Journal of
Military and
Strategic
Studies

VOLUME 19, ISSUE 4

Deterrence, Resilience and Hybrid Wars: The Case of Canada and NATO

Nicole J. Jackson

Modern deterrence strategies are complicated by the need to consider whether and how to respond to a whole host of aggressions that fall short of conventional war. These now come from a range of (state and non-state) actors and are directed towards a wide range of targets (states, businesses, societies, and increasingly individuals). Challenges weave through different domains from the global and national to regional and local and have implications at domestic and international levels. In Canada, what once were federal security issues (involving public safety, CSIS, defence, foreign affairs) increasingly impact on provincial and local levels in areas such as education, law, and infrastructure as well as on our alliances such as NATO and our relationships with multilateral groups such as the G7 and the EU.

Traditional deterrence was set up for past conventional wars, which are no longer the norm. Today, in response to hybrid warfare, non-military tools, tailored to fit particular contexts, are increasingly being used to detect, prevent or pre-empt crises, and are filling in the gaps from traditional structures of deterrence (nuclear weapons and conventional forces). In other words, non-military tools are being used, often simultaneously, in areas that are not clearly war (military) or peace (political). In

ISSN : 1488-559X

reviewing these developments, this paper suggest that it is important to think through the implications of this current transformation for deterrence. To respond to hybrid warfare, we need comprehensive defence strategies and plans. But what exactly should be the responsibilities of civilian, government and armed forces? Are deterrence strategies keeping pace with political, military and technological changes? Are there dangers for liberal states of entering into new hybrid wars that have no end?

My critical literature review of Canadian and NATO political and military responses to Russia[1] published in 2017 discovered many academic and policy gaps. [2] Interviews highlighted that bureaucratic knowledge was ahead of academic conceptual thinking and policy development on hybrid challenges. I argued that strategic thinking needed to be updated and I found uncertainty about whether or not, and how exactly to respond to a whole array of non-military activities and what NATO's 'red lines' should or should not be.

Over the past two years, many of the policy gaps are being filled (while many academic gaps on Canada's role remain). In reviewing rhetoric and actions, this paper will show that NATO and Canada have employed a range of responses to address so-called hybrid challenges. NATO and Canada have become more internally focused (deterrence as resilience) adopting a "whole of government" and increasingly "whole of society" approach, while at the same time taking more offensive actions (deterrence by punishment, eg in the cyber, diplomatic and political realms) and developing multinational partnerships (NATO, G7, EU) and capabilities.

Similar to the period after 11 September 2001, when there was a rush to create counter-terrorism and counter-insurgency policies, much of Canada's current actions and institutional initiatives are being implemented in haste. Hybrid or blended threats are not new, they have recognized for a long time.[3] However, today - in response to

[1] This paper uses "Russia" in reference to the government of "The Russian Federation". The author acknowledges the importance of domestic politics and the role of the public, but here the focus is on the government or regime.

[2] Nicole Jackson "NATO's and Canada's Responses to Russia since the Crimea Annexation of 2014: A Critical Literature Review," *Simons Papers in Security and Development*, no.61 (December 2017). Download available: http://summit.sfu.ca/item/17651

[3] Frank G Hoffman is generally credited as an early articulator of "hybrid." See for example, Frank G Hoffman, "Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict," *Strategic*

globalization, technological advancements, as well as a heightened perception of "democracies being under threat" and the "erosion of international norms", there is a scramble both to adjust with new policies and to build upon earlier achievements. The result has been more about implementing what is possible in response to an evolving context of 'threats', rather than a top-down strategy that aims at peace or addresses the root causes of conflict.

Of course, Russia is only one of several state and non-state actors that have inspired this transformation. However, Russia's recent actions[4] have been widely understood as part of a "wake up call" – a realization that Western adversaries are taking actions, often below the level of conventional wars, in areas that international law and institutions have not been able to constrain. How Canada and NATO interpret major transformations, and the language of 'hybrid war' that they adopt, matter because they influence responses.

The paper first examines the controversies and advantages of the term 'hybrid warfare' (including, briefly, Russia's perception) and some implications and dangers in responding to such activities. Second it briefly looks at deterrence and controversies over how to respond to hybrid warfare through a variety of measures ranging from the more defensive 'hybrid deterrence' and societal and institutional resilience to more aggressive measures, and lists some of the strengths and limits of classic deterrence theory for thinking about hybrid challenges. Third, the paper outlines the evolving rhetoric of NATO and Canada and their overall responses. I will show that Canada and NATO are taking significant steps towards more "comprehensive deterrence,"{ and suggest that we need more clarity in how we combine responses. NATO counters hybrid warfare globally as part of its collective defence. It also now cooperates on strengthening member states' domestic security and societal and institutional resilience. In line with NATO, Canada's defence policy also addresses hybrid warfare and Canada

Forum, National Defence University, April 2009; and Frank G Hoffmann, "Hybrid Warfare and Challenges," *Joint Forces Quarterly*, Issue 52, 1st quarter (2009). Hoffman pointed to the 2006 Second Lebanon War as an example of a hybrid war.

[4] These begin with Russia's annexation of Crimea in 2014 in contravention of international law (following its military involvement in Georgia in 2008), and include its continued involvement in Eastern Ukraine, military actions in Syria, a variety of confirmed and alleged electoral, cyber and other interferences in the US and other countries including the chemical poisoning of the Skripals.

has adopted similar rhetoric and a wide range of military, and increasingly civilian responses, to various hybrid threats, both at the international and, most recently, at the domestic level. Here we are witnessing the development of "whole of government" and "whole of society" approaches which include a wide array of new institutions, military and civilian non-military activities.

