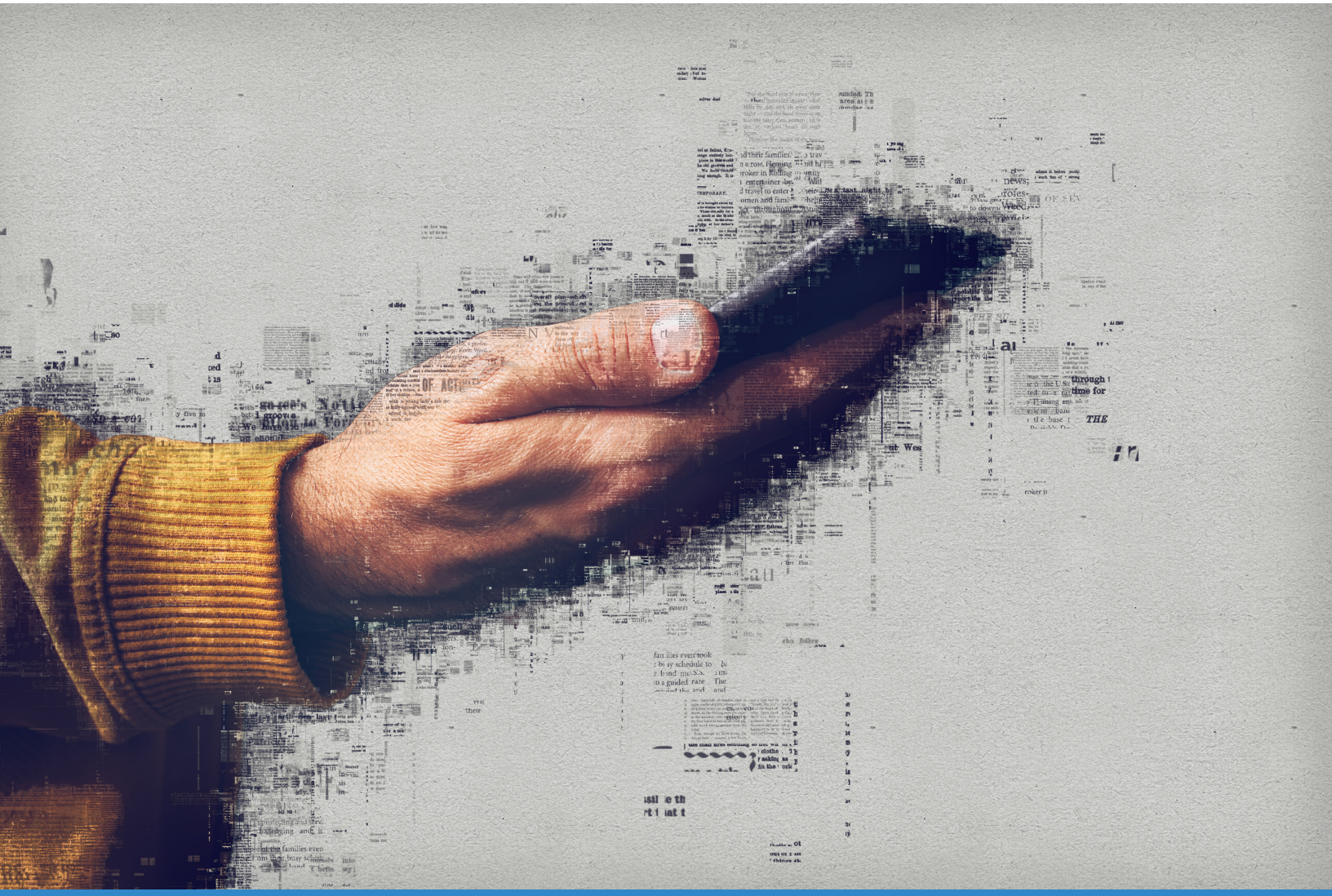


DEZINFORMATSIA:

The dangerous axis of Russian and Chinese Disinformation, Deception and Disruption

DAVE MCMAHON, SLG | NOVEMBER 2023
a contributor to the University of Ottawa Information Integrity Lab

