in Eastern Ukraine and Crimea, where the operational and tactical environment resembles hybrid warfare.

In Eastern Ukraine, Russia draws on economic tools and cyber-space to harm its adversary's energy sector and infrastructure as well as non-state actors to fight against Ukraine's conventional forces. In 2014, during the unrest in Eastern Ukraine and the Maidan, the Russian government-operated Gazprom annulled the gas discount agreement the Yanukovych administration had signed. Furthermore, in December 2015, Russia was accused of attacking Ukraine's power grid through cyber-space, thereby disabling a large portion of the country's infrastructure.<sup>4</sup>

Even though non-military tactics play a significant role in Russia's arsenal against Ukraine, conventional forces have been critical in a number of operations such as in Crimea. Working with the 16,000 uniformed forces already stationed in Crimea (under a basing agreement with Kiev which permitted up to 25,000 soldiers to be stationed there), Russia deployed a covert military operation, using special unmarked military units to capture Ukrainian soldiers located at strategic government and military sites on the peninsula. Furthermore, in Eastern Ukraine, Russia aided the rebel forces of the LNR and DNR fighting against the Ukrainian army. However, relative to its actions in Ukraine, Russia's engagement in the Baltics is more closely associated with grey-zone conflict.

Since the Baltic states are members of the EU and NATO, Russia uses unconventional tools to disrupt communications infrastructures as well as to provoke political unrest through appeal to the Russian diaspora (Nicolko and Carment, 2017). First, in October 2017, Russia conducted a cyber-attack on Latvia, resulting in an interruption in the country's emergency response telecommunications network.<sup>5</sup> Second, considering that Russian speakers make up nearly 30 per

---

<sup>4</sup> Ministry of Energy and Coal Industry of Ukraine. [http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art\\_id=245086886&cat\\_id=35109](http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat_id=35109)

<sup>5</sup> "Russia May Have Tested Cyber Warfare on Latvia." <https://www.reuters.com/article/us-russia-nato/russia-may-have-tested-cyber-warfare-on-latvia-western-officials-say-idUSKBN1CA142>



cent of the population of Latvia and Estonia, Russia has been able to effectively use various information tools to promote disquiet among the diaspora – highlighting the repressive and fragmented nature of minority rights in these countries. In 2005, a television platform called the Baltic Media Alliance (BMA) began broadcasting to the entire region. This entity serves as a platform to transmit programs from state-run channels in Russia to the Baltic's Russian-speaking population (Król, 2017).

### **Israel and Regional Hybridism**

Israel represents a rare case of engagement in hybrid warfare as the country experienced a considerable shift in its priorities toward conventional forces – a phenomenon counter to the other cases we discussed previously. Even though the country has been increasingly engaging in covert operations alongside regional neighbours such as Saudi Arabia, Israel's hybrid warfare tactics largely target other Arab states such as Syria, Lebanon and Iran, as well as non-state actors such as Hamas and Hezbollah. This regional application of hybrid warfare is the result of an antagonistic relationship with its neighbours, many of whom do not recognize Israeli statehood. However, Israel does not place great strategic emphasis on changing the pre-existing, and highly rigid, regional order of alliances or influencing the political process of its neighbouring states. We characterize Israel's emphasis on the tactical and operational levels, confined to a limited geographic area, as "regional hybridism." We find that the 2006 Israel-Hezbollah war was pivotal in explaining how (and why) Israel engages in hybrid warfare. Prior to 2006, Israel was defunding its conventional ground armed forces while increasing capabilities for low-intensity conflicts using sophisticated covert operations.

