Logically.

Understanding Russia's Information Confrontation Tactics

Analysis for potential implications for New Zealand

Disclaimers

This report was prepared independently by Logically. The report represents the assessments of the authors and does not represent the views of the Department of the Prime Minister and Cabinet. Content derived from posts online represents the views of the content originator, including sensitive or hateful material, and does not represent the views of the client or Logically. Personally identifiable information has been removed at the request of the Department of the Prime Minister and Cabinet.

Executive summary

Among noted state MDM actors, the Russian government has the longest legacy of effectively using disinformation. It is arguably the most capable MDM actor in the autocratic world and the most proficient at leveraging MDM to promote its foreign policy agenda. Over many years, Russia has demonstrated its significant capabilities in conducting hybrid threats, covering cyber threats, hack-and-leaks, coercion, espionage, economic pressure, and traditional military activity. A key component of Russia's hybrid approach is online information campaigns and the spread of disinformation and foreign information manipulation and information (FIMI). These covert online campaigns aim to shape public perception, manipulate opinion, and undermine strategic adversaries across political, economic, and military spheres.

The case studies outlined in this report cover Burkina Faso, Ukraine and Canada, demonstrating the global nature of Russia's information campaigns. The case of Burkina Faso provides an example of the destabilising impact of wide-ranging Russia MDM activities; Ukraine's case study exemplifies how Russia's ability to implement a sophisticated and sustained disinformation campaign over a decade; and Canada's case study highlights how Russia combines information operations with coordinated cyber-attacks, primarily with the intention of undermining democratic institutions and critical infrastructure.

There are a number of common tactics, techniques and procedures (TTPs) across these case studies, including Coordinated Inauthentic Behaviour (CIB) bots, "spamouflage" (the term for flooding social media platforms with content), and embedding links to biased or misleading content within seemingly trustworthy articles or social media posts. These TTPs also have a notable impact on the online media and news outlets. These tactics include 'pink slime journalism' (a deceptive practice involving creating fake local news websites that serve as propaganda tools) and 'information laundering', whereby disinformation narratives are disseminated through recognized and traditional media outlets.

These case studies highlight the global nature of Russia's information campaigns, and illustrate how tailored and localised disinformation threats can be, with narratives sowed in each country specifically intended to resonate with their intended audiences. These disinformation narratives cover themes related to military strength, historical revisionism, anti-Western, and anti-democracy.

New Zealand is not currently a target for Russia state-backed FIMI and MDM campaigns. However, against the backdrop of Russia's increasingly sophisticated campaigns against its adversaries globally, it is essential to be aware of Russia's playbook and the potential implications this could have on New Zealand's information environment. By understanding both Russia's information confrontation tactics and the likely vulnerabilities in New Zealand's online ecosystem, New Zealand and its allies can better identify, anticipate, and respond to any emerging and future threats.

Logically identified vulnerabilities specific to New Zealand's online and media ecosystem that could be exploited by Russia, based on the hostile state's previous and existing FIMI campaigns. Logically assesses these narratives would likely target New Zealand's geopolitical aims, social cohesion, and elections. The relatively strong state of national social cohesion and democratic processes in New Zealand would indicate if Moscow took this tack, it would have to augment its activities in order for them to be effective. Given Russia's approach to hybrid online threats, this would likely cover cyber operations, hacking, and campaigns to undermine New Zealand's media landscape, alongside legitimate activities including cultural diplomacy.

Glossary

Coordinated Inauthentic Behavior (CIB)
The organised use of fake accounts and networks to manipulate public discourse.

Disinformation
False or misleading information that is deliberately spread to manipulate a person, social group, organisation, or country.

Foreign Information Manipulation and Interference (FIMI)
Information manipulation to include MDM activities executed through a planned effort by a foreign state designed to "influence, disrupt or subvert New Zealand's national interests by deceptive, corruptive or coercive means."

Information Confrontation
The Russia government's approach to the weaponisation of information related capabilities to target adversaries and advance its geopolitical interests. Generally perceived to consist of disinformation, social media manipulation, state media control or influence, cyber activities, and covert or clandestine operations.

Malinformation
Factual information that is taken out of context to mislead, harm, or manipulate.

Misinformation
False or misleading information that has not been created or shared to cause harm

MDM
Misinformation, disinformation, and malinformation.

Tactics, Techniques, and Procedures (TTPs)
Influence methods and strategies used by adversaries, particularly in the context of cybersecurity and information warfare (MDM, FIMI, CIB), to achieve their objectives.

Background

The Russia government exploits information confrontation and FIMI as one of its most essential weapons. The use of misinformation, disinformation, and malinformation (MDM) enhances its ability to indirectly attack or subvert its adversaries. These narratives aim to advance Russia's national security, political, and economic goals, including devaluing Western institutions and the international rules-based order and sowing discord as an element of subversive foreign policy.

The roots of Russia disinformation strategies can be traced back to the Soviet era, during which multiple organs of the state and communist party used "active measures" to influence global public opinion or destabilise Western and capitalist adversaries. Present-day Russia under the autocratic control of Vladimir Putin has revitalised and adapted the use of the information environment to meet Moscow's domestic and international goals. Within this context, Russia's government has adapted its legacy information confrontation

capabilities and enhanced them with digital and information age technologies to enhance and magnify the impacts of its disinformation campaigns.

Despite global criticism for its FIMI activities, Russia persists in operating against international norms. Its strategies combine overt state-controlled media with covert tactics to promote harmful and false narratives that serve its strategic goals. Russia targets social, political, economic, and security vulnerabilities to expand its influence. This approach is reminiscent of the Soviet era, as evidenced by its activities in the Middle East, Africa, and Latin America. Concurrently, Russia seeks to weaken Western alliances such as NATO and the European Union, attempting to erode collective resistance against its strategic pursuits.

Advancements in technology, particularly in artificial intelligence (AI) and social media analytics, have enhanced Russia's ability to conduct sophisticated MDM campaigns. AI-driven bots generate and spread content at an unprecedented scale, creating the illusion of widespread consensus or dissent. Machine learning algorithms analyse social media trends to identify the most effective narratives to push, ensuring MDM campaigns are highly targeted and impactful. Similarly, Russia's intelligence agencies are among the world's most capable cyber actors, providing Moscow the ability to combine cyber and MDM activities. This combination has been prevalent in most of the recent Russia state-directed major MDM activities. They have been a major factor in the advancement of Russia government interests over those of Western states and institutions aligned with Western values, such as NATO, the European Union, and the Five Eyes Alliance. These institutions often promote democratic values, human rights, and market economies, which can be at odds with Russia's strategic goals.