uOttawa
Laboratoire sur l'intégrité de l'information
Information Integrity Lab

EXECUTIVE SUMMARY

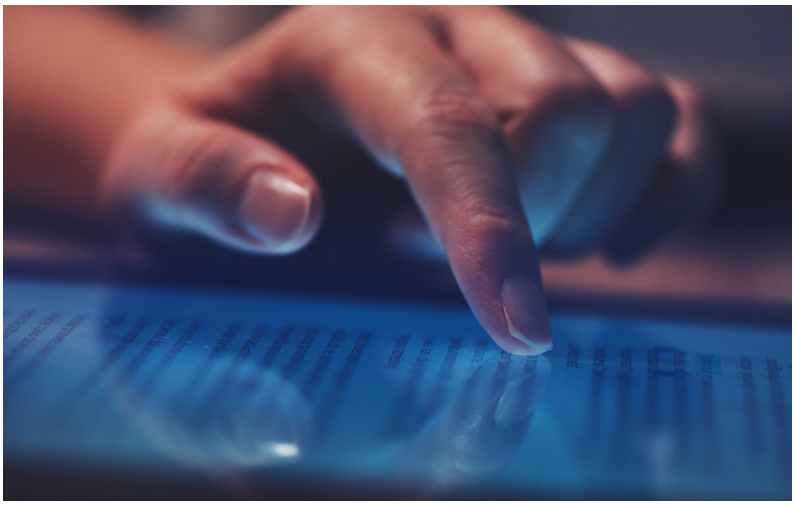
Through misinformation, disinformation and malinformation (MDM), Russia and China engage in strategic deception and manipulation to achieve political, economic, and military objectives. Disinformation ecosystems operated by Russia and China, use obfuscated and sophisticated tactics. The Kremlin employs a distributed-uncoordinated approach, using proxies and creating disinformation storms on social networks to amplify their messages. Russian influence narratives propagate blended fabrications, conspiracies, and half-truths. China, on the other hand, uses a cohesive partnership between industry, government, and the military to achieve its goals. This representants a vast disinformation ecosystem consisting of nested layers of intelligence services, front companies, vicariously state-owned research institutes, military units, universities, research facilities, private military contractors, transnational criminal organizations, and state-controlled media.

The complexity and sophistication of foreign threats posed by MDM ought to be met with both resiliency and active countermeasures as part of a national cognitive infrastructure protection and information peace keeping strategy involving all stakeholders. Currently, these disinformation networks are often uniquely discoverable and attributable with, and targeted by, open-source intelligence (OSINT) methods. Consequently, supplemental to actions by government entities, the private sector can continue to play a central role in countering foreign disinformation, influence, and interference.

INTRODUCTION

In the era of strategic competition, the war on truth, through disinformation, will pose the greatest challenges of our lifetime. But defending the truth requires deep knowledge of adversarial capabilities, tradecraft, and intent. Those insights about adversaries will be gained principally through open-source intelligence. One of the greatest challenges will be attribution – who is behind a disinformation campaign and why. Attribution is often intentionally confounded by those who created it by both technical means and through deception and misdirection – making disinformation appear to be legitimate discourse protected as free speech. Attribution is critical to formulating a response by both the Canadian government, the private sector and civil society.

Disinformation is misinformation deliberately spread to deceive people. Whereas malinformation is information that is true, often private, or confidential, that was intentionally leaked to inflict actual harm. These tactics have become so common that they now have their own colloquial names such as "doxing" and "swatting."



The problem of disinformation is nothing new. It has appeared in many forms for as long as people have sought to deceive each other. It has long been employed by states as a weapon in military, political and economic warfare. A 1993 white paper on information warfare by the Canadian Department of National Defence introduced the concept of "information peace keeping" - perhaps a uniquely Canadian approach to the issue[1].

The 1993 white paper explained that the challenge of information peace keeping (IPK) is how to use the power of the cyberspace, and leverage the global information grid and its content, to act with effect within new social networks, political spaces to safeguard truth systems. If cyber physiological operations (CYOPS) can influence the human terrain, and if information warfare is about destroying knowledge, truth, and belief systems, then the prime objective of information peacekeeping would be to help us understand the cognitive processes that validate what ultimately is trustworthy knowledge and to engineer countermeasures to radicalization, foreign influence, and interference in the democratic process. Information theory talks about the medium and the message. Equally important to cognitive warfare is the

technical means. Cyber is the modern-day battleground of ideas, influence, and deception.

Three decades later, a 2020 NATO-sponsored study on cognitive warfare characterized disinformation as the **"weaponization of brain sciences,"** which can hack the human "wetware" by exploiting human vulnerabilities and then socially engineer behaviour.

Foreign influence, interference, disinformation, deception, and disruption are entwined tools of modern statecraft, which are amplified by cyber.

PACING THREATS

Russia and China maintain vast disinformation ecosystems and run sophisticated operations at scale against domestic and global target audiences. The governments of these two countries exercise control over domestic media, and target diasporas, through native language programming and platforms. Disinformation is widely spread into diaspora Chinese communities via social media such as WeChat. The Kremlin uses Vkontakte (VK), a Russian online social media and social networking service based in Saint Petersburg, to carry their narrative. Similarly, Telegram, launched in 2013 by the founders of VK, is another popular platform exploited by the Russian state propaganda machine.

Cantonese, Taishanese and Mandarin are the dominant non-official languages spoken in Canada. Over 1.7 million (4.6%) Canadians speak a Chinese dialect. Beijing's hyperactive United Front Work Department spends massive resources in cultivating deep ties to the hyper-rich elements in the Mandarin bloc, while at the same time bullying and intimidating the diaspora's reformists, Uyghur refugees, pro-democracy Hongkongers, Falun Gong adherents and defenders of Taiwanese autonomy.[2]

Diasporas may not have access to mainstream media, owing to a language barrier. The reliance on social media like WeChat or VK news creates an "echo chamber" that is further amplified by platform algorithms. Groups tend to endorse a belief held by their community to seek social recognition in groups that they are familiar with. Hence, diaspora communities are trapped in the vicious cycle of reinforced information consumption patterns. Equally, social media discourse in languages other than English or French generally remains opaque to review by the Canadian public, mainstream media, or the government; therefore, disinformation on these platforms, particularly foreign interference conducted via disinformation, is insidious and virtually invisible.