The shift away from conventional forces stems from an increased comfort and complacency with existing deterrence tools and tactics against surrounding Arab states. Israel fought several successful high-intensity conventional wars against a coalition of neighbouring Arab states such as the 1948 Arab-Israeli War, the Six-Day War in June 1967 and the Yom Kippur War in October 1973. In all three cases, the country's survival was the main consideration. The primary tools of defence and deterrence were Israel's conventional forces. However, this preoccupation with state survival began to wane in the 1970s – around the time it is believed the country produced its first nuclear weapon (Special National Intelligence Estimate 1974, 20). This period also corresponds with an overall improvement in Israel's relationship with its neighbours, Egypt and Jordan. In fact, the 1973 war against its neighbours was the last high-intensity conflict in which Israel directly engaged neighbouring states. The decreasing prevalence of the conventional wars, however, did not mean a decrease in hostilities. Rather, conflict transformed into a fight against asymmetric, often state-backed, entities such as in the First and Second Intifadas as well as the war against Hezbollah in 2006. This asymmetry necessitated a considerable reorientation of Israel's resources away from conventional forces toward low-intensity covert operations (Ben Yehuda and Sandler, 2002).



This change in the operational environment demanded an increased investment in counterterrorism-related tools and techniques – largely used in Gaza. In the 1990s and early 2000s, Israel invested heavily in targeted assassinations and other covert intelligence capabilities.<sup>6</sup> A number of prominent examples demonstrate Israel's increased capability to conduct covert operations outside its borders. First, there was the assassination of Fathi Shaqaqi, a leader in the Palestinian Islamic Jihad, who was killed by a group of Mossad agents in Malta in October 1995.<sup>7</sup> Another example is the assassination of Yahya Ayyash, killed by a cellphone bomb in Beit Lahya, Ayyash, Gaza in 1996.<sup>8</sup> Even though such targeted assassinations constituted an important part of Israeli operations, conventional forces were used to a limited extent as support in cases such as the Second Intifada. In November 2000, Israeli troops were deployed into Gaza to restore order.

Over the course of that November and December, Israel Defence Forces (IDF) soldiers engaged directly with Hamas militants in ground operations (Eiland, 2010). Furthermore, IDF soldiers were deployed regularly throughout the Second Intifada as a response to frequently violent demonstrations along the Israel-Palestinian border. The Second Intifada created a perception among Israeli military strategists and policy-makers that the country's increasing proficiency in the conduct of covert operations and seemingly sufficient, yet declining, conventional capabilities would suffice to respond to future threats. This proved to be a miscalculation.

For example, the 2006 Israel-Hezbollah war facilitated a major shift in Israel's hybrid balancing. The Winograd Commission, appointed by the Israeli government, concluded in its 2008 final report that Israel's failure to deter and defeat Hezbollah in south Lebanon was the result of the IDF's decreased conventional tactical and operational capabilities as well as mismanagement by political and military leadership. Targeted strikes were not sufficient to defeat Hezbollah fighters who relied heavily on conventional tactics. Such operations by Hezbollah required a rapid and effective conventional ground response, which Israel undertook in the latter stage of the conflict, but in a tactically ineffective manner. The events of the 2006 war and the findings from the Winograd Report instilled doubt in Israel's conventional capabilities, sparking a re-evaluation of Israel's hybrid balancing between conventional and unconventional capabilities, a subsequent air force and ground force modernization plan and updating of conventional tactical training.<sup>9</sup> Several generals resigned or were fired, such as chief of staff Lt.-Gen. Dan Halutz. The IDF also rethought the role of heavy forces and resumed mass production of the Merkava IV tank, concluding that heavy armour is indispensable for the successful execution of tactical objectives (Johnson, 2010).