Hybrid wars, hybrid threats: terminology and controversies

The terminology of "hybrid warfare" has been widely used to describe the mix of tactics used by Russia in its annexation of Crimea. The term helpfully highlights the (ever-present) "grey zones" of international relations that lie between peace and war. The tactics include the use of special forces, military intelligence, propaganda or information warfare, agitation, and the use of nationalist actors and unmarked soldiers to cause disorder or enact change within a state. The term points to the secrecy and subterfuge of some of these tactics, and the lack of clarity about others, which adds uncertainty about what exactly is or is not occurring (whether one is really under attack or not).

Today's critics of the term "hybrid warfare" often explain that it is too vague and includes too many different tactics to be analytically helpful or accurate. The reality is that even before 2014, the term had been roundly criticized for lacking academic vigour, conceptual vagueness and applying to just about every conflict.[5] Since Russia's annexation of Crimea in 2014, the term "hybrid warfare" has been adopted in reference to many different kinds of actions that Russia has undertaken globally (some share similarities with former Soviet techniques such political and economic interference or propaganda, others include newer elements such as cyber attacks and electromagnetic activity operations) as well as in reference to a variety of activities undertaken for example by China and Iran and non-state actors, e.g. ISIL.

[5] See, for example, Colin Gray, *Another Bloody Century* (London: Phoenix, 2006); Peter Mansoor and Williamson Murray, eds., *Hybrid Wars – Fighting Complex Operations from the Ancient World to the Present* (Cambridge: CUP, 2012); Francis G. Hoffman "Future Hybrid Wars: An Update," *Perspectives on the Future Security Environment, Statement to the Subcommittee on Intelligence and Emerging Threats and Capabilities, US House of Representatives Armed Services Committee*, 13 February 2012.

The “warfare” part of the label may also be criticized as dangerously justifying or "securitizing” military responses, for example in the area of cyberspace and information, just as the “war on Islamic fundamentalism” came to be perceived as a military security problem when it was packaged as part of a broader transnational and global conflict. A recent RAND study proposes the term “statecraft” so as not to adopt the language of war.[6] In the policy literature and in practice, hybrid “warfare” also remains poorly differentiated from hybrid “threat.” Nevertheless, the terminology of “hybrid warfare” and “hybrid threat” have become widely adopted, which continues to lead some commentators to mistakenly assume that these are new tactics, when, as mentioned above, they have a long history of use by state and other actors.[7]

Nevertheless, despite the many criticisms, the term “hybrid warfare” continues to be used because it helpfully highlights the hostile nature of many current challenges and the “weaponization” of non-military means. In the case of Russia, there is evidence that it uses a wide range of hostile non-military and sometimes clandestine tactics. These are often sophisticated and increasingly deployed by the Russian state and non-state actors both domestically and externally. They seem to be strategically coordinated or more ad hoc, depending on the case. Every war has some degree of hybridity, however as is often noted, unlike Western doctrine Russian doctrine does not distinguish between peace and war. And similar to many non liberal democracies, Russia’s civilian and military responses (and responsibilities) are not as clearly divided. It may thus be that we need a specific term for Russia’s more recent hybrid actions, some of which seem to have unique (Soviet) characteristics, for example Russia’s increasingly overt (and almost mocking) use of denial and ambiguity as means in themselves to achieve legitimacy or generate support for its objectives.[8]

The Russian Ministry of Defence itself uses a very broad interpretation of “strategic deterrence’ (sderzhivanie strategicheskoe) which includes a vast array of

[6] Linda Robinson, et al., *Modern Political Warfare: Current Practices and Possibilities* (Santa Monica: RAND 2018). Online at https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1772/RAND_RR1772.pdf

[7] For a recent review of the literature on hybrid warfare see: Robert Johnson, “Hybrid War and its Countermeasures: A critique of the literature,” *Small Wars and Insurgencies* 29, no.1 (2018): pp.141-163. For a review of the Canadian literature see Jackson, *Ibid*.

[8] The Soviet Union was well-known for using deception and ”active measures.”

coordinated military and non-military tools (including cyber, diplomacy, information, economic, legal, ideological, military, political) to be used as a complement to nuclear deterrence capabilities in times of peace.[9] It should be emphasized here that Russia claims that the West itself has used a mix of non-military instruments around the globe, in particular in the so-called "colour revolutions" and even within Russia itself. Russia's hybrid (or ambiguous or blended) activities are thus understood as rational means of response that correspond to Western activities (equivalent to its militaries' "comprehensive approach"[10]), and necessary for Russia to counter real and perceived asymmetries.[11]

Despite the many controversies, this paper shows that the term "hybrid warfare" is used by NATO and the Canadian government. Of course, in practice, as well as conceptually, it remains important to strive for a common understanding of 'hybrid warfare' so that policymakers, military personnel and bureaucrats are 'on the same page' and able to consider and implement appropriate responses. Canada has been involved in a multinational initiative that has recently produced a Handbook (2019) which provide conceptual guidance on hybrid warfare. The Handbook emphasizes the following characteristics of hybrid warfare: multiple instruments of power used in a synchronized attack, tailored to specific vulnerabilities, with an emphasis on creativity

[9] For analyses of the Russian approach see: Kristin Van Brusgaard, "Russian Strategic Deterrence", *Survival* 58, no.4 (2016): pp. 7-26; Charles K Bartles, "Getting Gerasimov Right," *Military Review (Jan-Feb 2016):* pp 30-38; Dmitri Adamsky, "Cross-Domain Coercion: The Current Russia Art of Strategy," *Proliferation papers*, Ifri Security Studies Center 54 (2015); Ofer Fridman, "Hybrid Warfare or Gribidnaya Voyna," *The RUSI Journal* 162, no.1 (Feb/March 2017): pp.42-29.