Russia's strategic narratives often depict Western governments as corrupt and hypocritical while emphasising Russia's supposed moral and cultural superiority. These narratives attempt to undermine Western criticism of Russia by framing it as baseless and politically motivated. Moreover, Russia promotes conspiracy theories to foster discord and distrust in Western institutions. These narratives are disseminated using various techniques, including dismissing criticism, distorting facts, distracting from important issues, and using negative framing. State-controlled media, social media bots, and coordinated inauthentic behaviour (CIB) are employed to amplify these messages to a global audience. For example, Russia's media played a role in spreading disinformation during the Brexit campaign to destabilise the EU, showcasing the effectiveness of these techniques.

The intent of this report is to analyse the historic and recent use of Russia government and proxy MDM, cyber, and broader information confrontation strategies to conceptualise under what conditions and through what mechanisms Moscow might direct a larger campaign targeting New Zealand. To make this case, the report is broken into four sections. First, Logically selected three case studies - Burkina Faso, Ukraine, and Canada - to highlight the potential threat of Russia MDM against New Zealand, based on the tried-and-tested Kremlin playbook of hybrid threats and information operations. Each case study provides a summary of the issue, an overview of MDM tactics employed, including narrative elements, an assessment of the impact of the MDM, and an identification of the implications of the effort on both the targeted country and New Zealand. Second, Logically applies the lessons from these case studies within potential usage if levied against New Zealand. Third, Russia's social media and dissemination strategies are also highlighted. In the final section, Russia's approach to information confrontation and MDM dissemination is applied against constructed localised New Zealand vulnerabilities. The intention of this section is to assist in the conceptualization of the potential threat the most likely targets, and support ideation on potential limitation and mitigation strategies.

Methodology

This report frames MDM activity within the broader context of hybrid TTPs, collectively constituting FIMI. It is important to recognize that the report examines Russia's hybrid warfare TTPs broadly because MDM does not occur in isolation, and FIMI encompasses a much wider set of interventions. However, the report aims to clearly distinguish between legitimate and illegitimate components of these activities. For example, cultural diplomacy can be a legitimate activity, but it becomes problematic when integrated into or used alongside illegitimate hybrid warfare TTPs like MDM.

The report is a summary of the extensive collection and analysis of Russia government and proxy MDM activities by the Logically team. It uses extensive in-house and external subject matter expertise on Russia's history, military activities, intelligence and security agencies, current and historic MDM and information confrontation activities, and international security expertise. Africa security experts were consulted for the Burkina Faso case study, and government and military intelligence professionals were consulted for the Ukraine and Canada case studies.

As a summary report, this document does not cite every unique analysis and report within the broader scope of Russia MDM activities. Instead, it provides a synthesised overview of key findings and trends, supported by targeted references to specific incidents and authoritative sources. This approach allows for a cohesive and accessible presentation of the complex landscape of Russian influence operations.

Summary of Russian TTPs

Russia leverages advanced social media strategies globally to influence public opinion and manipulate perceptions of governments, populations, institutions, and groups. Through social media, Russia can swiftly and effectively reach a wide audience, shape and reinforce narratives, and amplify the impacts and effects of its greater geopolitical objectives. To complement Russia's overt propaganda through news outlets like Sputnik and RT, there are a number of covert means through which it disseminates MDM campaigns:

'Spamouflage' and CIB

One tactic known as 'spamouflage' floods social media platforms with content supporting pro-Russian government narratives or that undermines opposing viewpoints. For example, this could involve overwhelming platforms in New Zealand with posts criticising the country's participation in international alliances like Five Eyes or AUKUS. Spamouflage attempts to create an artifice of widespread agreement or dissent on a specific issue or event to give the false impression of solvency or unanimity. In so doing, users and populations are denied access to contradictory information and lead to believe a majority agrees with the information purported within the spamouflage barrage. This approach almost certainly includes various aspects of CIB including fake accounts and bots. Often multiple CIB vectors are used to dynamically and repeatedly expand reach and engagement on the issue. Recent Russian government and proxy activities have indicated the potential of AI incorporation into these CIB efforts.

Information laundering

Russia government and proxy MDM actors have improved their abilities to disseminate narratives through recognized and traditional media outlets. Co-opting these news sources enables widespread reach with an increased perception of veracity related to the MDM narratives and themes. These activities can occur in the open or through cyber intrusion. Russia MDM actors have also established aggregator networks that pose as

legitimate media outlets but in reality, promote Russia-centric MDM narratives. Aggregator networks are generally linked to CIB activities as a means to further enhance the perception of legitimacy through reach. Often, multiple aggregator networks cross reference one another's narrative promotion to give the further guise of corroborating information. Within the current Ukraine invasion, Russian aggregator networks have become so adept, that their fabricated narratives have been picked up by legitimate news agencies, as occurred in June 2024 related to Russia government activities targeting the Paris Olympics.[1]

'Pink slime' journalism [2]

This is a deceptive practice involving creating fake local news websites that serve as propaganda tools for the advancement of Russia MDM narratives. These sites publish content with the aim of manipulating public opinion and often hide their funding sources and affiliations. In New Zealand, 'pink slime' journalism could be used to disseminate articles that criticise the government or push pro-Russia narratives, adding to the confusion in public discourse. As pink slime journalism tactics have improved, it has become increasingly challenging for users to detect illegitimate reporting as many of these sites promote actual relevant news.

Concealed links

This is another method used by pro-Russia MDM actors to spread false information. This tactic involves embedding links to biased or misleading content within seemingly trustworthy articles or social media posts. Readers may unwittingly click on these links, leading them to propaganda sites that subtly influence their views. In New Zealand, concealed links could be used to redirect users from popular social media platforms to sites promoting pro-Russian narratives or undermining trust in the government.

Exploiting domestic threat actors

Another common tactic employed by the threat actors is seeding disinformation narratives through local politicians and influencers (often accepting bribes or having financial ties to Russia). By disguising the source of the narratives, they have the appearance of being credible, organic and grassroots narratives from local and trusted sources. These narratives are then often amplified and exploited through state-backed propaganda and overt channels and networks, to further the reach of these narratives.

