Winner of the 2021 CNMT Essay Competition

Winning the Narrative Battle on the High Seas: A Warning for the RCN

Christopher Verklan

Credit: Anto Holoborodko, Wikimedia Commons

'Little Green Men' are pictured at the Perevalne military base during the occupation of Crimea and the city of Sevastopol by Russian troops in 2014.

The modern strategic landscape is becoming one in which traditional binaries such as friend-foe and war-peace have become increasingly convoluted and blurred. The result of this has been the expansion, notably in the West, of the conception of warfare and, with it, the domains in which states now contest and fight. One such domain of increased importance is the information environment, which encompasses "the information itself, the individuals, organizations and systems that receive, process and convey the information, and the cognitive, virtual, and physical space in which this occurs."[1]

Although a topic for debate in the aftermath of the Gulf War during the 1990s, the use of information as an independent tool of state power gained notoriety in the 2010s. This notoriety was in large part due to Russia's use of information in the annexation of Crimea, where it employed a range of media outlets and online resources against Ukraine to legitimize Russian actions and generate distrust of the Ukrainian government.[2] Russia, however, is not alone in its use of information as a tool of state power. In 2015, China's People's Liberation Army (PLA) introduced the Strategic Support Force that has formed the backbone of China's information warfare effort that has targeted Taiwan, among others, in recent years.[3]

The increased use of information operations, notably those targeting the cognitive understanding of an individual or collective, is a concerning – albeit not new – development that will only increase as the competition among China, Russia and the United States intensifies. This is particularly true in the maritime domain, where these three states have competing views regarding the status of the South China Sea and the Northern Sea Route, among other areas. As a member of the North Atlantic Treaty Organization (NATO), a stalwart ally of the United States and a state with maritime interests in the North Atlantic and the South China Sea, the Royal Canadian Navy (RCN) needs to begin considering how the information domain can benefit or harm its objectives at home and abroad.

Unfortunately, the intersection of information warfare and the maritime domain remains under-researched, particularly in a Canadian context. This article aims to rectify this oversight by examining the Black Sea incident that took place in June 2021 between the United Kingdom and Russia and exploring Canada's understanding of, as well as practices in, the information domain. The main finding of this research is that the RCN is ill-prepared to operate in this arena and needs to begin adapting its forces by improving its strategic communications efforts in the short term, and developing new doctrines, force structure and capabilities in the mid- to long term.

The Black Sea Incident

To ground this discussion of information warfare at sea, it is best to begin by reviewing a real-life case. The incident between the United Kingdom and Russia in the Black Sea in June 2021 serves as a representative case from which general insights can be drawn.

The beginnings of the incident can be traced back to March and April 2021, when tensions between NATO and Russia were on the rise due to Russia's massing of military forces along its border with Ukraine in preparation for military exercises.[4] The build-up quickly led to concerns expressed by Ukraine, the European Union and the United States about the possibility of Russian aggression against Ukraine or the inadvertent escalation of the ongoing conflict in the country. These fears, however, proved to be unfounded as Russia did not escalate the conflict using its armed forces or those of its proxies in any meaningful way. Despite this, tensions continued to persist in part due to uncertainty regarding the number of troops and equipment that would remain in the area following the completion of the exercises.

The tensions, and the uncertainty regarding troop and equipment movements, necessitated a Western response to demonstrate solidarity with Ukraine. Aside from supportive rhetoric given by the G7 and NATO members, a notable way that this was done was by using naval diplomacy. The first indications of this came from the United States, which according to reports, planned on sending two warships into the Black Sea in a show of support for Ukraine and to monitor the Russian exercises taking place in the area.[5] This plan was later discarded to prevent escalating tensions with Russia. Instead, the United Kingdom sent two warships shortly thereafter, ostensibly as part of the Royal Navy's (RN) preplanned missions into the Black Sea.[6]

Regional tensions decreased slightly in the weeks that followed, and a joint Russia-US summit in Switzerland was held in June to discuss the conflict in Ukraine, among other aspects of their bilateral relationship. However, shortly after the summit, events in the Black Sea began to deteriorate once again. The first signs of this came on 18 June when automatic identification system (AIS) signals for HMS *Defender* and HNLMS *Evertsen* were spoofed to show that they had sailed to within two miles of Sevastopol in Crimea.[7] While the AIS tracks were quickly proven to be false by open-source researchers, the intent, aims and actors responsible for this incident remain unknown.[8] Interestingly, just one week later – on 23 and 24 June, respectively – these same ships transited through Ukrainian territorial waters around the southern tip of Crimea. In both instances, Russia responded aggressively to what it claimed were incursions by foreign warships in its own territorial waters – using both air and naval forces to threaten and intimidate the transiting warships.[9]