---

<sup>6</sup> "How Israel's Secret Service Has Become the World Leader in Assassins." <http://www.dailymail.co.uk/news/article-6001335/How-Israelis-secret-service-world-leader-assassins.html>

<sup>7</sup> "Islamic Group Vows Revenge For Slaying Of Its Leader." <https://www.nytimes.com/1995/10/30/world/islamic-group-vows-revenge-for-slaying-of-its-leader.html>

<sup>8</sup> "How the Phone Bomb Was Set Up." <https://www.independent.co.uk/news/world/how-the-phone-bomb-was-set-up-1323096.html>

<sup>9</sup> "Gov't Officially Approves Deal To Buy F-35 Fighter Jets." <https://www.jpost.com/Israel/Govt-officially-approves-deal-to-buy-F-35-fighter-jets>



## **Canada, NATO and Restricted Hybridism**

There are several different perspectives one could take on Canada's (and by extension NATO's) approach to hybrid warfare, most of which are covered in greater detail elsewhere (Hoffman, 2007; Hartmann, 2017). But for our purposes we want to focus on the idea of hybrid warfare not just as something that is conducted by other states and to be defended against, but as a form of war combined with a heavy civilian and preventive component, nested within a broader security architecture and which Canada and its allies conduct on a restricted but regular basis.

For example, Canada's intervention in failed and fragile states is a form of hybrid warfare even if it has never been described that way. That is because such interventions combine all elements of civilian and military co-operation, and informational, economic and political assets seeking to simultaneously eliminate known enemies such as terrorist organizations while working to strengthen governance and development. Current Canadian missions in Iraq and Mali involving a training and peacekeeping component, on the one hand, and JTF2 search-and-destroy components, on the other, are pertinent examples.

This idea challenges the more conventional perspective, that only Russia uses hybrid warfare techniques often identified with subversion, propaganda and cyber-warfare to undermine the Western alliance without triggering a full NATO military response (NATO Strategic Concept, 2010). They attack. We defend (in a limited way). This perceived change in the nature of warfare has generated a great deal of controversy as to whether NATO should consider hybrid threats sufficient to prompt an Article 5 response.

But such thinking is misguided for a couple of reasons. First, using hybrid tactics, NATO's opponents continue to exploit the alliance's intervention ineffectiveness and weaknesses in out-of-area operations. For example, as noted above Afghanistan demonstrated deep flaws in developing policy coherence among NATO members in non-existential conflicts.

Drawing on its assets, though not a NATO mission, the Iraq intervention led by the British and the Americans showed similar failure to properly resource the problem, think through the consequences of covert military actions and promote long-term political solutions while favouring short-term military gains. According to the Chilcot Report (2016) experts predicted the chaos following the invasion of Iraq due to the lack of contextual evidence-based analysis in both planning and post-conflict operations. The U.K., the report notes, entered Iraq without a clear understanding of the resources that would be needed to do the job properly.

Furthermore and what is crucial here, there was an inadequate analysis of the country's political, cultural and ethnic background which resulted in promoting inter-ethnic rivalries rather than preventing them. If this sounds familiar in the context of the current conflicts in Syria, Libya and Ukraine, it is because the West has participated in similar outcomes in all three cases, encouraging continued war rather than quelling it (Howard and Stark, 2017; Marantz, Sun and Soegiarto, 2017).



These flaws in the hands of an adversary like Russia (or China), are the main strengths of hybrid war. Those areas over which NATO has only a limited interest and control, such as inter-ethnic divisions, economic underdevelopment and political corruption are ripe for exploitation. Hybrid war's strength derives from its societal impact, its ability to destabilize conventional statecraft and its weakening of political resolve and economic capacity against which there is no effective military solution (Hartmann, 2017).

Among the most significant of these perceived threats are democratic backsliding and the rise of unconsolidated democracies within the alliance, and among those on the periphery of NATO influence, in which NATO has operational interests such as failed and fragile states (Calleja, Carment, Haichin and Tikuisis, 2017; Carment and Floch, 2018).

Consider the above-mentioned examples of the Baltics in which Canada and NATO members have invested heavily to establish a deterrent against a conventional forces invasion. This military contribution is modest at best given that the source of instability among these states, just as elsewhere within NATO, is generated from within (Spruds, 2001; Carment, 1995). Their weakness invites intervention, not the other way around. Consider the equally problematic case of Ukraine, a country which must in the first instance demonstrate a strong functional economy, fair and even-handed treatment of its minorities and corruption-free leadership before it can even consider finding a lasting and legitimate solution to the conflict in the Donbass or integration within the EU (or NATO). (These points are laid out in our recent CGAI policy papers and elsewhere. See Carment, Nikolko and Belo, 2018b; Foresight Ukraine, 2017).