Information Confrontation Case Studies

The following specific case studies illustrate the multifaceted nature of Russian influence activities and the TTPs set out above. These examples highlight the strategies and impact of the Russia government-sponsored MDM, FIMI, and CIB campaigns as they influence the information ecosystem across different regions, providing insights into the effectiveness of Russian tactics and their broader geopolitical objectives.

[1] Catalina Marchant de Abreu, "*Russian Influence Campaign Targets Paris Olympics Using Fake Tom Cruise Documentary,*" France 24, April 2024.
[2] Priyanjana Bengani. "*Hundreds of 'Pink Slime' Local News Outlets are Distributing Algorithmic Stories and Conservative Talking Points,*" Columbia Journalism Review, December 2019.

Case Study: Burkina Faso

The Russia government has employed a broad spectrum of MDM activities in Burkina Faso as a means to advance its international agenda which has included replacing France as the partner of choice for Ouagadougou. A military coup in 2022 included pro-Russia agitation and affiliation with the Wagner group. By January 2024, Russia military forces were permanently deployed to Burkina Faso to work with the host nation's military to presumably conduct counter terrorist operations. At the same time, positive public opinion toward Russia and negative public opinion regarding France have increased. The new pro-Russia government has ended long-standing military, economic, and political engagements with Paris.

Russia MDM has been a consistent factor in shaping public perceptions at least since the immediate aftermath of the 2022 coup. The overall strategic foci of these MDM campaigns have been to shape positive sentiment toward Russia and negative sentiment toward France by promoting pro-Russia narratives through disinformation and manipulated social media content. Russia MDM has also sought to exacerbate friction points between domestic groups as a means to solidify government control, and has targeted other regional states, such as Ghana, as a means to create external threats to Burkina Faso stability.

Russia has secured its position of influence regarding Burkina Faso, and through that geographical location established a foothold in Western and Sub Saharan Africa from which it, or a proxy organisation such as the Wagner Group, can expand covert or clandestine military and intelligence activities and direct and overt MDM campaigns targeting other states or those states foreign. As a result, the Russian influence within Burkina Faso can be perceived as a net destabilising condition that threatens the region.

Tactics and Implementation

- **Anti-French Sentiment**: Russia capitalised on historical grievances and current frustrations with the French presence in Burkina Faso, portraying France as a neocolonial power to stoke public resentment.[3] Anti-imperialist rhetoric was a hallmark tactic of the Soviet era. It remains one of the principal manipulations of MDM activities used by Russia or its proxies throughout the developing world and global south.
- **Media Manipulation**: Russia operatives used local media and social platforms to disseminate disinformation, creating and amplifying content that portrayed Russia as a more favourable ally compared to Western powers.
- **Militarised Narratives**: Across the spectrum of the information environment, Russian government actors, proxies or affiliates promoted a false optic of global Russia military success. The intent of this information tactic was to alter the perceptions of the population to perceive the Russia military, - and through the military the Russia government, as a reliable partner for domestic and regional security matters - or at least a more reliable partner than the "imperialist" West.[4]
- **Combining cultural diplomacy and disinformation**: Russia government actors, proxies or affiliates used the information environment to build a positive image among Burkinabe citizens by amplifying, often falsely, cultural initiatives and educational programs. In doing so these disinformation efforts attempted to enhance the legitimate engagement by Moscow and its use of soft power approaches

[3] "*Russia flooding Burkina Faso with disinformation*," ADF, February 2024.
[4] Grigor Atanesian, "*Russia in Africa: How disinformation operations target the continent,*" BBC, February 2023.

in the region. Often soft power information narratives were combined with counter narratives regarding Western hard power such as military occupation.[5]

Immediately following the 2022 coup, pro-Russia support was found among demonstrations in favour of the removal of president Damiba. Rumours of Wagner Group involvement in the coup plotting and execution were identified in Western press but absent among most local media. Russian flags were present among demonstrations in support of the coup, highlighting the integration of planning required across the Russian forces and local authorities.[6] If Wagner or other Russia government proxies were indeed involved in the planning and execution of the coup, it is almost certain, they were able to expand their access to information narratives especially domestic media once the pro-Russia government was in place.

By early 2023, pro-Russia social media accounts were engaged in the spreading of MDM narratives related to French military deployments to and operations in Burkina Faso. The French military forces, which has been conducting counter terrorism operations and conducting training with the Burkinabe military since 2014, were accused in these MDM narratives of being an occupation force that was enabling resource and other economic exploitation of Burkina Faso by France. Such narratives found fertile ground among the population that sustained cultural memory of French colonial occupation and management. Given that the real purpose of the approximately 400 French troops was combating islamic militant groups in the Sahel, Russia government MDM efforts attempted to further discredit the French force by stoking claims regarding military failures and supposed support for the militants they were supposed to be fighting.

In addition to profligate claims targeting France and the French military deployment, Russia government disinformation actors and proxies expanded their narratives toward the U.S. claiming Washington was conducting illegal biological testing in Africa. Like imperialism, illegal biological testing has been a standard trope used since the Soviet Union to attack the U.S. and the greater West. The inclusion of this narrative paired with other legacy Soviet Russian disinformation themes strongly indicates centralised management by an agency or multiple agencies in the Russia government to foster a pro-Moscow information environment in Burkina Faso.

As a result of these efforts, social media trends across most platforms used by Burkinabes revealed a corresponding and significant increase in posts, engagement, and other activities promoting anti-French sentiment as well as pro-Russia viewpoints. Social media activity showed clear evidence of the use of bots and fake accounts to seed, spread, and amplify these MDM activities. Notably, local, regional and international journalists and activists identified and reported a notable shift in public opinion within the country toward a rapidly growing distrust of France and acceptance of Russia. Social media and pro-Russia news outlets promoted these false narratives and encouraged engagement in protests and public outcry against the French presence.

Assessment and Implications

The case of Burkina Faso provides an example of the destabilising impact of a massive campaign of Russia MDM activities that rapidly enabled a coup, reduced Western capacity against regional Islamic extremist militancy, and provided Russia a geographically strategic foothold in the Sahel. Moscow's goals for its replacement of France as the strategic partner of choice had little to do with the falsely purported cause of improving counter terrorism effectiveness and broadening security and economic access for the Burkinabe.

[5] Michael R. Gordon, Gabriele Steinhauser, Dustin Volz, and Ann M. Simmons, "*Russian Intelligence Is Pushing False Claims of U.S. Biological Testing in Africa, U.S. Says,*" WSJ, February 2024.
[6] Edward Mcallister, "W*ho is Ibrahim Traore, the soldier behind Burkina Faso's latest coup?,*" Reuters, October 2022.

