Cognitive Warfare: Securing Hearts and Minds

DANIEL NIKOULA, DAVE MCMAHON | JULY 2024

uOttawa

Laboratoire sur l'intégrité de l'information

Information Integrity Lab

"In Cognitive War - The Weapon is You!"

— Dr. Zack Rogers

EXECUTIVE SUMMARY

This article, produced and published by the Information Integrity Lab, explores the complex terrain of cognitive warfare, encompassing tactics such as information manipulation, cyberattacks, and narrative shaping to sway public opinion and undermine trust. With the rise of digital technology, adversaries such as Russia and China have sought to exploit social media and online platforms disseminating disinformation and sowing discord. The rise of cognitive warfare has placed pressure on Canada and its allies to develop an understanding of the threat, and to develop countermeasures including bolstering cyber defenses, promoting media literacy, and fostering resilience against information manipulation. Understanding the dynamics of information and perception is crucial to protect against the evolving threats of cognitive warfare. Collaboration amongst governments, tech companies, and civil society is integral to combat adverse cognitive strategies — disinformation principally among them — and to safeguard democratic institutions.

Daniel Nikoula is an Analyst at the University of Ottawa Information Integrity Lab.
Dave McMahon is an Associate of the University of Ottawa Information Integrity Lab.

INTRODUCTION

Cognitive warfare (CW) is a varied concept encompassing information operations, cyber capabilities and strategic communication, but is typically defined as the "use of the means of action that a state or an influential group makes to manipulate the spontaneous mechanisms of the cognition of an enemy or its people, in order to weaken, penetrate, influence, or even subdue or destroy it."[1] This includes the use of psychological tactics, information manipulation, and cognitive strategies (narratives, semiotics, iconographies) to influence emotions, beliefs, perceptions, and behaviours of individuals, groups, or whole populations. In essence, cognitive warfare represents a combination of "psychological-social-technical warfare" and "influence warfare" through cyber means.[2]

Psychological operations, influence and deception tactics have existed as long as human warfare. The preeminent military strategist of his time, Chinese general Sun Tzu famously wrote in The Art of War that "all warfare is based on deception." He notes that a great military leader is not necessarily one who wins many victories in the field but one who achieves his aims without making resort to violence in the first measure. The means of achieving a bloodless victory — subversion, stealth, and subterfuge — have evolved over time, primarily being used in asymmetrical conflict where a weaker force opposes a conventionally stronger one.

Today, the world's populations are bombarded with overwhelming sums of information, much of which is false or misleading. Although the use of false or distorted information to gain advantage over one's opponent is not new, the relative weight and presence of such methods has risen considerably in recent years with information warfare reaching never-before-seen levels[3]. The rise of mass media has made the human mind more susceptible to malign influences while eroding people's ability to make informed choices.

In CW, the human mind forms the battleground. CW primarily targets cognition, which is "the mental process of acquiring and comprehending knowledge, as well as interpretation and perception of information."[4] Building on psychological warfare of the past which employed propaganda in to target emotions, CW harnesses advance modern technology to "exploit biases or mental automatisms, [provoking] distortions of representations, alterations of the decision or even inhibitions of action, and to bring about disastrous consequences, both at the individual and the collective level."[5] Unlike conventional (or kinetic) warfare which utilizes physical violence, destruction, and territorial conquest, CW operates in the realm of ideas, emotions, and perceptions. Recalling Sun Tzu, CW seeks to exploit the vulnerabilities of the human mind in an attempt to "win the war before the war."[6] While conventional capabilities — which aid in seizing and holding territory through overwhelming force — may determine tactical or operational outcomes, securing the cognitive domain (the human mind) is essential for achieving a lasting victory. Recent kinetic conflicts have underscored the importance of this maxim.