[10] Canada's 'Comprehensive Approach' is defined in CAF doctrine as bringing "together all the elements of power and other agencies needed to create enduring solutions to a campaign. These may include: military (joint and multi-national forces), Canadian government departments and agencies (whole of government), foreign government and international organizations (e.g. NATO and UN) and public funded organizations (e.g. NGOs). *Canadian Forces Joint Publication CFJP 3.0 Operations*, September 2011. Quoted in Neil Chuka and Jean Francois Born, *Hybrid Warfare, Implications for CAF Force Development DRDC*, August 2014, p.11.

[11] Mark Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine', *Foreign Policy Magazine*, 5 March 2018. Online: https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/ Valery Gerasimov "Contemporary Warfare and Current Issues for the Defence of the Country", *Journal of the Academy of Military Sciences* 2, no.59 (2017); Valery Gerasimov "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations", *Voyenno-Promoyshkennyy Kurier,* 26 (February 2013). http://vpk-news.ru/articles/14632

and ambiguity.[12] The argument presented below is that how Canada and NATO interpret what is occurring as a "war" (and an assault on the 'rules based order') and the language of hybridity that it uses, guides responses to what is believed to be evolving.

Thinking Through the Spectrum of Responses to Hybrid Threats and Hybrid Wars: Advantages, Controversies and Limits

The inconclusive debate over the term 'hybrid warfare' in the academic and military literature is part of a larger conversation about definitions of war and controversies over whether and how to discourage a wide range of undesirable behaviour or activities[13] Since hybrid threats include a wide range of activities, it follows that measures are considered along the full spectrum of responses. However, compared to trying to respond to each activity, a more strategic approach would provide clarity of purpose. This point largely has been absent from the academic and policy literature on hybrid warfare.[14] At the same time, hybrid warfare takes place on a continuum of threat, and therefore responses also need to be tailored to the specific type or degree of the threat or 'attack.[15] Policy choices range from not responding, to deterring aggression, to taking more aggressive actions to disrupt or prevent further attacks.

Deterrence here is about preventing an attack in the first place. The traditional military understanding of deterrence is based on the idea that a potential aggressor's cost-benefit calculation might be influenced by the threat of a punitive response or by

[12] This document was written by contributing nations and international organizations of the Multinational Capability Development Campaign (MCDC) 2017-18. It does "not necessarily reflect the official views or opinions of any single nation, government or organization, but is intended to provide conceptual guidance and recommendations for multinational partners' consideration". Ed. Sean Monaghan, "MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare", *Multinational Capability Development Campaign*, March 2019, p. 13. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf

[13] For a review, see Rod Thornton, "The Changing Nature of Modern Warfare," *The RUSI Journal* 160, No. 4 (2015); pp. 40-48.

[14] This point is developed in Johnson, *Ibid.*; and in Jackson, *Ibid*.

[15] MCDC, *Ibid.*, p. 17.

the realisation that the defender's preparations are so advanced or effective that the costs of carrying out the aggression would be too great. Deterrence is thus a psychological means to alter the cost-benefit interaction between actor and adversary. The literature on classical deterrence posits that deterrence prompts voluntary changes in behaviour, in which a capable adversary is convinced not to harm you. Adversaries weigh the costs *and* benefits of their actions and alter their behaviour accordingly. Red lines need to be drawn, communicated and defended, showing the resolve to carry out threats. The traditional deterrence literature thus argues that for deterrence to function, the deterrer must have the will and ability to communicate a credible capability (referred to as the "three Cs"). [16]

In practice, deterrence is about manipulating another's behaviour to suit your goals. It may occur "by denial," threatening an adversary's behaviour with failure (stopping an aggressor from achieving goals by disrupting their activities) or 'by punishment' (through some retaliation and imposition of harm or costs). When hearing the term "deterrence" many people think about Mutual Assured Destruction (MAD) which threatened a US nuclear exchange with the Soviet Union in order to deter Soviet use of nuclear weapons against the US and its allies. However, a less extreme understanding of deterrence is one which combines several threats such as conventional and nuclear attack, economic sanctions or other diplomatic pressures etc.

As will be seen below, hybrid warfare complicates the traditional logic of deterrence, which is already controversial.[17] Nevertheless, there is a body of literature that argues that deterrence can still be accomplished. The so-called "fourth wave" of deterrence is considered to have begun at the end of the Cold War, when threats came to be perceived as more uncertain and less predictable. Many scholars have written about a new, more complex and less state-centric environment defined by asymmetric challenges. Actors seemed to be beyond traditional deterrence approaches and no longer reacted as expected. Today, some scholars are arguing that we are entering the

[16] There is a very large literature on this subject. Some recent examples include: David Jordan et.al, *Understanding Modern Warfare* CUP, Cambridge 2016; Andrew F Krepinkevich Jr, "The Eroding Balance of Terror", *Foreign Affairs* 98, no.1 (January/February 2019).

[17] I am examining this in detail in a forthcoming publication on NATO and Canada in the Baltics. See also Alex S. Wilner, "Cyber Deterrence and Critical Infrastructure Protection: Expectation, Application and Limitation, *Comparative Strategy* 36, no.4 (2017): pp. 309-318.

"fifth wave" of deterrence, a period defined by the need for "resilience," that is to "establish socio-technical systems with the dynamic ability to anticipate and respond proactively to potential threats by learning and adapting."[18] In other words, the diffuse nature of today's threats may lead to more distributed responses through existing or new networks as opposed to traditional and hierarchical approaches. It is widely believed that improving overall resilience requires addressing vulnerabilities and taking a long-term approach to build strong and adaptive infrastructure, ensure social cohesion and sustain trust in government. Resilience thus not only mitigates the harmful effects of hostile influence, but it can also change the adversary's overall cost-benefit calculation.