Rather, Russia seeks to weaken Western influence and establish itself as a dominant power through the establishment of a multipolar world order.

To bring about this turn of events, it is almost certain that Russian government actors or their proxies were engaged with the coup leaders during the early planning of their military seizure of power. Immediately following the coup, these actors or proxies and their local agents immediately expanded the MDM and cognitive influence efforts to secure the position of the pro-Russia coup leaders. MDM efforts increased to manipulate public sentiment against France so that by January 2024, the new government could order the end of France's military mission.

Case Study: Ukraine

The Russia government has been executing a sophisticated and sustained disinformation campaign related to Ukraine since at least 2013 when it began a concerted effort to manipulate the Ukraine domestic political environment to favour Russia claims of sovereignty over territorial areas or large Russian majority population centres within Eastern Ukraine. Over the past decade, Russia Ukraine-focused MDM activities have grown to scale to correspond with expanded Russia strategic desires vis-a-vis territorial control, sovereignty and international relations. As these efforts have expanded, they remain focused on several different audiences, Ukrainian citizens, ethnic Russians within Ukraine, Russian citizens in Russia, and the international community. With these different targeted demographics, Russia, or its proxies and agents, have used adapted messaging narratives to increase reach and resonance among the specified audience.

MDM directed and sponsored by the Russian government can be perceived through four periods within the scope of its belligerence against Ukraine,

1) the illegal occupation of Crimea in 2014,

2) the expansion of the Crimean effort into the Donbas region through ethnic Russian agitation,

3) just prior to and early in the invasion of Ukraine in 2022, and finally

4), the ongoing conflict between Russia military forces and the Ukraine military backed by the West.

Russia MDM efforts have been employed prior to each of these periods to create a notional *casus belli* for military and paramilitary actions. After the initial military activity or occupation, MDM adapts to purport the veracity of the Russia activity, manage control of the occupied territories, and limit international response or interference. The fourth period appears to be enduring, and as such within the scope of MDM, Russia has attempted to prevent Western interference by going as far as invoking the threat of nuclear confrontation, and attempting to build alternative international political associations to sustain its economic, military, and political efforts.

Since 2013, the Russia government and proxy MDM tactics have included spreading false narratives about Ukrainian politics through the labelling of the government as fascist or “Nazi,” claiming its military actions were warranted due to the imminent threat of Western or Ukraine invasion of Russia, providing false historical accounts, and using state-controlled media to disseminate and amplify its breadth of propaganda. Among noted state MDM actors, the Russia government has the longest legacy of effective use of disinformation, is arguably the autocratic world’s most capable MDM actor, and is the most proficient in the use of MDM to promote its foreign policy agenda. All of these tactics and their implications remain a feature of the ongoing war in Ukraine.

Tactics and Implementation

- **Narrative Manipulation:** Russia promotes false narratives about Ukraine's government and its intentions toward Russia. From prior to the occupation of Crimea through the early months of the total invasion, most frequently Ukraine was identified as a "fascist" or "Nazi" entity that was violently oppressing ethnic Russian minorities in Ukraine. Correspondingly, Putin famously claimed in the international press Ukraine was to be used as a staging ground for a NATO invasion of Russia. Since the stalling of the Russia invasion and the flow of Western weapons and intelligence to Ukraine, these narratives have continued to adapt and now promote Ukraine and President Zelensky as hapless puppets of the West and especially the U.S. in their proxy war against Russia.
- **Historical Revisionism:** The Russia government through state (and occasionally international) media has attempted to promote a Putinist version of Russian and Ukrainian history as a means to legitimise its military activities. Within this narrative all Kyivan and Rus culture is centred upon and prioritises Moscow in contrast to the broader historical understanding of Kyivan and Rus cultural development. Russia proxies, agents, and sympathisers are often co-opted or independently seize on these narrative elements for coordinated and supporting amplification.
- **Cyber Operations**: Coordinated cyberattacks and data breaches are used to undermine Ukrainian institutions and disrupt critical infrastructure. In 2023, Russia cyber actors associated with the GRU, such as the group Cadet Blizzard, targeted government agencies and IT service providers in Ukraine. These attacks included the destructive WhisperGate wiper attacks and phishing campaigns designed to steal sensitive information. These operations highlight the integration of cyber capabilities with traditional disinformation efforts to maximise impact.[7] Russian government actors have also employed cyber capabilities as a means to limit counter-MDM efforts.
- **Social Media Influence and FIMI**: Russia government, proxy and affiliated operatives use social media platforms to spread propaganda and disinformation, creating echo chambers that amplify false information. For instance, Russia actors have used Telegram and other platforms to spread false claims about Ukrainian activities and intentions, furthering disinformation campaigns. While there are strong indications of centralised management of social media messaging, the structure of Russia MDM allows for affiliated promoters of disinformation to respond independently within the shared understanding of the strategic intent of their mission.

Russia's approach to the Ukraine crisis can be characterised by a combination of conventional military tactics, cyber warfare, MDM, and other asymmetric methods. This hybrid warfare strategy aims to exploit weaknesses in Ukraine's defences, undermine public trust in the government, and create instability in the country. Since at least 2015, Russia has been combining cyber attacks with MDM strategies to maximise disruptions to social and political order in Ukraine and support its establishment of sovereign control over most parts of the country. The Sandworm Group widely considered to be an element of Russia military intelligence, the GRU or Main Intelligence Directorate/*Glavnoye Razvedyvatelnoye Upravlenie* has been one of the most active cyber groups. Sandworm gained attention for its involvement in the 2015 cyber attack on the Ukraine power grid, the 2017 NotPetya cyber attack targeting business and government agencies that spread globally, and coordinated attacks against government agencies, critical infrastructure, and economic targets in 2022-2023. Each of these attacks also was coupled with and amplified by aggressive MDM activity by Russia government actors and proxies thus highlighting the highly sophisticated and proficient nature of Russia government pairing of cyber and MDM capabilities.

[7] "*A year of Russian hybrid warfare in Ukraine*," Microsoft, March 2023.

In addition to such hybrid approaches, it must also be noted that Russin state or pro-state media has an enhanced role in the development and spread of advanced MDM narratives throughout the decade of Moscow's aggression against Ukraine. Since 2013, Russian media outlets have actively promoted Russia government MDM narratives and attempted to alter international news perspectives or those of non-Russian figures. Much of this information has sought to falsely portray the supposed reasoning for Russia government's military belligerence. Media is also used to spread distrust in the international response to support for Ukraine and attempt to sway global opinions toward Russia. To do so, Russian government actors and their proxies will often work within the media to advance narratives that directly attack the West and specific states supporting Ukraine.