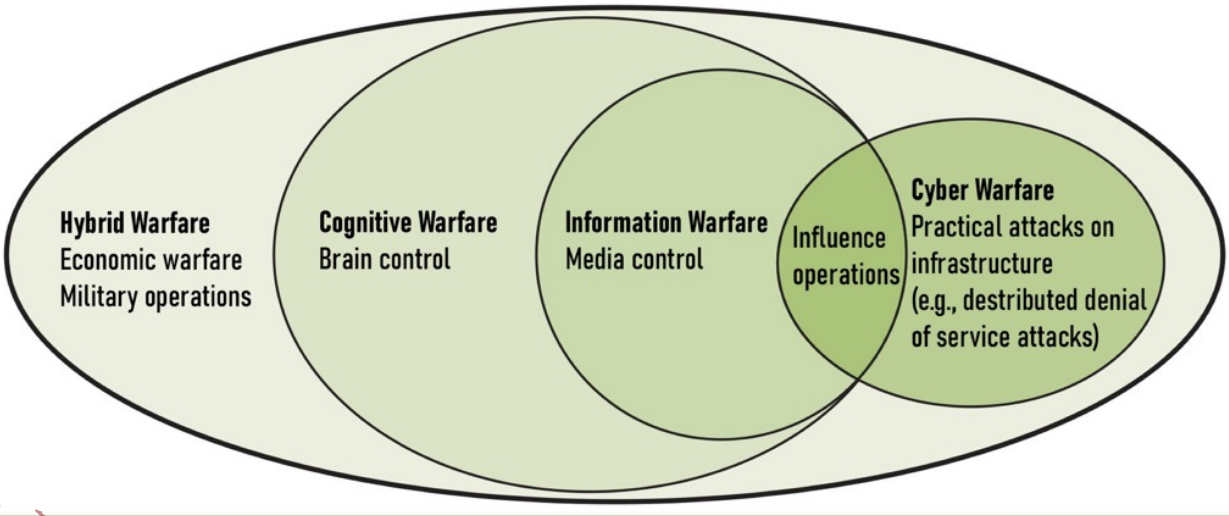

Figure 1. Cognitive Warfare Conceptual Relationships[17]

Defending Canada in an Age of Cognitive Warfare

Although covert influence groups (like extremist organizations) are employing CW techniques as means gaining influence, achieving their strategic goals and compensating for their lack of conventional military power, state actors continue to wield the most significant resources for crafting and deploying such strategies, particularly in the domains of foreign interference operations and hybrid warfare. Canada and its allies have become the focus of malign attention from two prominent state actors: Russia and China.

The Bear (Russia)

Russia has systematically learned to use the principles of liberal democracies against them by weaponizing information. This now forms a vital part of the Kremlin's concept of "non-linear" war, which encompasses many elements of CW.[7] In the past, Russia has used non-kinetic activities such as targeted propaganda and disinformation campaigns to propagate its narratives abroad. The country's around-the-clock, multilingual channel Russia Today (RT) operates in over 100 countries — including, until recently, Canada. Its effects are far-reaching as "receivers of Russian-aligned disinformation experience deterioration in their ability to identify fact from fiction, decaying their mental resilience, and with potential long-term impact, such as loss of trust in media."[8]

The Role of Disinformation in CW

Disinformation, which is verifiably false information that is created and spread intentionally in a bid to confuse, manipulate, or mislead is being increasingly deployed as part of CW strategies: presenting a serious threat to the national security of Canada and its allies.[9] The creation and dissemination of disinformation is a primary method for CW as it involves fabricating alternative realities and the dilution of truth as a referential concept. This has the effect of confusing people, making them more susceptible to buy into conspiracy theories and falsehoods. The exploitation of people's cognitive biases, a major focus of CW, can drive them to strongly identify with a particular thought group and create in them a hostility towards other people, groups or institutions who do not align with their conformist worldview. If left unchecked, this cognitive siloing can lead to societal discord, polarization and instability. Over the last few years there have been countless examples of state and non-state actors using disinformation to interfere in elections, undermine scientific and medical consensus, sow societal division and destabilize economies have forced democratic countries to recognize disinformation as a serious and ongoing nation security threat. Jens Easterly, Director of the U.S. Cybersecurity and Infrastructure Security Agency, has been quoted as saying "the most critical infrastructure is our cognitive infrastructure, so building that resilience to misinformation and disinformation, I think, is incredibly important."[10] His admission reflects the increasing recognition of CW in public policy circles and in NATO countries as a separate domain which merits serious attention.

Disinformation amplifies the frequency and coverage of falsehoods. The goal is to build an audience willing to first buy into and then re-propagate a falsehood. Attacks against the cognitive domain amalgamate cyber, disinformation, psychological, and social-engineering capabilities. CW positions the mind as a battle space and contested domain. Its objective is to sow dissonance, instigate conflicting narratives, polarize opinion, and radicalize groups. Cognitive warfare can motivate individuals to act in ways that may disrupt or fragment an otherwise cohesive society. The ensuing disorder can influence decision-making, change ideologies, and generate distrust among Allies.