The militarized reaction to the transiting warships is not surprising given Russia's regular use, notably of its aircraft, to harass NATO ships operating in the Black Sea. What is unique, however, is Russia's use of information in the days and weeks that followed in both English-language

Credit: LPhot Dan Rosenbaum, HMS ***Defender***

HNLMS ***Evertsen****, HMS* ***Defender*** *and USS* ***Laboon*** *sail together in the Black Sea on 17 June 2021.*

Table 1. Narratives pushed by various Russian news outlets about the UK following the Black Sea incident, classified by similarity.

Interfax (Russian-language)	RT (English-language)	Tass (English-language)
The passage of HMS *Defender* was an unprecedented, dangerous provocation.	The passage of HMS *Defender* was an unwarranted, unnecessary, counterproductive and irrational action.	-
The actions undertaken by the UK were contradictory to international law.	The actions undertaken by the UK were contradictory to international law (UNCLOS) and norms.	The UK's actions were designed to be provocative, and increase revanchist sentiment in Ukraine.
NATO's activities in the Black Sea are provocative, and anti-Russian in nature.	NATO's activities in the Black Sea are aggressive, increase revanchist sentiment in Ukraine, and prevent real issues from being addressed.	The actions undertaken by the UK could have led to inadvertent escalation.
The Russian Federation's borders are inviolable, and military force will be used to defend them.	More severe consequences will be imposed by Russia in the future, should a similar action occur again.	Russia will choose to escalate should a similar action occur again.
-	-	The actions undertaken by the UK would not have occurred without approval, direction from the United States.

Credit: Provided by Author

and Russian-language news outlets. Focusing on the case of HMS *Defender*, several narratives can be seen in the coverage that followed, as noted in Table 1.

Although the narratives surrounding the events have their differences, all three outlets promoted the Kremlin's core messaging, namely that: (1) the UK's actions in the Black Sea were provocative and uncalled for; (2) the UK's actions were contradictory to international law; and (3) such actions will lead to a stronger military response from Russia in the future. In doing so, Russia was able to advance the idea of itself as a victim of aggressive Western actions, undermine the UK's narrative that was predicated upon the right of innocent passage, and create a narrative to support its deterrent efforts in the region. Equally as important is that the messaging noted here is consistent with previous narratives advanced by the Kremlin such as NATO being an aggressive entity and Ukraine being a revanchist actor.

At a more granular level, these narratives were largely, though not entirely, based on statements from various Russian government officials. However, academics sympathetic to the Russian government's narratives were also used. For example, in an article published by *RT*, a Russian state-sponsored media outlet, a professor at the University of Ottawa concluded that:

> sending signals by military means is a dangerous game, and best avoided. Sadly, it seems that in the UK, moral posturing takes precedence over sound strategic planning. Crimea is a long way from Britain. There's absolutely no need for British ships to be there, and in the long term, this action is unlikely to work to London's advantage.[10]

In addition to these efforts, audio-visual elements and leaked documents were used to delegitimize the UK's version of events, bolster Russia's narratives and justify Russia's actions.[11]

In contrast, the narrative of events communicated by the UK government largely followed the statement made by the Secretary of State for Defence Ben Wallace on 24 June, and corroborated by two journalists aboard HMS *Defender*.[12] Overall, this account stated that: (1) HMS *Defender* conducted an innocent passage through Ukrainian waters in accordance with international maritime law; (2) the actions of HMS *Defender*'s crew were courteous and professional, as compared to Russian units whose actions were at times neither safe or professional; and (3) Russia's claims of warning shots being fired and bombs being dropped in the path of HMS *Defender* were false.[13]

Information Warfare at Sea: Considerations for the RCN

At a superficial level, Russia's efforts in the information domain in the case highlighted above forced the UK as well as the United States to respond in kind. However, beyond this, the case also highlights the need for a deeper understanding of how information warfare may be utilized to affect the perception of events that transpire at sea. For instance, how might the information domain be used to shape the area of operations prior to or following the operations themselves? How might information be used to benefit or harm domestic and international operations? Unfortunately for Canada, these questions have yet to be answered in a meaningful way by either the Canadian Armed Forces (CAF) or the RCN.