The most prevalent Russian proxy for the use and advancement of MDM with regard to Ukraine has been, and continues to be, the Wagner Group. While Wagner's role in Ukraine has been primarily focused on standard military activities - especially where the Russia military has repeatedly failed - it is also believed to be involved in centralised control of MDM efforts. It is likely the Wagner Group has been and is involved in spreading misinformation and propaganda about Ukraine and the conflict. While the extent to which the Wagner Group is directly involved in executing these campaigns is not definitively known, its close ties to Putin and the Russian Ministry of Defense and involvement in other covert activities strongly suggests it is also involved in most coordinated MDM activities.

Assessment and Implications

The full spectrum of Russia MDM activities remains on display in Ukraine and are integrated into almost every aspect of political engagement by the Russia government on the issue as well as military operations on the ground. So far MDM activities have not sufficiently altered the outcome of the conflict, but as early as late 2023 and early 2024, Russia MDM themes were being promoted by politicians in Western countries threatening military and economic support to Kyiv.[8] Therefore it is almost certain Moscow continues to see the value in MDM - to include its inclusion in hybrid warfare strategies - in the current and any future conflict.

The recent increase in the reflection of pro-Russia rhetoric in the capitals of NATO states and other West-aligned countries almost certainly indicates to Moscow the efficacy of their MDM and cyber campaigns. With major elections in 2024, it is almost certain Russia's efforts will be amplified during key cycles (especially the U.S. Presidential elections) in the hope of reducing or eliminating support to Ukraine - without which it will likely fall to Russia military action resulting in a protracted partisan conflict.

New Zealand has played an active role in the broader Western effort in support of Ukraine through various interventions. It has imposed sanctions, provided both lethal and non-lethal military equipment, enabled NATO lethal aid provision through the RNZAF and logistic deployments, and conducted extensive training of Ukrainian military personnel. Currently, New Zealand is not perceived by Moscow as a major contributing nation to the defence of Ukraine, which is why Russia has not targeted its MDM or hybrid capabilities towards the country. However, it is possible that should New Zealand take new pro-Ukraine actions, such as increasing its support for NATO and other states' weapons shipments to Ukraine, Russia could perceive such actions as a new threat and directly target the country within its MDM campaign or with cyber disruptions.

If this occurred, MDM narratives would likely remain focused on justifying Russia's actions while delegitimizing Ukraine and its supporters. Cyber actions would most likely consist of disruptions to services

[8] Dan De Luce and Syedah Asghar, "*Luxury yachts and other myths: How Republican lawmakers echo Russian propaganda,*" NBC, April 2024.

or government agencies as a way to attract the attention of the population and garner additional support for Russia's version of international events.

Case Study: Canada

Russia's influence operations in Canada demonstrate the effectiveness of its hybrid warfare tactics, which combine disinformation, cyber operations, and cultural manipulation to achieve strategic goals. Russia has exploited various societal and political vulnerabilities within Canada to disrupt democratic processes and create divisions among citizens. These activities have not resulted in fundamental change in Canada's domestic or international policies or social cohesion, but notably, Russia sustains its hybridised approaches to information confrontation.

Presently, Russia is engaged in at least five areas of engagement in the information environment targeting Canada:

1. Russia government actors and proxies are actively engaged in attempts to shape perceptions of populations and decision makers through aggressive MDM activity across social media platforms. Russia-sponsored or supporting activities on social media range from dissemination of pro-Russia propaganda to wide engagement in conspiracy theories.
2. These actors engage in multiple traditional and tailored MDM campaigns targeting Canada, its government in power, and specific policies such as Canadian support to Ukraine to include within NATO.
3. Suspected Russia government and affiliated cyber actors have been implicated in Canada-directed cyberattacks, including the hacking of political organisations and government agencies.
4. Given the Russia government's legacy techniques of fomenting dissent between domestic ethnic groups, it is probable Russian actors are involved in similar activities within Canada.
5. Finally, Russian actors used the information environment to influence domestic perceptions and government policies. These efforts have not been sufficiently successful to date.

Tactics and Implementation

- **Disinformation Campaigns**: Russia used state-controlled media and social media platforms to spread false narratives, targeting both the political left and right, amplifying divisive issues, and promoting conspiracy theories. This included both misinformation and disinformation. For example, during the 2021 Canadian federal election, Russia disinformation efforts sought to amplify conspiracy theories about election fraud and promote distrust in the electoral process.
- **Cyber Operations**: Coordinated cyber-attacks, including phishing and malware, are used to undermine Canadian institutions and critical infrastructure. In 2023, pro-Russia cybercrime groups launched distributed denial-of-service attacks on Canadian government websites, financial institutions, and transportation systems, including border checkpoints and airport check-in systems. These cyber operations promote service disruption, steal sensitive data, and amplify the impact of concurrent disinformation campaigns. Cyber-attacks on Hydro-Québec and Canadian airports caused significant disruptions and highlighted vulnerabilities in critical infrastructure.
- **Cultural Diplomacy**: *It is important to note that cultural diplomacy is a legitimate national activity practised by many countries to promote cultural exchange and understanding. However, in this context, we are examining how Russia integrates these legitimate activities with illegitimate MDM and FIMI operations.* Through initiatives that promote Russian culture and language, Russia builds a

positive image and fosters sympathies that can be leveraged geopolitically. This soft power approach helps Russia to continue to establish a foothold in Canadian society, subtly influencing public opinion. For instance, Russia has sponsored cultural events and academic exchanges to promote Russian heritage and foster favourable views among Canadian citizens.

- **Influence on Elections**: Russia has attempted to interfere in Canadian elections by spreading false information and supporting fringe political groups to sow discord. These activities have involved disseminating misinformation and disinformation to polarise the electorate and undermine confidence in the electoral process. For example, Russia-affiliated actors have used social media to amplify false narratives about election integrity and manipulate public perception during election cycles.