The targeting of English-speaking native communities in Canada by adversaries is a bit more nuanced. Here, foreign influence is often directed at fringe groups. Russia targets left- and right-wing groups in Canada as well as those who are prone to believing in conspiracies. On the other hand, China plays to woke culture and racism. The national post commented, "dismissing worries over election interference as 'racism' is part of a well-known China propaganda tactic."[3]

Both Russia and China use disinformation as a weapon to disrupt and harm the Canadian economy and the democratic socio-political framework. Their objective is to empower organic disinformation nodes (involving real Canadians) and fuel divisive opposition within Canada. Both powers also employ traditional agents of espionage, influence, and interference, including deliberately, cyber-facilitated technical interference against critical infrastructure and exploitation of supply chains. Examples of this include Nortel, ASN.1 and the Solar Winds attacks.

In the following pages, we will compare how Russia and China use disinformation in more detail.

RUSSIA

The Russian term dezinformatsiya is derived from the title of a KGB "black propaganda" department. "Black propaganda" is defined as a falsely accredited form of propaganda associated with covert psychological operations. The principal feature of black (covert) propaganda is that the audience is unaware that they are being influenced. Gray propaganda does not identify its source, whereas white (overt rhetoric) propaganda tends to be, at least superficially, sourceable promotional material.

The Russian use of **dezinformatsiya** began with a "special disinformation office" in 1923 to propagate false information to intentionally deceive public opinion within the USSR. "Information confrontation" is the term used in Russian strategic and military circles to describe their approach to the use of information in both peacetime and conflict, whereas "active measures" is used to describe long-standing Russian political warfare methods.

Initially, Russian propaganda was designed to appeal to socialist ideology; indeed, some found the tenets of communism appealing. But the allure of communist narrative has since crumbled with the fall of the Berlin Wall. Today, Russia is seen in many parts of the West as the grand antagonist. The Kremlin and its proxies mislead and influence public opinion in ways that benefit the Russian government by deliberating spreading false or misleading information through various channels, including social media, news outlets and other forms of communication including radio, television, and film production.

Russian disinformation often uses a combination of half-truths, doublespeak[4], psychological projection, conspiracy theories and bold lies to create confusion, sow discord and undermine public trust in democratic institutions. Russian narratives can be incongruous or bizarre - meant to confuse and shock.

Sometimes anti-West propaganda or disinformation is used to support Russian foreign policy objectives, such as promoting pro-Russian sentiment, advancing Russia's geopolitical interests ("de-natizifying" Ukraine is one example), or destabilizing rival governments and political parties in fragile states such as those in Africa. In short, Russia seeks to create opportunities through chaos.

Russia Is Opportunistic in Spinning Disinformation Campaigns

Some examples of Russian disinformation campaigns include promoting bizarre conspiracy theories and spreading falsehoods about the COVID-19 pandemic and 5G safety or using fake social media accounts to influence elections. These campaigns often involve the use of bots, trolls, and other automated systems to amplify their message, in both mainstream channels and homegrown conspiracy movements like QAnon, to make it appear more credible.

Interestingly, China has been trying to promote the planet-wide adoption of Chinese 5G technology under the Belt and Road Initiative, whereas Russia's efforts go in the opposite direction. Indeed, some Canadians who believe Russian disinformation about 5G have torched cell towers.

The US Department of State's Global Engagement Centre explains that Russia's disinformation and propaganda ecosystem is the collection of officials, proxy, and misattributed communication channels and platforms that Russia uses to create and amplify false narratives.[5] The ecosystem consists of five main pillars: official government communications, state-funded global messaging, cultivation of proxy sources, weaponization of social media, and cyber-enabled disinformation. The Kremlin bears direct responsibility for cultivating these tactics and platforms as part of its approach to using information as a weapon.

The US State Department further argues that Russia invests massively in its propaganda channels, its intelligence services, and its proxies to conduct malicious cyber activity to support their disinformation efforts. It also leverages outlets that masquerade as news sites or research institutions to spread these misleading narratives.

There is no single media platform for propaganda and disinformation, nor is there uniformity of messages among different sources. Individual messages within the system may appear contradictory. The ecosystem approach is fitting for this dynamic because it does not require harmonization among the different pillars.[6] This provides strategic ambiguity within the information ecosystem.

Russia's willingness to employ a distributed-uncoordinated approach to disinformation provides the Kremlin with three perceived advantages. First, it facilitates the introduction of numerous variations of a false narrative. This enables the pillars of the ecosystem to tune the narratives to retarget new audiences. Secondly, proxies can propagate dangerous messaging while Kremlin overlords remain anonymous. Thirdly, it creates a media amplification effect among the different channels to boost their reach and resonance. This media multiplier effect can, at times, create disinformation storms or infodemics.

The Kremlin outsources a great deal of its cognitive warfare, and a lot of this outsourcing goes to one entity: the Wagner Group.

WAGNER GROUP AND DISINFORMATION

In the north-west of St. Petersburg stands as the northernmost skyscraper on earth – the Lakhta Centre. The local media call it the "Eye of Sauron" - constantly looking to the west, a dark source of malign influence, misinformation and lies. It is the former headquarters of the Russian Internet Research Agency (formally dissolved July 2023 but whose operations continue under a different front) - a state-sponsored troll factory formerly owned by Putin's lieutenant oligarch Yevgeny Prigozhin, who also ran the Wagner Group.