The primary reason for this appears to be a lack of attention and the slow pace at which large institutions such as

Credit: LPhot Dan Rosenbaum, HMS **Defender**

*HMS **Defender**, USS **Laboon** and HNLMS **Evertsen** in the Black Sea on 17 June 2021. A Russian **Project 22160**-class corvette watches in the background.*

the CAF and the RCN are able to implement change. For example, Canada's 2017 defence policy *Strong, Secure, Engaged* (SSE) briefly acknowledges the growing importance of grey zone warfare and the threats posed by information in this type of warfare.[14] It also highlights that improved information operations, including military-specific information operations, will be developed going forward.[15] Yet it is unclear based on public documents what, if any, progress has been made – with the CAF likely still relying on part-time reservists to provide a full-time capability.

The *Pan-Domain Force Employment Concept*, which aims to modernize the CAF's approach to competing with and fighting Canada's adversaries, also recognizes the importance of the information domain. Notably, it explicitly states that:

> The information domain has become the decisive domain in contemporary operations. Its centrality stems from the fact that actions in other domains inevitably have impacts in the information domain. Examples include both the transit of RCN vessels through international waters in the South and East China Seas, and *Op REASSURANCE* in Latvia, which use actions in the maritime and land domains to achieve effects in the information domain.[16]

However, much like SSE, it does not prescribe specific actions for the CAF to undertake, despite providing a foundation for Canada's new approach to warfighting.

The lack of strategy and policy documents to guide the CAF, and the RCN, is not without consequences. A prime example of this can be seen in the Canadian army's effort as part of *Operation Reassurance*, in which Canada serves as the framework state for NATO's Enhanced Forward Presence (eFP) mission in Latvia. Here, Russia has become increasingly active in the information space, promoting narratives that undercut the Canadian army's credibility and portray NATO as an aggressive actor. In response to these narratives, a strategic communications cell was established to monitor the information environment and coordinate information operations. Aside from gaining and maintaining situational awareness in the information domain, this new cell has enabled the eFP to craft targeted outreach efforts to specific communities and regions and uncover signals in the information environment that could signal escalatory efforts by the Russians.[17]

Despite these successes, this effort has been hampered by several challenges, including: a reliance on other branches of government and third parties for data; a lack of program-specific funding; a lack of support from headquarters in Canada; and difficulties in integrating strategic objectives with the conventionally focused planning at the eFP headquarters. Taken as a whole, this has led to bureaucratic inefficiency and a degree of improvisation on the ground that has reduced the unity of effort and capabilities in this domain.[18] To put this in more tangible terms, several years after the formation of the strategic communication cell, there are "no translators or cultural advisors attached to the cell. Cell members must use Google Translate to search online sources for Latvian- or Russian-language news articles, or simply to gather basic information about Latvian communities or individuals."[19] This, naturally, is problematic given that knowing the language and culture of those with whom you are trying to communicate is essential to being able to accomplish information operations.

Although occurring on land rather than at sea, this example illustrates that the approach to the information domain is insufficient to meet the challenges of tomorrow. This, in turn, imposes costs on Canadian forces across all domains at the operational and strategic levels. For instance, without a successful military operation being

(Credit: Sgt Juan Camacho enhanced Forward [illegible] Imagery Technician, Ejército de Tierra

A Transfer of Command Authority parade takes place for the enhanced Forward Presence Battle Group Latvia, at Camp Adazi training area in Latvia, 22 January 2021.

translated to the information domain, adversaries can create wedges in domestic politics regarding the success of military forces on a given operation. Similarly, at the strategic level, adversaries could use information to delegitimize Canadian forces and their mission in the area – thereby undermining the strategy of Canada and its allies in a given area of operations.

This reality is particularly concerning as the strategic competition(s) between NATO and Russia, and China and the United States will likely have strong maritime and informational components. In the case of Russia, as evidenced above, the strong information and maritime focus is visible in its approach to the Black Sea. It can also be seen to some extent in the Arctic, where Russia has repeatedly called for the region to be a "zone of peace"[20] despite building up its military forces in the region. Similarly, China has also crafted a strong domestic narrative surrounding the status of the South China Sea and has begun to legitimize its efforts in the Arctic by declaring itself a 'near-Arctic state.'