Assessment and Implications

The case of Canada underscores the persistent and multifaceted nature of Russian hybridised warfare including information confrontation. These tactics create immediate disruptions and foster long-term instability by eroding public trust in democratic institutions. The impacts of these operations are far-reaching, contributing to political polarisation, undermining the integrity of electoral processes, and weakening national cohesion. Furthermore, the adaptive nature of these tactics, with a blend of online and offline strategies, means that they can evolve quickly, posing continuous challenges to Canadian national cohesion.[9]

Russia's steadfast commitment to the targeting of Canada, its government, population, and policies highlights the extent Moscow is willing to engage with the major states of the West and close allies to the United States. It is likely the information confrontation strategy targeting Canada is, in part, related to Ottawa's close relationship politically with Washington.

MDM: potential impact for New Zealand

Current geopolitical realities indicate **it is much more likely for New Zealand to be targeted through the country's partners or influence its roles within international institutions and cooperative regimes.** Taking the above case studies into account, **New Zealand's unique geopolitical environment and information landscape present specific vulnerabilities that the Russia government and proxy actors could exploit with MDM activities and information confrontation strategies.** By exploiting New Zealand's unique social, political, and economic vulnerabilities, Russia could disrupt democratic processes, sow distrust in institutions, and influence public opinion.

The calculus for an expanded Russia-centric effort to target New Zealand, as shown in the above global case studies, could result from factors that have little to do with relations between Moscow and Wellington. There are distinct possibilities Russia could directly target New Zealand. However, the role of domestic threat actors and conspiracy communities, who are either knowingly spreading disinformation or unwittingly spreading misinformation narratives harmful to the New Zealand population, presents a cross-cutting risk. These groups could be co-opted, even unwittingly, by malign state actors.

In 2022 it was noted that "New Zealand's conspiracy theorists are almost unanimously supportive of the Russian invasion and are creating or spreading conspiracy theories about bioweapons facilities and paedophile cabals linked to Ukraine."[10] Even though no direct-targeting of such audiences was identified, this

[9] Dave McMahon, "*Maligned Influence and Interference in Canada,*"Canadian Global Affairs Institute, July 2023.
[10] Marc Daalder, "*NZ anti-vaxxers fall for 'tsunami' of Russian disinformation*," Newsroom NZ, August 2022.

still presents a vulnerability within New Zealand's information space, due to Russia and other hostile state TTPs.

The following examples characterise Logically's assessment of the three key MDM topics in New Zealand's information environment that could be exploited by Russia, and amplified if they are seeded by domestic conspiracy theorists or threat actors.

MDM Undermining New Zealand's Geopolitical Objectives

New Zealand's major alliances and partnerships could present as key vulnerabilities to Moscow MDM and information confrontation planners. Russia may utilise state-controlled media and social platforms to propagate false narratives regarding New Zealand's political alliances, such as its relationships with the so-called Five Eyes intelligence sharing regime, perceptions of potential participation in the nuclear submarine development and construction programme between Australia, United Kingdom, and United States, known as AUKUS, or New Zealand's relationship with China. For example, Russia could depict New Zealand as excessively dependent on China or question its strategic alignment with Western powers.

The historic relationship with the British Commonwealth and English-speaking world powers and regimes such as the Five-Eyes intelligence sharing regime could provide the Russia government the means to target other states governments and policies tertiarily through New Zealand. Russia has a limited history of such activities. However, domestic and international discourse regarding New Zealand's potential involvement in the AUKUS program could provoke a response from Russia. This development might lead Russia to leverage disinformation campaigns and cyber activities to influence the discourse and policy decisions

These tactics could be designed to sow confusion and undermine trust in the government and its international alliances. Disinformation in this context would probably involve distorting facts to imply New Zealand is compromising its sovereignty or security due to its economic ties with China or perhaps its relationship with the United States. Such a situation would mirror the way Russia employs disinformation to shape public opinion in Ukraine and Canada by emphasising the vulnerability and geopolitical decisions of the country.

Similarly, given the standard Russia government MDM playbook, a probable venture in the potential targeting of New Zealand would be to portray a government in power or specific leaders as pawns of the United States, NATO, or other institution. In historic examples of the use of this tactic, the actual policy or affiliation is often innocuous, the more important matter to Russian actors is the suitability for exploitation. This case was evident in Russia disinformation in the U.S. that exacerbated relations between minorities and police or in Burkina Faso wherein anti-French sentiment was rapidly magnified.

MDM Undermining Social Cohesion in New Zealand

Russia's information confrontation efforts including cyber attacks and MDM have traditionally sought to disrupt adversarial governments through stoking of social or ethnic divisions. The relatively strong state of national social cohesion in New Zealand would indicate if Moscow took this tack, it would have to augment its activities in order for them to be effective. To do so Russia could target an emergent social divide or issue as a means to advance its objectives through the aggravation of this issue.

Transitioning from this focus on indirect influence and the cultivation of a positive national image through cultural and academic means, it's important to also consider the tactics Russia might deploy to exploit social and ethnic divisions within New Zealand. By intensifying existing tensions, such as issues related to rights or immigration, Russia could deepen societal divides and divert attention from its influence operations. Potential target communities and issues could possibly include Māori-Pakeha (European origin) relationships, sensitive immigration issues especially immigration by minority populations, housing affordability or inequality issues, and environmental concerns.

Should Russia decide to engage in this aspect of MDM, it would likely select an issue it perceived most able to support its overall objectives. In Logically's assessment, based on prior reporting, this would likely involve targeting New Zealand's diverse society and in particular its indigenous population and various immigrant communities.[11] New Zealand's multicultural makeup, with its mix of historical grievances and contemporary issues related to immigration and integration, presents opportunities for external actors to amplify tensions and create discord. Russia's influence operations could exploit these divisions to create societal discord through MDM, FIMI, and CIB. Misinformation about land rights or immigration policies could spread through social media, causing confusion and heightening community tensions. Deliberate disinformation might involve fabricating stories about government favouritism towards certain ethnic groups, inflaming inter-ethnic tensions, as cited in previous Logically reporting.

Russian actors could use coordinated social media accounts to spread these narratives widely, making them appear credible. Russia could also exploit local media outlets or create fake news websites to publish divisive stories. For example, manipulated stories about the government handling ethnic issues could erode public trust in government institutions. Russia operatives could also use fake accounts and bots to amplify divisive content and orchestrate online campaigns that seem grassroots but are, in fact, state-sponsored.