Thus, deterrence can be accomplished through a coordinated approach by governments and civilians to address vulnerabilities by building resilience. Strengthening resilience can been done both domestically and globally through political means (e.g. efforts to secure elections, to increase trust in democratic institutions), military means (e.g. military strength and defence cooperation), economic means (e.g. anti-corruption, securing of strategic resources), social means (e.g. increasing awareness of hybrid threats, preventing the exploitation of social division through foreign financing or support), infrastructure means (physical and digital), or information means (e.g. strategic communication).[19]

However, to deter or dissuade an adversary from aggression one may need to go beyond resilience. Here, "comprehensive deterrence" requires to threaten or impose costs (deterrence by punishment). This may include military actions (kinetic and non-kinetic), political (e.g. travel restrictions, expulsion of diplomats), economic (e.g. sanctions, financial penalties), civil (e.g. transparency through public blaming and making public names of suspects e.g. in the Skripal case), and information (e.g. education, legal action) as well as through international law.[20] To prevent an adversary from taking further action, some decision-makers argue for responses beyond

[18] Tim Prior, "Resilience: The 'Fifth Wave" in the Evolution of Deterrence", *Strategic Trends 2018; Key Developments in Global Affairs*, Center for Security Studies, ETH Zurich, 2018.

[19] MCDC, *Ibid,* p.44-45

[20] Aurel Sari, *Blurred Lines: Hybrid Threats and the Politics of International Law*, The European Centre of Excellence for Countering Hybrid Threats, Helsinki, January 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3164265

deterrence which may disrupt or degrade capacity for action. These are some of the most controversial cases. A very recent example is when the US placed "implants" – software that can be used for surveillance or attack - inside Russia's power grid. Apparently, this was in response to Russian intelligence units shutting off power inside Ukraine in December 2015, and then allegedly making inroads into the US energy grid. To quote US National Security Advisor, John Bolton, "We will impose costs on you until you get the point."[21]

As mentioned above, an application of traditional deterrence logic to hybrid activities, reveals substantial obstacles and potential limits. Here, I briefly list some of these in relation to two examples, cyber and disinformation. First, these tactics, similar to terrorism, give more power to comparatively weaker states and non state actors. This helps to explain Russian (and other actors') attempts to try to "offset" their comparative (and perceived) military weaknesses by investing in these areas. Relatively tronger societies, such as Canada, are the most connected to cyber, and democracies are the most supportive of free speech. They are therefore especially vulnerable and to some degree such activities are inevitable. Second, responses to these phenomena (especially, but not only, retaliatory or offensive actions e.g. cyber attacks or counter-propaganda) are not at all straightforward, they are controversial and pose many challenges. As such, stronger states and democracies tend to favour other types of (cross domain) responses (e.g. sanctions, diplomatic expulsions etc.). This in turn poses a dilemma for traditional deterrence theory because, over time, a continued lack of direct response is said to harm credibility. Third, in both cases, it may be difficult to detect a hybrid "attack" (many cyber attacks go undetected as does much disinformation) and it is not easy to differentiate between which activity merits a response and which one does not. What is legitimate spycraft? What is the line between normal public debate and disinformation with the intent of destabilization or harm? Who gets to decide? Thus, in considering responses to hybrid challenges an urgent and ongoing issue is, and will be, how to ensure that we can retain our liberal values.

[21] David Sanger and Nicole Perlroth, "US Escalates Online Attacks on Russia's Power Grid," *New York Times,* June 15, 2019. Online: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html With new authority granted to the US Cyber Command, the US has also taken action to overwhelm the computer systems at Russia's Internet Research Agency, one of apparently four operations organized around the midterm election.

Fourth, there are many difficulties in creating and communicating ‘red lines’, deciding when a threshold is crossed and what kinds of response or retaliation is necessary. There may be advantages in not telling your potential adversaries what your plans and ‘red lines’ are, to allow political freedom of movement or to give pause to an adversary that is uncertain whether there may be retaliation. However, this vagueness may also strengthen hybrid warfare and the probability of conflict. In some cases, clarity may help prevent accidental flashpoints and promote general stability. A solution proposed by the UK is to clearly communicate to an adversary that you do not wish them to pursue a particular course of action, but at the same time to withhold details of the specific threshold or response.[22]

A fifth challenge in applying classic deterrence theory, is that it posits that deterrence is best practiced against a known adversary, yet attribution in many of these cases may be technically, or perhaps even more likely, politically challenging or even impossible. It may also be hard to know when responses have succeeded (or failed). Recently, the literature has acknowledged that some attacks (and failure to see or respond to them) are inevitable. The term “cumulative deterrence” has been used to suggest a realistic approach, one in which partial responses are delivered gradually in the hope of changing an adversary’s behaviour in the long run.[23]

Most measures examined in the MCDC study (of 16 countries) mentioned above were defensive, focusing on resilience in the political and informational spheres, as well as increased intelligence gathering measures, and capacity building. [24] Meanwhile, over half the offensive measures were taken by the military (defence and civil). The challenges of relying on military activities are that they may be overly forceful, result in dangerous miscalculation or provoke escalatory reactions (or adverse reactions among the domestic population). In comparison, addressing hybrid war through non-military means has many advantages and seems to be the obvious response for Western liberal democracies. However, there are also possible dangers in addressing hybrid war

[22] UK Ministry of Defence, “Deterrence: The Defence Contribution,” *Joint Doctrine Note* 1/19, February 2019, p. 47. Online: https://www.gov.uk/government/publications/deterrence-the-defence-contribution-jdn-119

[23] Uri Tor, “’Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence”, *Journal for Strategic Studies* 40, no.1 (2017): pp. 92-117.