The next generation disinformation operations have the potential to render serious cognitive damage. These include the rapid spread of "deepfakes": videos which seek to create the illusion of an individual doing or saying something with face-transplant technology. Even with the technology in its relative infancy, these videos can be convincing. Additionally, audio-only versions of this same faking technology — such as the so-called AI application — are also seeing further development. Social media networks such as Facebook and TikTok have already launched campaigns to ban deepfake content.[11] The harm potential of fake content carries seismic concerns for truth advocates. Even if fake content can be revoked or removed from an online platform, corrections and reversals rarely reach those who viewed the original content.

As noted in the Canadian Security Intelligence Service's (CSIS) recent report on Foreign Interference Threats to Canada's Democracy, that Russian CW activities aim to subvert democracy through polarization[12] including by exploiting pre-existing fissures in society. In terms of reach, before the Canadian Radio-television and Telecommunications Commission (CRTC) removed RT's authorization for distribution in the country in 2022, it is estimated that over 100,000 Canadians watched RT daily[13][14]. At the outset of 2022, RT precisely covered developments in the Freedom Convoy protest and emphasized inflammatory narratives — a well-developed tactic of information and cognitive warfare dubbed "anything that causes chaos.[15] Furthermore, the research by Canadian NGO Disinfowatch demonstrated that Russian information activities demeaned Canadians of different communities while exploiting "negative emotional reactions to sensitive issues like residential schools, the environment and anti-LGBTQ issues."[16] Russian propogandists pay close attention to local sensitivities seeking to use Canada's support of multiculturalism against it. Russia's strategy of identifying and exploiting wedge issues which pit communities against each other or the government, is a particularly acute threat to a country as diverse as Canada.

Having become internationally isolated by the West after its invasion of Ukraine, Russia has retreated into itself. Faced with constraints on its equipment and ability to operate beyond its geographical neighborhood, it has been increasingly pivoted to using disinformation campaigns as part of a strategy to promote disunity amongst its adversaries. Building on an expanded network of troll farms, botnets, and hackers, Russia actively pushes disinformation against individuals and communities to sow division and cripple Western resolve in backing Ukraine.

The Dragon (China)

As Russia looks to re-establish itself as a major world player in a multipolar world, China, uses its growing influence to seek economic and political advantage and weaken the confrontational resolve of its adversaries.[17] China's "Three Warfares Strategy" is a form of CW incorporating media, legalistic, and psychological warfare. This strategy does not merely mimic Russia's playbook regarding propaganda and disinformation; rather, China continues to craft its own approach, leveraging advanced technology and its human resources. For instance, the United Front Work Department (UFWD), directly overseen by the Central Committee of the Communist Party of China (CCCPC), actively targets audiences abroad. The Chinese diaspora in Canada has weathered influence operations and intimidation from Chinese authorities and their proxies. Organizations such as the Chinese Students and Scholars Association (CSSA) operate within Canadian universities, working to advance political objectives. Additionally, the People's Liberation Army Strategic Support Force (PLASSF) of the People's Liberation Army (PLA) is responsible for executing influence and psychological operations.

Chinese state media represents the "central kitchen" model of content distribution across media outlets and social media platforms. Its content is amplified by a wide network of public-private partnerships. Companies like Spamouflage, Onesight, Nothing Technologies, Urun Big Data Services, Chinaii, and others are implicated in the government's censorship and propaganda campaigns, boosting propaganda and disinformation abroad using semantic botnets[ii]. A private sector analysis echoed by the Canadian Centre for International Governance Innovation highlighted that "Canada's national security is directly impacted by elements of current Chinese policies, including China's conduct of espionage, aggressive use of cyber power, willingness to engage in hostage diplomacy, and efforts to interfere with our democracy and society." [18]

In its recent investigative report, Disinfowatch has issued a stark warning regarding the concerning tactics utilized by the Chinese government to advance its interests in Canada. According to the report, in addition to tactics such as hostage diplomacy, interference with democratic processes, this includes concerted efforts to manipulate public opinion through widespread disinformation campaigns.[19]

Of particular concern is the revelation regarding Huawei's campaign to influence Canadian public opinion. According to the report, Huawei Canada maintains a dossier of individuals, including politicians, university professors, lawyers, and business figures, whom it identifies as key opinion leaders. These individuals are believed to be targeted for their potential to support Huawei's agenda and assist in influence campaigns aimed at inserting Chinese technology into critical information infrastructure within Canada.