MDM Targeting Democratic Processes

Russia-directed MDM often targets governments aligned with the U.S., NATO, or other purportedly anti-Russia organisations. As seen in Russia disinformation associated with the 2016 and 2020 U.S. presidential elections, while Russia interference and MDM may not necessarily have an appreciable impact on the election's outcome, the net result is a restriction on the political freedom of elected officials and the expansion of popular distrust of the political and governmental system. This restriction occurs because disinformation campaigns can erode public trust in officials, making it difficult for them to govern effectively, and create an environment of increased scrutiny and pressure. According to some reports, political polarisation had been steadily increasing in the U.S. since at least the 1970s, but following the 2016 and 2020 elections there was a noted increase in political violence and a reduced belief in the solvency of the electoral process. [12] [13]

Russia could direct a major MDM campaign against New Zealand to influence its political landscape and promote policies favourable to Russia's interests. Based on previous efforts, disinformation could be used to attempt to polarise the electorate or undermine confidence in the electoral process. This is further reinforced by the fact that anti-establishment narratives are a dominant theme of MDM in New Zealand's online information environment, making this section of the population particularly susceptible to MDM efforts aimed

[11] Logically, "Misinformation, Disinformation and Malinformation Threats Impacting New Zealand Audiences," May 2024
[12] *"America's trust in its institutions has collapsed"* The Economist, April 2024.
[13] Benedict Vigers, "*U.S.: Leader or Loser in the G7? Americans least confident in national government, judiciary and other key institutions*," Gallup, April 2024.

at amplifying distrust and division. Elements of these analyses indicate the role in the spread and acceptance of known Russia-government MDM activities in these trends.[14]

Potential MDM targeting New Zealand should be conceptualised not so much as directed against a specific party or candidate, but rather within the scope of instigating increasing levels of instability and weakening democratic institutions. It is possible Moscow perceives a weak government as more malleable to its entreaties or perhaps less capable of supporting other states' anti-Russia initiatives. Tactics for election disruptions could include promoting conspiracy theories about election integrity, highlighting divisive political issues, or circulating misleading information regarding voting procedures or candidate backgrounds. For example, Russia could spread misinformation about New Zealand's COVID-19 response, disinformation about election integrity, and malinformation targeting political figures to erode public trust in democratic institutions.

New Zealand's relatively transparent democratic practices, small population, and active political engagement are potential targets of Russia information confrontation to especially include cyber attacks and MDM dissemination. It is most likely Russia would choose to interfere in elections to cause specific changes in policies to benefit Russia. These benefits may not necessarily be readily apparent. Secondarily, Russia FIMI could simply be to reduce trust in democratic processes in order to make the country more malleable to Russia's political will or prevent New Zealand from engaging with other states' or institutions' counter-Russia activities.

There is sufficient evidence and examples of Russia-sponsored election interference to highlight the most likely means that could be employed. For instance, Russia could interfere in New Zealand's political processes, including elections, by spreading false information, or supporting and empowering fringe political groups. Incorrect information about voting procedures or the integrity of the electoral process could be used to spread confusion among voters and potentially reduce voter turnout. Deliberately false narratives could be crafted to deceive the public and manipulate opinions to skew results. Pro-Russia actors have previously disseminated false claims about election fraud or political corruption on a global scale. These claims have been spread through social media, mainstream and fringe media, and via malleable entities shaped to support Russia's objectives, often without the entities' knowledgelnaccurate or misleading information could be leaked to harm individuals or organisations involved in the political process, including the selective release of private communications or other sensitive data to create a negative perception of political figures or parties. In total, there is an extensive list of potential vectors for Russia information targeting of New Zealand political processes and events. It would be possible to assess historic Russia tactics and align to the most likely and most vulnerable targets.

Russia's TTPs: Potential Impact for New Zealand

As demonstrated by the global case studies outlined above, Russia's MDM and FIMI campaigns are just one method in their complex approach of hybrid threats. Based on Russia's approach, any such information campaign that would target New Zealand would likely be accompanied by broader TTPs, including attacking the country's cyber defences, reputation on the world stage, and the free and pluralistic fourth estate.

[14] Rachel Kleinfeld, "*Polarization, Democracy, and Political Violence in the United States: What the Research Says,*" Carnegie Endowment, September 2023.

Cyber Operations

Any increase in Russia government-directed MDM campaigns targeting New Zealand or its population is or would almost certainly be complemented by targeted cyber-attacks against New Zealand's critical infrastructure and governmental systems. These attacks would have the initial intent of causing political, economic, and social disruptions. Additionally as has been seen in the three case studies and other Russia MDM and cyber activity, the combination of these efforts would also seek to undermine trust in public institutions and create a sense of various levels of insecurity. Russia cyber actors might exploit known vulnerabilities to disrupt essential services, steal sensitive information, or spread malware, amplifying disinformation campaigns' impact. These cyber operations are integral to government-directed MDM as they often accompany information manipulation efforts to magnify the psychological impacts. Historically, MDM is also used after a cyber attack to further the deleterious effects and exaggerate or amplify the message or the impact. Should Russia's activities recover government or other sensitive information through its cyber actions, it is almost certain it will leak that information to amplify current or cause additional harm. [15]

Russia's cyber operations could target New Zealand's critical infrastructure and government systems. New Zealand's increasing reliance on digital infrastructure for essential services and its relatively smaller cybersecurity resources compared to larger nations make it particularly vulnerable. Any cyber-attack could cause significant disruption and foster public insecurity. Russia's government or affiliated actors might exploit these vulnerabilities to disrupt services, steal sensitive data, or spread malware, thereby amplifying the effects of concurrent disinformation campaigns. For example, an attack on New Zealand's power grid or healthcare systems could cause widespread disruption and fear, undermining trust in the government's ability to protect critical infrastructure. Furthermore, these cyber activities could serve as access points for attacks or MDM campaigns against New Zealand's allies, partners, or participating institutions, exploiting the nation's cybersecurity gaps to indirectly target other states' governments and policies

In any case wherein Russia would target New Zealand with cyber activities, it is almost certain it would preempt and follow up the attack with a concerted MDM effort to amplify the impacts and disruption. An example of the pairing of cyber capabilities and dissemination of MDM occurred when Russia actors used cyber operations to hack and leak sensitive information from the Democratic National Committee (DNC) in the United States, which was then exploited in disinformation campaigns to influence public perception and sow discord. Similar tactics could be used to target New Zealand, combining cyber-attacks with disinformation to create widespread confusion and mistrust.

Combining MDM, Cultural Diplomacy and Soft Power

It is important to note that cultural diplomacy is a legitimate national activity practised by many countries to promote cultural exchange and understanding. However, in this context, we are examining how Russia integrates these legitimate activities with illegitimate MDM and FIMI operations.