[24] The MCDC Handbook Countering Hybrid Warfare includes 16 countries and organizations.

through non-military means. As the MCDC warns, "Paradoxically, overdoing resilience and government-led intervention here may undermine the very fabric of society that it is trying to be preserved in the first place."[25] And as Simpson, writing about global terrorism and counter-insurgency, warns: if war is expanded to include "all means that can deliver political effect: violence is mixed with other political activities, so that there is a severe erosion of the interpretive different between military and political activities, war and peace" and organized violence is then no longer constrained.[26] Similarly, in hybrid war, traditional war is merged with other activities, and the danger is that policy to address it may become an extension of war rather than vice versa.

Additionally, as I have written elsewhere, to effectively respond to (deter) Russia there needs to be a balanced political and military strategy, focused on Russia, and based upon a sound understanding about Russia's perceptions, aims and limits.[27] For example, many scholars believe that Russia is using hybrid warfare, among other means, to ensure or enact its status as a great power and sovereign state.[28] Its actions are, in part, in response to Western (US, NATO) actions with the aim (as the Russian state claims) to create a more pluralist order or (as many in the West interpret) to challenge the current rules-based order. Whatever the case, "root causes" need to be directly confronted as part of Western responses, and possible repercussions of actions carefully thought through.

NATO and Hybrid: From Collective Defence to Internal Resilience

Since mid-2014, NATO has been using the terms "hybrid threats" and "hybrid warfare" in relation to Russia (and other actors). And aside from its more "traditional" (nuclear and conventional) military responses, NATO has also been developing its own

[25] MCDC in Annex C looks at the current state of countering hybrid warfare policy.

[26] Emile Simpson, *War From the Ground Up; Twenty-First-Century Combat as Politics* (New York: OUP, 2019), p.231.

[27] Nicole Jackson, "Canada, NATO and Global Russia," *International Journal* 73, no. 2 (June 2018): pp. 317-325.

[28] See for example, Roger Kanet, ed., *Handbook of Russian Security* (London: Routledge, 2019).

"hybrid responses."[29] NATO's definition of "hybrid warfare" is all-encompassing in that it includes the use of both conventional tactics traditionally associated with violent warfare *and* so-called non-conventional or non-violent tactics. NATO defined hybrid issues a strategic priority at the Warsaw Summit in 2016. Section 72 of the Warsaw document states that the Alliance and the Allies will be prepared to counter hybrid warfare as part of collective defence and that the Council could decide to invoke Article 5 of the Washington treaty in response.[30]

NATO's difficulties in countering hybrid efforts are partly because of the very nebulous and secretive nature of many hybrid activities and because NATO is a large, rules-based organization made of democratic states which does not have the same flexibility as authoritarian Russia. NATO's strategy to "prepare, deter and defend" against hybrid threats is based on a "all-of-NATO" approach, of which Canada is part.[31] My research in 2017 showed that hybrid activities were perceived by NATO as the "number one" threat emanating from Russia and this continues to be the case.[32] While Russia's various activities in this area were the focus of a lot of attention post 2014, policy in countering them was mostly piecemeal. This has now changed. In a forthcoming article, I examine more specifically Canada's significant role in Latvia and Ukraine as a response to Russia and possible conventional (and hybrid) action. However, the point here is that NATO (and Canada in NATO) has become engaged in a very wide spectrum of *global* responses to hybrid threats. To give just two very recent examples of its global role, NATO now has a Joint Intelligence and Security Division

[29] There is now a large literature here. See for example, Guillaume Lasconjarias and Jeffrey A Larsen, eds., *NATO's Response to Hybrid Threats,* NATO Defense College, 2015; Elizabeth Oren, "A Dilemma of Principles: The Challenges of Hybrid Warfare From a NATO Perspective," *Special Operations Journal* 2, no. 1 (2016): pp. 58-69; Sorin Dumitru, "The Cyber Dimension of Modern Hybrid Warfare and its Relevance for NATO," *Europolity* 10, no. 1 (January 2016): pp. 9-23; Safak Oguz, "The New NATO: Prepared for Russian Hybrid Warfare?" *Insight Turkey* 18, no. 4 (2017): pp. 165-180; Andrew Radin, *Hybrid Warfare in the Baltics: Threats and Potential Responses* (Santa Monica: RAND Corporation, 2017). Online: https://www.rand.org/pubs/research_reports/RR1577.html

[30] *Warsaw Summit Communique*, Issued by Heads of State and Government participating in meeting of the North Atlantic Council in Warsaw, 8-9 July 2016. http://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber

[31] NATO Website, *NATO Responses to Hybrid Threats,* 17 July 2018. https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=en

[32] Nicole Jackson, "NATO's and Canada's Responses to Russia since the Crimea Annexation of 2014: A Critical Literature Review," *Ibid.* http://summit.sfu.ca/item/17651

which conducts global analysis of hybrid threats. It also has "counter hybrid support teams," created in late 2018 and first fielded in 2019, to provide ad hoc assistance to member's militaries and governments upon request.