The Wagner Group is a private Russian paramilitary company and sanctioned transnational criminal organization[7] linked to disinformation campaigns aimed at advancing Russian interests. In fact, evidence of a former secret communication channel[8] exists between Yevgeny Prighozhin and the Office of the Presidential Administration of the Russian Federation. Some examples of the Wagner Group's disinformation campaigns include spreading false information about the conflict in Syria and creating fake social media accounts to influence elections in other countries. The Wagner Group's disinformation campaigns are seen as a threat to democratic societies, as they can undermine public trust in institutions and create division among citizens. The group has close ties to the Russian government and has been indicted in a range of activities, including human rights abuses, war crimes, election interference, propaganda, and other forms of disinformation.

Another key player was the Internet Research Agency (IRA) which was founded/financed by Wagner. It was also known by various aliases: Internet Research LLC, RIA, RIAN and RIAFAN. The IRA and its successor, the Federal News Agency (FAN), was part of the Russian "Lakhta Project." The only entity that is currently still in official operation is the Federal News Agency (FAN) with a new set of front domains designed to obscure the origin of the malign content. The IRA was liquidated by Vladimir Putin in 2014, when Russia invaded Crimea, by presidential order to create "Rossiya Segodnya Agency" (Russia Today Agency) and absorbing all the employees of IRA. The newly created agency also absorbed FAN on the day of Crimea's invasion, creating "RIA FAN" with the new addition officially registered to Rossiya Segodnya April 8, 2014.

These state-run troll farms of the former IRA have been implicated[9] in fomenting polarized discussions online, undermining liberal democracies, interfering in elections, stirring up the anti-vax movement and climate change denial, sowing fractured narratives, and violently attacking anti-doping organizations. In other words, they spread misinformation and disinformation, which is intended to erode, disrupt, and degrade trust in the democratic system, sabotage the industrial growth of Canada and undermine fundamental Canadian values and quality-of-life.

Russian influence narratives have blended fabrications, conspiracies, and half-truths to amplify their messages.[10] Russia's disinformation is tailored to capture Canadian audiences with narratives that resonate with them. As we in the West see cyber as a technical domain of ones and zeros, our adversaries think of cyber as ABC's - a domain of knowledge and influence. Russian Gerasimov[11] doctrine (hybrid warfare) combines military, technological, information, diplomatic, economic, cultural, and other tactics for the purpose of achieving strategic goals, through the theft of intellectual property, disinformation, and deception.

CHINA

China is working to become a global media and disinformation superpower through an arsenal of tactics, including through state media, disinformation campaigns and digital infrastructure. The Chinese government uses a whole-of-society approach for collecting intelligence and propagating disinformation. This sets it apart from anything undertaken by Western governments.[12]

China engages in systemic and strategic deception, disinformation, influence, and interference through their industrial collaboration in the Belt and Road Initiative, three warfare's strategy, thousand talents program, and unified front activities - more about that later.

Beijing is also working to influence public opinion through state media's partnership agreements abroad. Chinese state media journalists have been tasked with exploiting the ambiguity of their personal brands to push state propaganda. Flooding social media platforms like Twitter with "massive amounts of spam to make it harder for reporters and independent observers to access information about what's going on" explains Kurlantzick, a senior fellow for Southeast Asia at the Council on Foreign Relations.

China recruits millions of its citizens as 'keyboard warriors' to influence public opinion online and manipulate the truth on a massive scale like the troll farms in Russia. These recruits are known as the "50 cent army" because they are paid 0.5 yuan per post.

Recently, Beijing has shifted towards covert, malign Russian-style tactics and aggressive "wolf warriors"[13] online diplomacy and attacking Western media directly. As an example, the Chinese state media shift blame away from the origins of COVID by spreading the rumour that the virus was a USA bioweapon. Chinese Twiplomacy has varied wildly in content and forms of engagement, suggesting a lack of coordination approach by the China's diplomatic corps.

Beijing is getting better at disinformation on global social media. Their covert influence, interference and disinformation are gaining traction by polarizing public debates in the West, like Russia tactics. Chinese networks are resisting takedown efforts and gaining traction among real users. Still, they are getting caught running fake social media accounts and campaigns. For example, the spamouflage dragoninvestigation, a social media campaign targeting the Hong Kong protests, took down 23,000 twitter accounts linked to China involved in a range of "manipulative and coordinated activities.[14]

Ironically, online disinformation hampers China's grand initiatives for data supremacy and artificial intelligence, which relies on the veracity of big data. In other words, China's own data holdings become compromised by false data that China itself propagates as disinformation.

PROXIES

In many foreign jurisdictions, national industry and organized crime form an integral part of their country's military and intelligence apparatus.[15] Russia, China and Iran use their industry to procure capability at an operational tempo far faster than Canada and to run disinformation campaigns on behalf of the State.

The Russian information warfare ecosystem is both vast and complex. Like a Matryoshka doll, it consists of nested layers of corporate entities, vicarious state-owned research institutes, military units, universities and Soviet-era research facilities associated with the state security apparatus developing signals intelligence and cryptographic capabilities. Complicating matters, the Russian state actively encourages and employs criminal hackers.