## **Conclusion: Collective Security is the Answer**

Drawing on the cases of China, Russia, Israel and Canada, we illustrated the concepts of hybrid warfare and grey-zone conflict. We identified hybrid warfare as a subset of grey-zone conflicts, in which conventional and unconventional tools and tactics are used in tandem. The revisionist element in grey-zone conflict differentiates it from hybrid warfare. Each of the actors in our case studies identifies a distinct balance between conventional and unconventional tactics, prioritizes success in various level(s) of warfare and pursues revisionism to different extents. We find that Israel and Canada/NATO use hybrid warfare more frequently now, relying not only on covert operations and soft power, but on conventional military tools and techniques to achieve their goals. In contrast, China and Russia engage in grey-zone conflict primarily through unconventional techniques with the hope of not only achieving short-term tactical victories against the U.S and NATO, but to challenge the regional and/or global order of alliances and influence international norms of conduct. China is most definitely seeking to revise the international order, while Russia is reacting to post-Cold War changes in its security environment and what it regards as NATO encroachment.

Looking ahead, NATO's value is negligible if its foremost purpose is to combat hybrid warfare with more hybrid warfare. There are three reasons for that. First, there are problems with democratic accountability, oversight and circumvention of the law as we noted in our



introduction. Second, as we also noted above, Western-led missions have fatal flaws in terms of policy co-ordination and coherence that render them susceptible to hybrid influence. Third, democratic states cannot guarantee complete immunity from hybrid warfare without becoming the enemies of their own open societies (Hartmann, 2017). To make vulnerable states fully resistant to hybrid influence is to render them closed societies.

The solution to challenges from Russia and China is not a military one but a political and collective one based on baseline requirements for building resilience or what we call strong state capacity, authority and legitimacy (Carment and Samy, 2017). In building resilience, the main role of the military is not to challenge Russian (or Chinese) influence with hybrid tactics but to envision a wider end state in which the application of non-violent techniques such as civil-military activities, social media operations and public affairs are more effective than the direct use of force. Success in building resilience depends on the ability to forecast a desired end-state that prioritizes long-term political and economic goals. An important prerequisite is Canadian public support for these long-term commitments and a fully accountable and open military command structure. Unless the Canadian public is behind these kinds of operations and understands their purpose, politicians should not be authorizing them.

A second and related point is that NATO is but one of several important security organizations that must be involved in building such resilience. NATO works well as a deterrent against the territorial invasion of one of its members, but when it comes to extending security guarantees to minorities at risk or building democracy, for example, NATO is sluggish, outmoded and archaic.<sup>10</sup> To build resilience among those states which are weak, backsliding and have poor minority rights, NATO (and Canada) must work more closely with the Organization for Security and Co-operation in Europe (OSCE) and the European Union (EU). The latter both have capacities that NATO does not, such as maintaining a position of impartiality in mediating ethnic conflict, economic and humanitarian political resources, inclusive and consensus-based decision-making and a history of non-violent involvement in complex conflicts.

Simultaneous oversight measures mandated by the OSCE and the EU are essential to achieving a co-ordinated and inclusive response. Inclusivity means Russia's involvement and not isolation is essential to ensuring that the need to resort to hybrid warfare is reduced and eventually eliminated. If, for example, Latvia and Estonia have problems with minority rights, these should be neither ignored nor exploited but confronted and dealt with. If Hungary has a democratic deficit this makes it susceptible to outside influence, leading to increased weakening of both NATO and the EU. The answer to why Hungary and other states in CEE are turning away from liberal values does not lie with confronting Russia. If Ukraine has limited capacity to control its contested territories, then some compromise must be found which gives full recognition to

---

<sup>10</sup> There are tools available to NATO that could allow it, in partnership with key regional organizations, to monitor minority security issues and strengthen security in Eastern Ukraine quickly and effectively. A good start would be for NATO to endorse and support the enforcement of a robust minority rights policy for Ukraine that builds on existing ones, such as the European Convention on Human Rights.



minority rights and autonomy while maintaining state integrity (Carment, Nikolko and Belo, 2018; Foresight Ukraine, 2017).