At the same time, NATO has also become increasingly focused internally on its member states' domestic security and resilience, as well as on the more well-known operations abroad such as in Eastern Europe and the Middle East. NATO's Civil Emergency Planning Committee, which supports civil preparedness and thus "resilience" against hybrid threats, has been resurrected. The result is that the roles of member states' ministries of the interior and ministries of public protection are being enhanced in relation to hybrid threats, while ministries of defence and foreign affairs are becoming part of a broader "whole-of government" effort. "Internally, providing credible deterrence to hybrid threats is straightforward: building and maintaining resilient, credible and capable governance that raises the price of hybrid aggression and reduces its chance for success. To do so requires cooperation and collaboration from all entities."[33]

Especially in the past couple years, NATO and member states such as Canada have clearly understood that they need to make their publics more aware of what is happening and to better explain the need for responses to hybrid interference, for example in the cyber and information/media realms.[34] Here NATO has increasingly turned to other partner organizations such as the EU and the private sector for assistance, including in the area of "societal resilience" through a "whole of society" approach. The reasoning is that if Russia (or other actors) interfere abroad, in part by exploiting liberal values and institutions, then taking action to "strengthen our democracy" should help to close "loopholes" that allow for (hidden) interference through disinformation etc.[35] Civil society actors such as NGOS, open media, and universities can help to monitor and expose this interference. And if societal security

[33] Chris Kremidas Courtney, "Working with NATO to Address Hybrid Threats," *The Foreign Service Journal*, April 2019. Online: https://www.afsa.org/working-nato-address-hybrid-threats

[34] Nicole Jackson "NATO's and Canada's Responses to Russia since the Crimea Annexation of 2014: A Critical Literature Review," *Ibid*. http://summit.sfu.ca/item/17651

[35] Mikael Wigell, "Hybrid interference as a wedge strategy: a theory of external interference in liberal democracies," *International Affairs* 95, issue 2 (March 2019): pp. 255-275.

can be strengthened, it will make it harder for nefarious actors to exploit Western democratic pluralism to their benefit.

In 2018, NATO headquarters began to assess member states' vulnerabilities and institutional resilience in the following areas: assured continuity of government and critical government services, energy supplies, ability to deal effectively with the uncontrolled movement of people, food and water resources, ability to deal with mass casualties, resilient communications systems, and transportation systems.[36] Efforts have also been taken to increase NATO's international cooperation in these areas, for example through 'enhanced cooperation' with the EU. In July 2016, a joint EU-NATO declaration made building resilience and the ability to counter hybrid threats a priority, in particular in the area of cyber security, information sharing and coordinated strategic communications.[37] In September 2018, NATO's North Atlantic Council and the EU's Peace and Security Committee began scenario-based discussions followed by parallel exercises on hybrid threats. And in July 2018 a second joint EU-NATO declaration focused on military mobility, counter-terrorism and resilience to risks posed by chemical, biological, radiological and nuclear agents. Thus, NATO is implementing a broad governance approach to hybrid threats, as opposed to developing a purely military framework.

Canada and Hybrid

Canada also is adopting a "whole of government" and, increasingly, a "whole of society" approach to hybrid warfare, focused on internal as well as external challenges. Hybrid warfare has been part of the Canadian Armed Forces joint level force development scenario since 2012.[38] Reflecting the broader academic debates over the concept hybrid, there has been little consensus about definitions in the literature

[36] Wolf-Diether Roepket and Hasit Thankey, "Resilience: The First Line of Defence", *NATO Review Magazine*, 27 February 2019. https://www.nato.int/docu/review/2019/Also-in-2019/resilience-the-first-line-of-defence/EN/index.htm

[37] President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, *Joint Declaration on EU-NATO Cooperation*, 8 July 2016. Online: https://www.nato.int/cps/en/natohq/official_texts_133163.htm

[38] Chief of Force Development (CFD), The Directorate of Capability Integration, *Hybrid Warfare Concept*, June 2012.

produced by the Canadian military.[39] Nor has there been much Canada (or Canadian) specific research on this topic.[40] However, despite their lack of definitional consensus, DND/CAF documents do highlight many of the same global trends referred to as hybrid warfare today (the blending and blurring of tactics, the involvement of wide variety of actors, the innovative use of technologies) and share similar conclusions (e.g. that the future security environment will be highly uncertain). [41] In 2014, a DRDC review of this literature argued for a better understanding of the military strategic and operational levels, and questioned key assumptions (e.g. that alliances are the best way to win such wars). [42] The authors' cautions remain relevant today - not to overlook conventional strengths in the search for new capabilities and skills, nor to over-assume adversarial capabilities, or presume that technology will be the solution for all challenges. More recently, there have been increased calls for 'threat-based planning' and for a Canadian strategy for countering hybrid warfare. And in 2017, Canada's defence policy, *Strong, Secure, Engaged* (June 2017) directly addressed challenges for Canada in detecting, attributing and responding to "hybrid warfare" and allocated new resources to cyber operations, intelligence, and information operations (including "influence activities" which may have psychological or behavior affects).[43] In my interviews that year, some stressed the importance of confronting hybrid issues as part of the "full spectrum of deterrence", while others (including many in DND) argued that Canada ought to remain focused on more traditional military threats and responses.[44]Canadian practitioners and government analysts were clearly working on the questions (many details of which are classified).

[39] Neil Chuka and Jean Francois Born, *Hybrid Warfare: Implications for CAF Force Development*, *DRDC*, August 2014

[40] Nicole Jackson "NATO's and Canada's Responses to Russia since the Crimea Annexation of 2014: A Critical Literature Review," *Ibid*. http://summit.sfu.ca/item/17651

[41] P J Gizewski and N J Faragalla, *Three Voices, One Vision: Land, Naval and Air Views of Future CAF Operations*, 2013.