Similarly, troll farms for disinformation/influence operations work independently from decentralized actors and crowdsourced campaigns. The Russian intelligence services like the Federal Security Service (FSB), the Foreign Intelligence Service (SVR) and the Main Intelligence Directorate (GRU) are all active players in this space, along with the Internet Research Agency (IRA) and the Wagner Group. These organizations frequently both cooperate and compete against each other and industry. There appears to be no central authority.

A good example of the above is a recent story by the Guardian[16], which confirms Sapper Lab's independent research concluding that the private information warfare company Ntc Vulkan is taking operational direction from Russian intelligence services for

offensive cyber and disinformation operations. The GRU 74455 (Military Intelligence) was listed as "approval party" for operations on secret documents with the company. The company has been implicated in blackouts in Ukraine, disrupting the Olympics in South Korea, launching the computer exploit Notpetya,[17] and creating the Sandworm program to control the Internet and spread disinformation. The Russian military hired this private contractor to build similar tools for automated domestic propaganda. The Ntc Vulkan Amezit subsystem allowed the Russian military to carry out large-scale covert disinformation operations on social media and across the Internet, through the creation of accounts that resemble real people online, or avatars. These avatars have names and stolen personal photos, which are then cultivated over months to produce a realistic digital footprint.[18] The GRU-backed SANDWORM has also been an influential player as a hacker group.

John Hultquist, the vice-president of intelligence analysis at the cybersecurity firm Mandiant, said that evidence suggests, "Russia sees attacks on civilian critical infrastructure and social media manipulation as one and the same mission."

China also uses industry proxies: Chinese industry, central government, intelligence services and the military form a cohesive partnership around joint national initiatives: Belt and Road Initiative, Thousand Talents Plan, United Front Work, Military-Civil Fusion, and Three Warfare's strategy. There is no analog in the West for this degree of integrated public-private partnership on a unified national strategy.

China's Road and Belt Initiative[19] is intended to shift the balance of economic, technological, and global military power. The Thousand Talents Plan recruits leading international experts in scientific research, innovation, and entrepreneurship. United Front Work[20] gather intelligence on, manages relations with, and attempts to influence or intimidate[21], individuals and organizations inside and outside, China including within Canada, using industry, government, military, intelligence services and organized crime. China's Military-Civil Fusion Strategy[22] has companies become direct benefactors of intelligence. China's Three Warfare's strategy[23] is a political and information pre-kinetic warfare calculus of the People's Liberation Army (PLA) encompassing media or public opinion warfare, psychological warfare, and legal warfare. Huawei is a leader in the Chinese Road and Belt Initiative.
There have been well-published incidents about foreign interference by China for the past few decades. Alleged interference activities reported in the media and published academic reports have included the use of strategic disinformation, economic coercion, political kidnapping, attempts to shape and divide public opinion through social media and other means, and the targeting of Canadian citizens and institutions for espionage. In a January 2019 essay in the Hill Times, China's ambassador to Canada, Lu Shaye, claimed that Canadian anger about Beijing's kidnapping of Michael Kovrig and Michael Spavor was "due to Western egotism and white supremacy."

Recent Chinese disinformation campaigns in our country have focused on the treatment of Canadian citizens of Chinese origin, allegations of systemic racism against Canada, and tarnishing Canada's reputation in international trade. The recent "spamouflage" campaign against key figures in Canadian political and media spheres is a more directed phenomenon aimed at political influence.

DIVERGENCE AND CONVERGENCE

It is worth noting that, historically, Russian, and Chinese disinformation goals, tactics, and strategies have differed in several ways. Russian disinformation campaigns tend to be more focused on undermining democratic institutions and creating animosity and chaos. Russian disinformation campaigns are also more aggressive and provocative, with the widespread use of bots, trolls, and automated systems to amplify their message. Sometimes no one wins with Russian disinformation.

Chinese disinformation campaigns, on the other hand, tend to be more focused on promoting China's image and interests on the global stage. They often involve the use of state-controlled media outlets to promote China's achievements and downplay its weaknesses, as well as the spread of approved propaganda. Chinese disinformation campaigns also tend to be more subtle and sophisticated, with the use of selective information and narratives to shape public opinion in a more subtle and nuanced way. They are often linked to covert influence, interference, and espionage. Conversely, Russian disinformation is not well coordinated with influence, deliberate interference, or cyber espionage. While recent Chinese responses to foreign interference have shown much less maturity, there has been a shift towards covert, malign Russian-style tactics and aggressive "wolf warrior" tactics.

Another key difference between Russian and Chinese disinformation is their approach to censorship. While both countries heavily censor information and control their media, China's approach tends to be more centralized and systematic, with a focus on controlling the flow of information within the country. China has far better technical control of their information environment. Russia's approach is more decentralized and ad hoc, with the use of a range of tactics to control information and suppress dissent.

Although Russian and Chinese interests diverge in important ways, they are increasingly collaborating on the narratives being supplied to domestic audiences, feeding similar disinformation and propaganda. James Rubin, a coordinator for the Global Engagement Center and US Special Envoy, says that China spends billions on pro-Russia disinformation.[24] Much of this does not appear to be planned or coordinated. Rather we see an alignment of Chinese information operations in direct support of Russian narratives and objectives.