Such activities not only pose a significant threat to the integrity of Canadian democracy but also undermine public trust in democratic processes and institutions. The use of these tactics underscores the urgent need for heightened vigilance and robust countermeasures to safeguard Canada's sovereignty and national interests against foreign interference.

Closer to its borders, China uses CW as means of inducing favorable conditions for Chinese unification with Taiwan. Chinese CW utilizes gray zone activities aimed at legitimizing challenges to the existing international order and rules-based systems among Chinese audiences. China promotes narratives alleging US provocations and incitement of conflict in the Taiwan Strait, alongside portrayals of the Government of Taiwan as an aggressive actor. These tactics aim to create conditions conducive to Chinese unification with Taiwan, potentially through kinetic means. They exploit vulnerabilities inherent in liberal democracies, including the lack of consensus on defining war and clear thresholds for unacceptable behavior among like-minded countries such as Taiwan and the G7.

The Alliance (NATO)

As the world's premier military Alliance, NATO has taken an interest in studying CW and beginning to develop collective action counter-strategies. NATO recognizes that its adversaries are becoming adept at using hybrid and unconventional warfare that combine kinetic, cyber, and cognitive elements to achieve their aims. On the disinformation front, the alliance actively monitors traditional media and online platforms to understand the narrative landscape and respond effectively to emerging challenges. NATO's Innovation Hub manager, LCol François du Cluzel has cautioned that "cognitive warfare [is being] used by adversaries to undermine trust, and to weaken, interfere with, and destabilize a target population, institutions, and States in order to influence their choices."[20] Future conflicts will likely occur amongst digitally connected peoples rather than those in geographical proximity to hubs of political, military and economic power.

In the context of military challenges, NATO describes CW as the "Invisible Threat" and warns of "adversarial attempts to manipulate Alliance members." NATO literature affirms that "the goal of cognitive warfare is for an adversary to destroy their target from within, rendering them unable to resist, deter, or deflect – thereby allowing the perpetrator to follow through with their own agenda." (citation) NATO discussions suggest that the primary objective is to cultivate trust, while acknowledging that adversaries employ cognitive warfare strategies aimed at undermining public institutions and shaping public or governmental policies. These tactics facilitate the proliferation of discontent within a society, fostering particular ideologies and behaviours. Despite its influence, significant work remains for NATO to gain cognitive superiority over its adversaries.

The Alliance is in the process of developing a dedicated Cognitive Warfare Concept, scheduled for release later this year (2024). This includes fostering a collective understanding and individual capabilities and the advancement of cognitive operations within the security alliance of 32 states — a task that will necessitate "a sustained cooperation between Allies in order to ensure an overall coherence, to build credibility, and to allow a concerted defense."[21] Moreover, the NATO Science and Technology Organization (STO) has endorsed a variety of Exploratory Teams (ET) and Research Task Groups (RTGs) on the subject.[22]

According to the Alliance, cognitive superiority over adversaries has three main pillars: awareness, understanding, and advantage. The first of the three, awareness, involves "acquiring, storing and exploiting information, data, and intelligence through multiple means."[23] It extends beyond the awareness of the strategic capacities of allies and adversaries to measure and understand the cognitive state of individuals in real time. Understanding includes "the long-term vision and strategy; strategic culture, behaviour, and operational art; long-term warfare development trajectory and technological focus; command and control arrangements and the like" (ibid). In simple words, it is making sense of the intentions of different actors.