[42] Neil Chuka and Jean Francois Born, "Hybrid Warfare: Implications for CAF Force Development," *DRDC*, August 2014, p.5

[43] Department of National Defence, *Strong, Secure, Engaged; Canada's Defence Policy*, June 2017. Online: http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf

[44] Nicole Jackson, "NATO's and Canada's Responses to Russia since the Crimea Annexation of 2014: A Critical Literature Review," *Ibid*. http://summit.sfu.ca/item/17651

Since then, Canada, has taken a range of political, military and other actions to address various transnational as well as global hybrid threats. And, just within the past year, the number of new initiatives, especially in the area of cyber and digital disinformation, has grown exponentially. According to my discussions at Global Affairs Canada, a key moment (beyond Russia's annexation of Crimea in 2014) contributed to the Canadian government's growing awareness that it needed to "step up" and respond with a 'whole of government' approach at the domestic as well as global level. [45] The catalyst for action was in March 2018 when Russian military intelligence officers allegedly poisoned the Skripals. Of course, Russia's many other (real and alleged) interferences especially in the US (and other) elections, had received a lot of attention and concern. However, in the Skripal case Canadian government officials watched in real time as the UK government scrambled over how best to respond.

The implications of hybrid warfare for Canada are somewhat unique. Although globalization and technological advancements have eroded borders, Canada's geography and geopolitical circumstances give it comparative latitude and allow strategists the luxury of thinking through advantages and costs of different responses and commitments. Thus as Canada becomes engaged in a wide range of military, political, economic and civilian responses, Canada has the opportunity to be clear in how and why we combine them. One difficulty in classifying some of these responses at the domestic, transnational or global level is that distinctions between levels have become blurred, with a possible danger that policies may also be ill-defined or overlapping.

Here are four examples that illustrate the diverse and wide range of Canada's *global* military responses to hybrid threats or potential hybrid threats from *Russia*. First and most significantly, Canada leads a NATO battle group in Latvia (extended to 2023) which, along with other troops in Eastern Europe, is both learning about hybrid challenges and engaged in a range of hybrid operations which include communications and, most recently, electromagnetic warfare.[46] This is the focus of a forthcoming article

[45] Discussions with officials at Global Affairs Canada, 22 May 2019.

[46] Stephen Fuhr, "Canada and NATO: an alliance forged in strength and reliability," *Report of the Standing Committee on National Defence*, Ottawa, House of Commons, June 2018. Online: https://www.ourcommons.ca/Content/Committee/421/NDDN/Reports/RP9972815/nddnrp10/nddnrp10-e.pdf ;

of mine and therefore not addressed in detail here. Second, Canada (and NATO) increasingly shares information and engages in analysis of hybrid challenges with other states and NGOs. For example, in 2018 Canada joined The European Centre for Excellence in Countering Hybrid Threats (Hybrid CoE). Third, Canada is helping Ukraine build its police force and counter foreign interference in its elections through its Police Training Assistance Project run out of Global Affairs Canada (GAC). Along with the Canadian Armed Forces (CAF) mission to support the Security Forces of Ukraine, Operation UNIFIER (recently extended to 2022), this is part of Canada's broader assistance to Ukraine including countering hybrid threats. Fourth, Canada is focused on preparing for future hybrid threats by updating the skills of its security and military forces. For example, the Special Forces are seeking a wider range of backgrounds and diverse skills and training as they aim to increase their numbers. [47]

Canada, of course, has taken other political, economic and legal steps towards 'comprehensive deterrence' in response to Russian actions. These have been subject to much less academic study than our military responses. They include the expulsion of Russian diplomats (after the Skripal poisonings), and a wide range of sanctions against Russian businesses and individuals. The latest round of Canadian sanctions was imposed (along with the US and EU) in March 2019 on 114 individuals and 15 entities in response to Russia's continued involvement in Ukraine and the confrontation in the Kerch strait.[48] The sanctions are controversial. They signal the unity of Western powers, but so far seem to have had a modest effect on Russia's economy and little immediate impact on Russia's behavior.[49] Canada has also made significant attempts in the area of international law to address gray areas of uncertain nor non-existent government

Government Response to the 10th Report of the Standing Committee on National Defence, Entitled: Canada and NATO: An Alliance Forged in Strength and Reliability, Online: https://www.ourcommons.ca/content/Committee/421/NDDN/GovResponse/RP10083758/421_NDDN_Rpt10_GR/421_NDDN_Rpt10_GR-e.pdf

[47] Lee Berthiaume, "Canadian Forces looking at recruiting elite, special forces right off the street", *Global News*, March 6 2019 https://globalnews.ca/news/5029229/canada-special-forces-soldiers-recruit-street/

[48] Canadian Government Website, *Canadian Sanctions Related to Russia* https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/russia-russie.aspx?lang=eng

[49] Andrew Chatsky, *Have Sanctions on Russia Changed Putin's Calculus?*, Council on Foreign Relations, 2 May 2019, https://www.cfr.org/article/have-sanctions-russia-changed-putins-calculus

authority. Here Canada has worked with other nations to clarify of laws surrounding the cyber domain. The Tallinn Manual 2.0 (published 2018) is currently the most comprehensive analysis of how existing international law applies to cyberspace.

Canada, like NATO has also adopted similar thinking about "resilience as defence:" "We… stand united in our resolve to maintain and further develop our individual and collective capacity to resist any form of armed attack. In this context, we are today making a commitment to continue to enhance our resilience against the full spectrum of threats, including hybrid threats, from any direction."[50] In reaction to Russian digital hacking and its manipulation and dissemination of false information (as well challenges from China, Iran, ISIL, and right-wing extremism (RWE)), Canada has recently focused on how to respond to foreign interference, including disinformation. Even among those who do not use the terminology of "warfare," many now believe that this disinformation, often carried out in the cyber world, is a key part of a broader "hybrid campaign" aimed to undermine social cohesion and the democratic process. Reflecting NATO's call to strengthen domestic resilience, Canada has developed loose coordination amongst different units in the government to do this. Government departments involved include not just CSIS, CSE, DND, GAC, PCO, RCMP but also Elections Canada, Heritage Canada and multinational actors including NATO, Five Eyes, the EU and G7.