CANADA – THE PERMISSIVE TARGET

Both Russia and China have been actively influencing and interfering in Canadian affairs for decades .[22 26]

Russian operatives were found to be spreading false information on social media platforms during the 2019 Canadian federal election to undermine the process. The disinformation was reportedly aimed at both right-wing and left-wing groups, with the intention of exacerbating existing tensions and disrupting the democratic process.

Further, a 2020 Global News report claimed that a network of websites linked to Russia had been spreading misleading information about COVID-19 in Canada[27]. The report alleged that the websites were spreading conspiracy theories and misinformation about the origins and spread of the virus, as well as promoting unproven treatments and remedies. A report by the Council of Canadian Academies reported that COVID-19 misinformation contributed to more than 2,800 Canadian deaths and at cost $300 million[28]. That is four times the number of Canadians who have died in wars since World War II. In short, disinformation can kill.

The Conversation reported, "Canadians are being exposed to pro-Kremlin propaganda. Slightly over half of Canadians (51 per cent) reported encountering at least one persistent, false claim about the Russia-Ukraine war on social media pushed by the Kremlin and pro-Kremlin accounts[29]. The most prevalent claim, encountered by 35 per cent of Canadians, was [that] Ukrainian nationalism is a neo-Nazi movement."

According to the National Observer[30], "homegrown protesters who participated in Canada's so-called Freedom Convoy last year were aided by the Russian state-funded propaganda outlets to exploit their grievances, amplify social divisions and delegitimize the Trudeau government." Ironically, the Chinese government has allegedly been trying to get the Liberals elected at the same time.

Proxy sites play an important role in the spread of disinformation. The US State Department identified the Montreal-based Global Research platform as major kremlin-aligned proxy amplifying Russian propaganda and disinformation. The CBC reported that global research, "offers an ever-expanding collection of conspiracy theories, such as the myth that the 9/11 attacks and COVID-19 pandemic were both planned to control the population[31]. The website also hosts articles experts have attributed to a Russian spy agency."

The Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE) have both made their concerns public of how Russian state-sponsored disinformation campaigns are distorting Canada's effort to help Ukraine defend itself. Russian disinformation is considered a serious threat to democratic societies, as it can undermine public trust in institutions and create division among citizens.

FAR LEFT AND RIGHT

The recent joint report by the Centre for Artificial Intelligence, Data, and Conflict (CAIDAC) investigated Russian weaponization of Canada's far right and far left.[32]

The research found that the far right and far-left communities in Canada are increasingly polarized and their rhetoric has been shifted from differences over policy to framing opponents as enemies who pose an existential threat to the country. The far right and far-left networks in Canada are among the most active online political communities. Russian-aligned networks produced twenty-seven times more content and three times as much engagement with Canadian Members of Parliament than from legitimate Canadians.[33]

Researcher Marcus Kolga, founder of Disinfowatch, writes that the Russian government continually monitors Western societies for divisive issues to exploit. Once such issues are identified, Russian mouthpieces and proxies inject and amplify these narratives in our information environment to intensify political divisions.[34]

Analysis found that Russian influence operations integrated sophisticated narratives with incendiary images and videos tailored to Canadian audiences - and average Canadians unwittingly amplify Russian influence operations. The responsive nature of the campaign to trending issues, as well as the breadth and volume of the narratives produced, suggest a well-funded effort by the Russian government and its proxies. Pro-Russian accounts ramped up influence operations in Canada three months before the invasion [of Ukraine] and built a supportive ecosystem.[35]

CASE STUDIES

OLYMPICS

Russia launched a no-holds-barred attack against Montreal-based World Anti-Doping Association (WADA) after the 2014 Sochi Olympics. These efforts involved disinformation, influence, intimidation, coercion, slander, and cyber attacks. In 2018 the US Charged Russian GRU officers with international hacking and related influence and disinformation operations.[36] Conspirators included a Russian intelligence "close access" hacking team that travelled abroad to compromise computer networks used by anti-doping and sporting officials.

AGRICULTURE

China continues to threaten the Canadian agriculture sector and food safety through espionage, deliberate interference, influence, misinformation, and state sponsored hacking.[37] In 2019, China falsely claimed that they found ractopamine in a batch of pork products exported from Canada. The Canadian Food Inspection Agency (CFIA) and RCMP investigated the assertion[38] and found the claims to be baseless; worse, the export certifications had been forged. Similarly, China spread disinformation that its inspectors have found pests in samples of Canadian canola[39]; it is a well-known fact that this is the number one cash crop for many farmers across the Prairies. China imported $2.8-billion worth of Canadian canola annually – amounting to about 40 per cent of Canada's exports of the crop. When disinformation doesn't kill, it can have profound financial damage.

Countermeasures

The Government of Canada has taken steps to address concerns about foreign interference, including the creation of a dedicated task force and the passing of legislation to strengthen election security and foreign interference prevention. It remains to be seen whether covert Russian and Chinese operatives will be signing into Canada's foreign influence transparency registry,[40] any time soon.

It is recognized that some of the most evolved initiatives to actively counter foreign disinformation, influence, and interference is being led by the private sector - industry, security research and academics, investigative journalists, and civil society.

Countermeasures are being applied at four strategic points: audience, message, infrastructure, and malign actors.

Audience

Building resiliency within the target audience starts with security awareness education, critical thinking and promoting access to authoritative sources of information. Fact-checking, media literacy programs and increased transparency in social media advertising can help the audience make informed decisions.