From the Soviet era to the present, Russia has used its outreach through cultural diplomacy and soft power as tools within its information confrontation strategies. Soviet efforts primarily targeted the developed world where autocratic leaders were more likely to engage in quid pro quo strategies and power dynamics to align with the Eastern bloc. Russia has built on this approach to sustain its engagement in Africa and expand the tactics, techniques, and procedures of cultural and soft power at other states believed vulnerable to coercion

[15] *"The Framework to Counter Foreign State Information Manipulation",* U.S. Department of State, January 2024.

via these means. In New Zealand this approach could manifest through the establishment of cultural engagement or education national programs to advance and promote pro-Russia narratives, conspiracy theories and anti-West messaging. In doing so, based on historic targeted communities, Russia would almost certainly target these efforts toward minorities or minority groups to include taking advantage of any cultural milieu it perceives as a point of friction between disadvantaged groups and the majority demographic or perceived "ruling elite."

Through cultural initiatives and educational programs, Russia could promote its narratives and foster pro-Russia sympathies within New Zealand. This approach might include sponsoring cultural events, academic exchanges, and media content highlighting positive aspects of Russian culture and policy, subtly influencing public opinion and political discourse. Such initiatives can result in misinformation if the cultural events distort historical facts or current political situations to present Russia in an unduly favourable light. Disinformation can also be part of these initiatives if Russia deliberately promotes false narratives through cultural channels. Since most Russia MDM efforts are for all intents and purposes centrally managed, when soft power would be used, it is almost certain the event or occasion would be aggressively amplified through government media, online activity and other controlled dissemination mechanisms.

Academic exchanges could be used to subtly promote Russia's political viewpoints, while media content can highlight pro-Russia narratives that align with its geopolitical goals. Such efforts are part of a broader strategy to create a positive image of Russia, making target officers more receptive to pro-Russia narratives or weakening popular or governmental resistance to Russia-managed influence activities. These strategies were observed in the Burkina Faso, Ukraine, and Canada case studies, wherein cultural diplomacy and soft power were effectively used to build a favourable image of Russia, its policies, and interests as well as influence public opinion supporting these geopolitical objectives.

Another aspect of soft power would be to target outreach at elements of social or political groups perceived as receptive to Russia's messaging. Since far-right groups often hold anti-establishment positions, it is possible they could be co-opted by Russia's soft power efforts. Historically, Russia has leveraged the activism and dissent of such far-right groups to sow discord and destabilize societies, aligning with its known TTPs.

Undermining the Media Landscape

There has been a decline in trust in news media among New Zealanders, with only 33% agreeing with the statement that they "trust the news most of the time". This erosion of trust is likely to leave New Zealand more susceptible to disinformation campaigns and activities originating from Russia. When confidence in traditional news sources wanes, individuals are likely to turn to alternative information channels, which foreign actors can manipulate more easily due to a lack of regulation and effective policy.

Compared to other countries, New Zealand has a small number of local media outlets. Such concentration means that successful targeting of a few key channels could allow Russia disinformation actors or Russia-aligned actors to potentially influence public opinion broadly across the nation. In recent years, New Zealand has witnessed instances of disinformation spreading through social media and smaller, less regulated news platforms, demonstrating the potential ease with which Russia disinformation can be disseminated within the country's concentrated media landscape. Additionally, during the COVID-19 pandemic, New Zealand's anti-vaccine groups fell for Russia disinformation, spreading false claims about the vaccines, which further fueled vaccine hesitancy and public distrust in health policies.[16]

[16] Logically, "Misinformation, Disinformation and Malinformation Threats Impacting New Zealand Audiences," May 2024

New Zealand is also experiencing a shrinking media landscape. Two main New Zealand media outlets have announced program closures and job cuts.[17] There is a realistic possibility that financial and resource constraints could lead to less rigorous fact-checking, making New Zealand's citizens more vulnerable to exposure to disinformation seeded by malicious state actors.

New Zealand has a relatively small and concentrated media market, which could provide the means to effectively disseminate MDM to a large percentage of the population with minimal effort. Moreover, given the concentrated nature of the media environment, targeted Russia actions could delegitimize news and therefore push New Zealand audiences to alternative online news sources that share MDM narratives.

The rise of alternative media sources in New Zealand increases the potential access points of Russia MDM activities. Once penetrated, these alternative content creators and producers generally lack the ability to detect and counter the Russia government or affiliated actors. Also, given the environment of open media access through online social platforms, even if knowingly penetrated, so long as public engagement is sustained (and often increased) there is often a disincentive to eliminate Russia government MDM content when it could be generating engagement and revenue for the alternative news website.

Conclusion

Currently New Zealand is not a major target country for the Russia government or proxy MDM and broader information confrontation attacks or manipulation. However, the Government Communications Security Bureau (GCSB) has established clear links between the Russian government and a campaign of malicious cyber activity targeting overseas political institutions, businesses, media and sporting organisations. Although New Zealand organisations were not directly affected by malicious cyber activities. GCSB has observed a range of activity in New Zealand that contains indicators which can be linked to Russia state actors.[18]

The case studies and tactics overview presented within this summary report detail the manner, means, and impetus of Russia MDM and cyber activities that could be conditionally employed against New Zealand should the current state change. As discussed, this report has attempted to highlight, based on precedent, the triggers and vectors for potential Russia government action in these realms against New Zealand.

The calculus for an expanded Russia-centric effort to target New Zealand, as shown in the above global case studies, could result from factors that have little to do with relations between Moscow and Wellington. There are distinct possibilities Russia could directly target New Zealand; however, current geopolitical realities indicate it is much more likely for New Zealand to be targeted through the country's partners or influence its roles within international institutions and cooperative regimes. At present, the current policies in relation to support for Ukraine, the strategic partnership with the U.S. and alliance with Australia, suspicion regarding participation in AUKUS, and role in the Five Eyes intelligence sharing regime are the most likely friction points that would lead to greater Russia government information confrontation actions targeting New Zealand.

---

[17] Eva Corlett, "*Blow to New Zealand media as two main news outlets announce program closures and job cuts*," The Guardian, April 2024.
[18] "Malicious cyber activity attributed to Russia," NCSC Government NZ, October 2018.

Should this occur, it is highly unlikely Russia would create a new approach within its MDM and cyber strategies and instead use its historic thematic and negative approaches tailored to New Zealand audiences. Therefore, a greater awareness and understanding of these themes and narratives should enable more effective counter-messaging and MDM disruption activities.