China's efforts in the information domain have recently affected Canada directly, with one Chinese-affiliated media outlet claiming in September 2021 that a Chinese sailor circumnavigating the Arctic was "illegally stopped" while transiting the Northwest Passage.[21] Canada has since denied that the vessel entered Canadian waters and stated that Transport Canada had informed the vessel's captain that the passage was closed to pleasure craft due to COVID-19.[22] The true intention behind this incident remains unclear, especially given the captain's ties to the Chinese government and his past support of China's maritime endeavours, including contesting waters in the East China Sea. However, it is likely that the voyage was an attempt to shape the information landscape to legitimize China's position as an Arctic actor and "write itself into the Arctic's history."[23]

This type of activity will only grow in the future as tensions continue to rise and as new disruptive technologies are utilized to enable larger and more targeted information operations to take place. Yet even without considering future trends in information warfare, the RCN needs to rethink its approach to the information domain to meet current challenges. Its approach should have the goal of achieving narrative dominance – i.e., ensuring that its narrative is the dominant one for the contested issue. In the short term, this requires that the RCN adopt ways to mitigate attempts by hostile actors to influence the domestic information environment by promoting resilience, engaging in shaping efforts and contesting hostile narratives (as, for example, was done by the CAF during the early stage of *Operation Laser*, the CAF response to the COVID-19 pandemic[24]).

While this approach can be proactive or reactive, there is room to improve the transparency, timeliness and reach of the RCN's current strategic communications. Some recommendations include:

1. Increasing the rapidity at which information is communicated to the public across all media platforms, with the goal of generating more timely and cohesive messaging.[25]
2. Increasing the transparency of the operations of Canadian ships by providing more frequent updates regarding transits and activities, beyond what is done by the monthly "Your Navy Today" operation updates.
3. Broadening the reach and accessibility of the RCN's communications by creating targeted communications for under-exposed demographics, and by legitimizing the RCN's actions by justifying their importance and rationale in basic terms that accord with Canadian beliefs and identity.

In the medium to long term, the RCN's efforts should move beyond denying hostile actors an uncontested permissive environment, and instead focus on developing a more agile strategic communications and information warfare force that is designed to generate influence and maintain narrative dominance abroad. To do so will require the RCN to:

1. Develop clear strategies and policies on information warfare in conjunction with the CAF that will enable the RCN to develop and adopt the relevant tactics, techniques and procedures to accomplish the goals identified by political guidance.
2. Develop an agile force structure that is capable of rapid and decentralized decision-making, with

Credit: Corporal Lynette Ai Dang, Canadian Armed Forces

*Water spouts appear as HMCS **Calgary** transits the Strait of Malacca during **Operation Projection** on 27 June 2021. China has regularly painted Western naval activity as illegal and aggressive.*

Credit: Corporal Simon Arcand, Canadian Armed Forces

*HMCS **Goose Bay**, HMCS **Harry DeWolf** and CCGS **Pierre Radisson** sail through Frobisher Bay during **Operation Nanook-Tuugaalik**, 11 August 2021. CCGS **Terry Fox** was also a participant.*

the goal of being able to develop a strategic communications force with the capability to operate and maintain narrative dominance in contested and fast-changing information environments.

3. Develop domain awareness in the information domain in areas of interest, possibly in cooperation with allies and partners, with the goal of identifying, countering and exploiting flaws in hostile narratives (particularly in local languages) in a way that is consistent with government messaging.

Although not an exhaustive or complete list, these proposed changes provide the basis from which the RCN can begin to utilize the information environment to advance its operational and strategic objectives. These efforts, of course, will take time and consideration of applicable laws, norms and operational security requirements but should nevertheless be pursued given the advantages that the domain brings to modern warfighting.

Conclusion

The increasing importance of the information domain has created new opportunities and vulnerabilities for the CAF to address. This is particularly true in the case of the RCN as the strategic competition with both China and Russia, in conjunction with non-state actors, will have strong maritime and informational elements. The RCN is currently ill-prepared to meet these challenges and must adapt to operate in the information domain to meet the challenges created by the blurring boundaries of warfare in the grey zone. The importance of adapting the practices of the RCN to encompass the information domain cannot be under-stated given the importance of this domain in conflicts that occur below the threshold of armed violence. The June 2021 incident in the Black Sea is emblematic of this fact, and marks a bellwether event the ramifications of which should not be ignored.