Message

We can tackle toxic messaging with content-based spam filters supported by Artificial Intelligence (AI), debunking/pre-bunking of posts, and suspending accounts of malign influencers. Counter-narratives are highly effective but should always be truth-based as part of an Information Peacekeeping Strategy (IPK) or global peace and stabilization operation.

Infrastructure

Disinformation campaigns rely on cyberspace to propagate and amplify their message with semantic botnets. Cyberspace also offers an effective means to hide through obfuscation and non-attribution networks. Enumerating global foreign disinformation infrastructure requires effective open-source intelligence and targeting resources. Ultimately, taking down malevolent infrastructure has been a more effective strategy than chasing billions of toxic messages consumed by a target audience.

Malign Actors

The threat actor sits at the top of the food chain. Whether that is a hostile intelligence service (HOIS) or paramilitary organization, troll farms or person-of-influence, targeting the threat actor requires strong attribution substantiated with sophisticated intelligence. This is worth the effort: effects can include sanctioning companies and individuals, freezing assets, dismantling financial networks, disrupting command and control, maintaining persistent engagement, or following through with indictment and prosecution. Industry has been actively disrupting and dismantling adversary networks, exposing and prosecuting actors effectively for quite some time.

Conclusion

Russian and China operate vast, complex, and sophisticated disinformation ecosystems that are principally outsourced through industry proxies. The two nation-state actors and their proxies have been sharing disinformation tactics, techniques, and procedures (TTP) while simultaneous contrary running campaigns, indicating that the system is somewhat decentralized if not chaotic - hence not easily targeted.

Disinformation is often discoverable with open-source intelligence (OSINT) and countered with open effects. Consequently, supplemental to actions by government entities, the private sector can continue to play a central role in countering foreign disinformation, influence, and interference. Key points will be to:

- Build audience resiliency, through awareness, education and critical thinking;
- Create and disseminate truth-based counter-narratives to debunk/pre-bunk dis/mis/mal-information;
- Enumerate and take down malicious infrastructure; and
- Target, expose, sanction, and prosecute malign actors.

State actors such as Russia and China will be using increasingly sophisticated means to propagate disinformation in and about democracies such as Canada. Countering such disinformation and foreign interference affecting Canadians is a team sport requiring collaboration and coordination between the government and the private sector.

References

1 The Canadian Forces Information Warfare Conceptual Framework developed by LCdr Robert Garigue, Ph.D., in 1994, as the deputy commander of the Canadian Forces Information Operations Group (CFIOG), prophesized of semantic warfare and cyber deception in-depth. The concepts remain valid today. Dr. Garigue went on to become the Chief Security Officer of Bell Canada and one of the highly recognized cyber security visionaries of the time.

2 National Post. 7 April - Beijing apologists have conjured a racist bogeyman. It's total nonsense, Terry Glavin, Published Mar 31, 2023, https://nationalpost.com/opinion/beijing-apologists-have-conjured-a-racist-bogeyman-its-total-nonsense

3 National Post. 7 April - Beijing apologists have conjured a racist bogeyman. It's total nonsense, Terry Glavin, Published Mar 31, 2023, https://nationalpost.com/opinion/beijing-apologists-have-conjured-a-racist-bogeyman-its-total-nonsense

4 Doublespeak - is language that deliberately obscures, disguises, distorts, or reverses the meaning of words. Intentional ambiguity in language or to actual inversions of meaning.

5 US Department of State Global Engagement Centre, Pillars of Russian Disinformation Propaganda Ecosystem https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report/

6 Ibid. US State Department

7 Treasury Sanctions Russian Proxy Wagner Group as a Transnational Criminal Organization https://home.treasury.gov/news/press-releases/jy1220

8 Russian mercenary leader's 99 calls to Putin revealed: Wagner chief Yevgeny Prigozhin's links to the Kremlin are revealed in leaked phone records and emails , Daily Mail, 14 Aug 2020 https://www.dailymail.co.uk/news/article-8627033/Russian-mercenary-leaders-99-calls-Putin-revealed.html

9 IRA Indicted by US Justice Department https://www.justice.gov/file/1035477/download

10 Adam B. Ellick and Adam Westbrook, "Operation Infektion: Russian Disinformation from the Cold War to Kanye," New York Times, 12 November 2018.

11 RUS Chief of the General Staff of the Russian Armed Forces

12 China has been waging a decades-long all-out spy war, 28 March 2023 www.foreignpolicy.com

13 Wolf warrior diplomacy is a style of coercive diplomacy adopted by Chinese diplomats during the Xi Jinping administration, noted for being confrontational and combative. The term was coined from the Chinese action film Wolf Warrior 2.

14 https://www.axios.com/2019/09/25/spamouflage-dragon-china-hongkong-social-media-campaign

15 Adversary innovation and procurement at operational tempo, Sapper Labs 11 Apr 2023 https://www.sapperlabs.com/post/adversary-innovation-and-procurement-at-operational-tempo

16 Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics 30 March 2023

17 Variants of Petya were first seen in March 2016, which propagated via infected e-mail attachments. In June 2017, a new variant of Petya was used for a global cyberattack, primarily targeting Ukraine. The new variant propagates via the EternalBlue exploit, which is generally believed to have been developed by the U.S. National Security Agency (NSA), and was used earlier in the year by the WannaCry ransomware. Kaspersky Lab referred to this new version as NotPetya

18 Ibid Guardian

19 "China's Massive Belt and Road Initiative." Council on Foreign Relations, Council on Foreign Relations, www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative. Accessed 20 Nov. 2023.