In all these cases, Russia should be encouraged to participate in the development of monitoring and oversight architectures as regional confidence-building measures to achieve transparency and predictability. Regional confidence-building measures that reflect norms of international co-operation should be supported and implemented. Canada's aim, as unpalatable as it might be to the Trudeau government, must be to strengthen those regional organs of collective security in which Russia plays an important role.<sup>11</sup> Only then will the incentive for Russian interference diminish with time.

---

<sup>11</sup> The ultimate goal must be to persuade the Russian nation to play a constructive and secure role in broader European society generally, and in Ukraine's security in particular. The strategic imperative for NATO is to recognize that regional solutions are the way forward. As a regional power, Russia and its armed forces will continue to solve problems on its periphery with or without Western sanction — so a confrontational posture on NATO's part remains counterproductive.



## Works Cited

- Bartles, Charles K. 2016. "Getting Gerasimov Right," *Military Review* 96, no. 1: 30.
- Ben-Yehuda, Hemda, and Shmuel Sandler. 2002. *The Arab-Israeli Conflict Transformed: Fifty Years of Interstate and Ethnic Crises*. New York: State University of New York Press.
- Boucher, Jean-Christophe. 2017. "Hybrid Warfare and Civil-Military Relations." Canadian Global Affairs Institute (CGAI). Policy Update. December.  
<https://www.cgai.ca/hybrid-warfare-and-civil-military-relations>
- Calleja, Rachael, David Carment, Mark Haichin, and Peter Tikuisis. 2017. "Backsliding and Reversal: The J-Curve Revisited," WIDER Working Paper 2017/170 Helsinki: UNU-WIDER. <https://www.wider.unu.edu/publication/backsliding-and-reversal>
- Campbell, Horace. 2008. "China in Africa: Challenging US Global Hegemony," *Third World Quarterly* 29, no. 1, 89-105.
- Carment, David. 1995. "NATO and the International Politics of Ethnic Conflict: Perspectives on Theory and Policy," *Contemporary Security Policy* 16, no. 3: 347-79.
- Carment, David, and James Floch. 2018. "Violence on the Horizon: Elections and Conflict 2018-2019," Canadian Global Affairs Institute. April. <https://www.cgai.ca/violence-on-the-horizon-elections-and-conflict-2018-2019>.
- Carment, David, Milana Nikolko, and Dani Belo. 2018. "Mediating an Impasse: The Way Forward in Ukraine." Canadian Global Affairs Institute (CGAI). Policy Update. February. <http://www.cgai.ca/mediating-an-impasse-the-way-forward-in-ukraine>
- Carment, David, Milana Nikolko, and Dani Belo. 2018. "Ukraine's Grey-Zone Conflict: What Lies Ahead?" Canadian Global Affairs Institute (CGAI). Policy Update. February. [http://www.cgai.ca/ukraine-s-grey-zone-conflict-what-lies-ahead?utm\\_campaign=carment-ukraine&utm\\_medium=email&utm\\_source=cdfai](http://www.cgai.ca/ukraine-s-grey-zone-conflict-what-lies-ahead?utm_campaign=carment-ukraine&utm_medium=email&utm_source=cdfai)
- Carment, David, and Yiagadeesen, Samy. 2017. "Exiting the Fragility Trap: Rethinking Our Approach to the World's Most Fragile States." WIDER Working Paper 2017/181. Helsinki: UNU-WIDER.
- Central Intelligence Agency. 1974. Special National Intelligence Estimate. <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB240/snie.pdf>
- Eiland, Giora. 2010. "The IDF in the Second Intifada," *Strategic Assessment* 13, no. 3. October.
- Friedrich-Ebert-Stiftung. 2017. "Scenario Group Ukraine 2027: Foresight Ukraine Four Scenarios for the Development of Ukraine." Vienna.