Notes

1. North Atlantic Treaty Organization, "NATO Military Policy for Information Operations, Draft MC 0422/6," 11 September 2018, p. 3.
2. Michael Kofman, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, Jenny Oberholtzer, "Lessons from Russia's Operations in Crimea and Eastern Ukraine," RAND Corporation, 9 May 2017, p. 14.
3. Nathan Beauchamp-Mustafaga, "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations," The Jamestown Foundation, 6 September 2019.
4. Rob Lee, "Russia's Coercive Diplomacy: Why Did the Kremlin Mass its Forces Near Ukraine this Spring?" Foreign Policy Research Institute, 23 August 2021, pp. 1-3.
5. Barbara Staarr and Jennifer Hansler, "US Considering Sending Warships to Black Sea amid Russia-Ukraine Tensions," CNN, 9 April 2021.
6. Tim Ripley, "British Warships Head for Black Sea as Russian Troops Mass on Ukrainian Border," *The Times*, 18 April 2021.
7. H.I. Sutton, "Positions of Two NATO Ships were Falsified Near Russian Black Sea Naval Base," *USNI News*, 21 June 2021.
8. Given its recent GPS jamming and spoofing activities, one possibility is that Russia was the actor behind this event, though it is unclear what the intent would be. See Henrik Lied and Martin Gundersen, "Norske Marineskip ble Manipulert inn i Russisk Farvann," *NRK*, 25 September 2021.
9. "HMS Defender: Russia's Putin Accuses UK and US Military of Military Provocation," BBC, 30 June 2021.
10. See Paul Robinson, "Britannia Fools the Waves: UK Sent Clear Signal to Moscow with Warship in Crimean Waters… Just Probably Not the One it Intended," *RT*, 24 June 2021.
11. For example, see "Russia Releases Video of British Warship's Incursion into Waters near Crimea, Clearly Contradicting London's Version of Events," *RT*, 24 June 2021.
12. See "HMS Defender: Russian Jets and Ships Shadow British Warship," BBC, 23 June 2021; "BBC Journalist Reports from British Warship as Russia 'Fires Warning Shots,'" BBC, 23 June 2021; Mark Nicol, "Russian Jets Thunder Overhead. […] Eyewitness Report as Vladimir Putin's Gunboat Opens Fire on HMS Defender," *Daily Mail*, 24 June 2021.
13. UK Parliamentary Hansard, "Exercises in the Black Sea," 24 June 2021.
14. Canada, Department of National Defence, *Strong, Secure, Engaged: Canada's Defence Policy* (Ottawa, ON: National Defence, 2017), pp. 41, 68-9.
15. *Ibid*., pp. 41, 68-9.
16. Canada, Department of National Defence, *Pan-Domain Force Employment Concept: Prevailing in an Uncertain World* (Ottawa, ON: National Defence, 2020), p. 16.
17. Chris Wattie, "Bringing a Knife to a Gunfight: Canadian Strategic Communications and Information Operations in Latvia, Operation Reassurance 2019-2020," *Canadian Military Journal*, Vol. 21, No. 1 (2021), pp. 57-59.
18. *Ibid*., pp. 59-61.
19. *Ibid*., p. 60.
20. Kristian Atland, "Mikhail Gorbachev, the Murmansk Initiative, and the Desecuritization of Interstate Relations in the Arctic," *Cooperation and Conflict*, Vol. 43, No. 3 (2008), p. 290.
21. Xu Fanyi, "Canada Stops Chinese Sailboat to Finish Circumnavigate the Arctic," *CGTN*, 16 September 2021.
22. John Last, "Canada Disputes Chinese News Report that Famous Sailor was Turned Back from Northwest Passage," CBC, 17 September 2021.
23. *Ibid*.
24. Suzanne Waldman and Major Marshall Erickson, "Strategic Communication in the Present and Future Military Enterprise," *Journal of Future Conflict*, Defence Research and Development Canada (DRDC), Issue 2 (Fall 2020), p. 7.
25. An example of this can be seen with the seizure of 1,200 kg of cocaine on 8 November 2021 following which it took the RCN's Instagram and Twitter pages 13 days to communicate the seizure to the public, and over three weeks for it to be acknowledged on its official website.

Christopher Verklan is a Master's candidate at the University of Calgary, pursuing a degree in Strategic Studies. Previously, Christopher was a Voluntary National Contribution at the NATO Defense College.