20 "United Front Work Department." Wikipedia, Wikimedia Foundation, 22 Nov. 2023, en.wikipedia.org/wiki/United_Front_Work_Department.

21 Sidewinder: Chinese Intelligence Services and Triads Financial Links in Canada, www.primetimecrime.com/Articles/RobertRead/Sidewinder%20page%201.htm. Accessed 22 Nov. 2023.

22 "The Chinese Communist Party's Military-Civil Fusion Policy - United States Department of State." U.S. Department of State, U.S. Department of State, 1 Dec. 2020, 2017-2021. state.gov/military-civil-fusion/index.html

23 "China's 'Three Warfares' in Perspective." War on the Rocks, 30 Jan. 2018, warontherocks.com/2018/01/chinas-three-warfares-perspective/.

24 "China Spends Billions on Pro-Russia Disinformation, US Special Envoy Says." The Guardian, Guardian News and Media, 28 Feb. 2023, www.theguardian.com/world/2023/feb/28/china-spends-billions-on-pro-russia-disinformation-us-special-envoy-says.

25 "Some Politicians under Foreign Sway: CSIS | CBC News." CBCnews, CBC/Radio Canada, 23 June 2010, www.cbc.ca/news/politics/some-politicians-under-foreign-sway-csis-1.909345.

26 Chiu, Joanna. "Chinese Interference in Canada? Chinese Canadians Say They Reported It for Years - and Were Ignored." Toronto Star, 6 Mar. 2023, www.thestar.com/politics/federal/2023/03/06/chinese-interference-in-canada-chinese-canadians-say-they-reported-it-for-years-and-were-ignored.html.

27 Stewart, Ashleigh. "The Great Covid-19 Infodemic: How Disinformation Networks Are Radicalizing Canadians - National." Global News, Global News, 27 Dec. 2021, globalnews.ca/news/8450263/infodemic-covid-19-disinformation-canada-pandemic/.

28 "Covid-19 Misinformation Cost at Least 2,800 Lives and $300m, New Report Says | CBC News." CBCnews, CBC/Radio Canada, 27 Jan. 2023, www.cbc.ca/news/politics/cost-of-covid-19-misinformation-study-1.6726356.

29 Philip Co-director and Senior Researcher, et al. "Russian Propaganda Is Making Inroads with Right-Wing Canadians." The Conversation, 11 Apr. 2023, theconversation.com/russian-propaganda-is-making-inroads-with-right-wing-canadians-186952.

30 Russia used state-funded propaganda outlet to whip up support for the 'Freedom Convoy' and undermine the Trudeau government By Caroline Orr | Analysis | February 10th 2023, https://www.nationalobserver.com/2023/02/10/analysis/russian-propaganda-freedom-convoy-disinformation

31 Canadian professor's website helps Russia spread disinformation, says U.S. State Department, Oct 2020, https://www.cbc.ca/news/science/russian-disinformation-global-research-website-1.5767208

32 Centre for Artificial Intelligence, Data, and Conflict (CAIDAC), by the University of Maryland College of Information Studies and Digital Public Square March 2023 - Enemy of my enemy – investigated Russian weaponization of Canada's far right and far left to undermine support to Ukraine https://www.tracesofconflict.com/_files/ugd/17ec87_c9aa91bdc83f4f0498b4b0123ed33d5e.pdf

33 Ibid CAIDAC

34 Marcus Kolga, "Confusion, Destabilization and Chaos: Russia's Hybrid Warfare Against Canada and Its Allies," Canadian Global Affairs Institute, October 2021.

35 Ibid CAIDAC

36 "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations." Office of Public Affairs | U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations | United States Department of Justice, 13 July 2022, www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

37 Cyber Barn Raising, cskacanada.ca/wp-content/uploads/2023/03/CSKA-CyberBarnRaising-FIN-digital.pdf. Accessed 21 Nov. 2023.

38 D'Amore, Rachael. "Canada Wants Proof of Chinese Claims That Fake Certificates Used to Ship Pork: Carr - National." Global News, Global News, 26 June 2019, globalnews.ca/news/5433257/canada-investigating-china-certificates-pork-ban/.

39 "'We Still Haven't Found Any Kind of Pest': Canada Presses China over Contaminated Canola Claims | CBC News." CBCnews, CBC/Radio Canada, 12 Mar. 2019, www.cbc.ca/news/canada/calgary/china-canola-pests-bibeau-calgary-chamber-1.5053283.

40 Canada, Public Safety. "Government of Canada." Canada.Ca, / Gouvernement du Canada, 10 May 2023, www.canada.ca/en/services/defence/nationalsecurity/consultation-foreign-influence-transparency.html.

AUTHOR

Dave McMahon

Dave McMahon is the chief intelligence officer of Sapper Labs Group, and former co-chair interdepartmental committee on information warfare and psychological operations. This article was commissioned and published by the University of Ottawa's Information Integrity Lab.