The Canadian approach broadens traditional security and takes on a coordinating role with other foreign governments and NGOS, for example in developing national and international regulatory frameworks and norms. To give just one of a plethora of examples, Canada and other G7 countries agreed in the Charlevoix Commitment to defend democracy from online foreign threats . The document calls "on others to join us in addressing these growing threats by increasing the resilience and security of our institutions, economies and societies, and by taking concerted action to identify and hold to account those who would do us harm."[51] As a result, Canada has become the network co-ordinator of the cyber Rapid Response Mechanism created to

[50] NATO, "Commitment to enhance resilience," Warsaw, July 2016. Online: https://www.nato.int/cps/en/natohq/official_texts_133180.htm

[51] The Charlevoix G7 Commique, 9 June 2018 Online: https://www.international.gc.ca/world-monde/international_relations-relations_internationales/g7/documents/2018-06-09-summit-communique-sommet.aspx?lang=eng

strengthen co-operation between countries to identify, respond and share regular reports about threats. On 23 April 2019 Canada's Minister of Democratic Institutions, Gould announced that the government has formed a plan to combat this interference based on four pillars: educating Canadians on the dangers and prevalence of misinformation online; improving organizational readiness within the government to quickly identify threats or weaknesses; combatting foreign interference via Canada's security agencies; and expecting social media platforms to increase transparency, authenticity and integrity of their systems.[52] Canada's 2019 federal budget shows that the Liberal governments priorities in national security include cyber and election security, as well as anti-racism, and economic security. The amount set aside for cyber and electoral security includes $144.9 million over five years to the CSE (including 22.9 million already allocated) to protect infrastructure in finance, telecommunications, energy and transport sectors, which will also include new legislation to develop a new "critical cyber systems framework;" $80 million to universities for cyber security networks, $67.3 million over five years followed by $13.8 million per year ongoing to Public Safety Canada, Innovation, Science and Economic Development Canada, Global Affairs Canada and the RCMP to raise cyber security awareness; 30.2 million over five years to project democracy and elections from foreign interference and election misinformation (which allows CSE to provide cyber advice and guidance to political parties and election administrators to protect information and data, Global Affairs to strengthen information sharing between G7 on "foreign threats," and Heritage Canada to educate Canadians to recognize online disinformation).[53]

Conclusion

In reviewing rhetoric and actions, this paper has shown that many of the previous policy 'gaps' have begun to be filled as Canada and NATO have taken

[52] James Jackson, "Minister assesses the cyber threat to Canada's upcoming federal election," *The Record.com*, 23 April 2019. Online: https://www.therecord.com/news-story/9298715-minister-assesses-the-cyber-threat-to-canada-s-upcoming-federal-election/

[53] *Investing in the Middle Class, Budget 2019,* House of Commons, 19 March 2019 https://www.budget.gc.ca/2019/docs/plan/budget-2019-en.pdf See also Howard Solomon, "Federal Budget 2019: more money for cyber security," *IT World Canada*, 19 March 2019 https://www.itworldcanada.com/article/federal-budget-2019-more-money-for-cyber-security/416155

significant steps to address so-called hybrid challenges. Hybrid warfare complicates the traditional logic of deterrence and there are many controversies for military and non-military responses that need to be carefully thought through. How Canada and NATO interpret what is happening today as major transformations, and the language of "hybrid war" that they adopt, matter because they guide responses. Russia's actions were widely understood as part of a "wake up call" – a realization that Western adversaries are taking actions, often below the level of conventional wars, in areas that have not yet been constrained by international law and institutions. The result has been more about implementing what is possible in response to an understanding of an evolving context of threats, rather than a comprehensive strategy aimed at peace or the root causes of the conflict. Hybrid threats are now being framed as local, global and transnational problems, which has both advantages and possible dangers.

NATO counters hybrid warfare globally as part of its collective defence and cooperates on strengthening member states' domestic security and societal and institutional resilience. In line with NATO, Canada's defence policy also addresses hybrid warfare and Canada has adopted similar rhetoric and a wide range of military, and increasingly civilian, responses to various hybrid threats, both at the international and, most recently, at the domestic level. Domestic security ministries are being enhanced in relation to hybrid threats, while ministries of defence and foreign affairs are becoming part of a broader "whole-of government" effort. Canada has become more internally focused (deterrence as resilience) adopting a "whole of government" and increasingly "whole of society" approach, while at the same time taking more offensive actions (deterrence by punishment, eg in diplomatic and political realms) and developing multinational partnerships (NATO, G7, EU) and capabilities. Yet more clarity is needed in how we combine all responses. While each "threat" is unique, a more strategic approach would provide more clarity of purpose. What exactly should be the responsibilities of civilian, government and armed forces? What combination of non-kinetic preventative and proactive measures will deter aggressors or pre-empt challenges or attacks? Can vulnerabilities be identified and prevented such that adversaries know they "can't get away with it?"[54] (deterrence by denial) and when and how should we take further action (deterrence by punishment)?

Some responses may pose dangers for liberal states like Canada entering into new hybrid wars that have no end. However, a nonresponse entails a certain amount of risk. While it may not be possible to come to any easy consensus, it is important that we have a public conversation about these dilemmas. "Security" is in the process of being reframed, our understanding of the nature of war and peace is evolving. Yet, there is still no obvious strategy or path in response.

[54] Patrick Cullen, "Hybrid threats as a new wicked problem; for early warning," *Strategy Analysis*, The European Centre of Excellence for Countering Hybrid Threats, May 2018. Online: https://www.hybridcoe.fi/wp-content/uploads/2018/06/Strategic-Analysis-2018-5-Cullen.pdf