- Gerasimov, Valery. 2016. "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations," *Military Review* 96, no. 1: 23.
- Gutmann, Ethan. 2010. "Hacker Non: China's Cyber Assault," *World Affairs*, vol. 173, no. 1.
- Hartmann, Uwe. 2017. "The Evolution of the Hybrid Threat, and Resilience as a Countermeasure." NATO Defense College. Sept. 6.  
<http://www.ndc.nato.int/news/news.php?icode=1083>.
- Hoffman, Frank G. 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies.
- Johnson, David E. 2010. "Military Capabilities for Hybrid War: Insights from the Israel Defense Forces in Lebanon and Gaza." Santa Monica, CA: RAND Corporation.  
[https://www.rand.org/pubs/occasional\\_papers/OP285.html](https://www.rand.org/pubs/occasional_papers/OP285.html).
- Król, Aleksander. 2017. "Russian Information Warfare in the Baltic States – Resources and Aims." Warsaw Institute. July. <https://warsawinstitute.org/russian-information-warfare-baltic-states-resources-aims/>
- Liang, Qiao, and Wang Xiangsui. 1999. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House Arts.
- Marantz, Uriel, Sharon Sun, and Fanny Siau-Soegiarto. 2017. "The Intervention Trap in a Time of Tumult," *Canadian Foreign Policy Journal* 23, no. 3: 197-204. Sept. 19.  
<https://www.tandfonline.com/doi/full/10.1080/11926422.2017.1359196>.
- Nikolko, Milana, and David Carment. 2017. *Post-Soviet Migration and Diasporas: From Global Perspectives to Everyday Practices*. Palgrave Macmillan.
- Roberts, Shaun. 2014. "Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors," *Northern Kentucky Law Review*, vol. 41, no. 3: 535-572.
- Rowlands D., and D. Carment. 1998. "Moral Hazard and Conflict Intervention," in M. Wolfson (ed.) *The Political Economy of War and Peace*. Recent Economic Thought Series, vol. 64. Springer, Boston, MA.
- Spruds, Andris. 2001. "Minority Issues in the Baltic States in the Context of NATO Enlargement." NATO Research Fellowship's End Product. July.  
[www.nato.int/acad/fellow/99-01/spruds.pdf](http://www.nato.int/acad/fellow/99-01/spruds.pdf)

## ► About the Author

---

**David Carment** is a full Professor of International Affairs at the Norman Paterson School of International Affairs, Carleton University and Fellow of the Canadian Global Affairs Institute (CGAI). He is also a NATO Fellow and listed in Who's Who in International Affairs. In addition Professor Carment serves as the principal investigator for the Country Indicators for Foreign Policy project (CIFP).

Professor Carment has served as Director of the Centre for Security and Defence Studies at Carleton University and is the recipient of a Carleton Graduate Student's teaching excellence award, SSHRC fellowships and research awards, Carleton University's research achievement award, and a Petro-Canada Young Innovator Award. Professor Carment has held fellowships at the Kennedy School, Harvard and the Hoover Institution, Stanford, and currently heads a team of researchers that evaluates policy effectiveness in failed and fragile states (see Country Indicators for Foreign Policy). Recent publications on these topics appear in the Harvard International Review and the Journal of Conflict Management and Peace Science.

**Dani Belo** is a doctoral student at Carleton University's Norman Paterson School of International Affairs. He specializes in conflict analysis, defence and security studies and Russian foreign policy.

## ► **Canadian Global Affairs Institute**

---

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.