Accounting for the significance of emerging technologies and the challenges and opportunities they present, the NATO Communications and Information Agency has launched strategic initiatives focusing on Artificial Intelligence (AI) and Cybersecurity Horizon Scanning. Additionally, NATO has launched research and technology groups to study this question and to understand how information manipulation influences allies' populations.[24]

At Home – Canada The Canadian Armed Forces (CAF) sees CW as a distinct and emerging threat, recognizing that the "digital age has re-oriented the rules of confrontation and rendered previously defensible borders vulnerable to incursions of a different kind"[25] and that "an adversary can attack below the threshold of armed conflict, shifting the 'battlefield' of a conventional war to a narrative war that is contested within the minds of a population."[26] The latest defence policy update released in April of this year outlines that: "Strategic competition between states is a path to major power conflict. Intensifying environmental crises, driven or augmented by climate change, and threats posed by disinformation".[27] However, Canada's approach to cognitive operations has long been largely treated as an extension of CAF public affairs rather than being treated as an integrated, joint requirement. malign below threshold activities, including cyber-attacks, disinformation, and foreign interference require new approaches to national defence".[28]

Based on publicly available information, the CAF's cognitive infrastructure is built around 10 Influence Activity "companies" which support 10 Canadian Brigade Groups within a four-division structure. Furthermore, there exists an Influence Activity Task Force within the 5 Canadian Division (Boudreau). The launch of the Canadian Centre for Cyber Security as part of the Communications Security Establishment (CSE) marked a positive development on the path to countering adverse CW activities. Given that many bad actors use cyber capabilities to influence political decisions, the Centre aims to protect Canada's information system and assets. In 2021, the Centre co-hosted NATO's Innovation Challenge, entitled The Invisible Threat: Countering Cognitive Warfare. Additionally, the Canadian Department of National Defence's Innovation for Defence Excellence and Security (IDEAS) program was established in 2023. It seeks to bring together innovators and find solutions to technological challenges of the future, including those that may affect perceptions on the battlefield and beyond.[29]

Lastly, the government has announced a $5.5 million investment through the Canadian Heritage Digital Citizen Initiative to create the Canadian Digital Media Research Network (CDMRN). The Network "will further strengthen Canadians' information resilience by researching how quality of information, including disinformation narratives, impact Canadians' attitudes and behaviors and by supporting strategies for Canadians' digital literacy."[30] These are all necessary steps to start countering CW operations at home while developing a foundation which can be built upon in the coming years.

Future of Cognitive Warfare

New advanced technologies accelerate traditional CW strategies in speed, scope, and scale. Any influence activity involves a thorough understanding of the target audience. Social networks, AI, and big data represent vital high ground for CW. Specifically, bad actors take advantage of populations' digital behavior by scraping large amounts of personal data, individual networks, their preferences, and their vulnerabilities. Modern AI programs have facilitated data collection and analysis processes at an unprecedented scale. Additionally, adversaries engage in cyber attacks on information systems in order to obtain sensitive state information. Such attacks serve a further purpose: to gain insight into the target state's knowledge and capabilities while undermining trust in its utilities and ability to protect itself and its citizens.

Information-facilitated cognitive influence also exploits social networks and human psychology. Several social cognitive theories explain how this information spreads and influences social media users. Among these are the uses and gratification theory, social capital theory, and social cognitive theory. Simply put, electronic word of mouth — supported by algorithms — can reach a large number of individuals in a short amount of time.[3132] Social media facilitates instant interactions and responses, offering an accessible platform for those seeking to gain influence. As a result of such engagement and the urge to stay relevant and visible, social media prompts users to share content, often without an assessment of its credibility.

CW actors have now begun using AI-created synthetic media, including those generated in war-related contexts in Ukraine and Gaza. These can take the form of doctored visual or audio files which misrepresent military and state leaders, sowing chaos among populations. Cognitively, visual deception is far more impactful owing to a concept known as the "realism heuristic." Experiments conducted by University of Ottawa professor Doris Graber in the 1990s demonstrate how visuals influence the formation and retrieval of memories — effectively, "seeing is remembering." Individuals tend to recall visual images more readily, even if they do not remember their source. This underscores another cognitive risk posed by technology. Even if promptly debunked, deepfakes can still quickly travel on social media and, in the long run, "may contribute to a state of generalized indeterminacy."[33] The hardware can induce strong negative emotions to encourage specific actions, collect large amounts of biometric data to calibrate cognitive attacks, and create false memories.

More efficient CW campaigns are emerging from the optimization of human-machine interactions. AI can adeptly fill any gaps based on publicly available information, thus enhancing its ability to understand human behavior and adapt responses.

Lastly, new-age CW methods integrate neuroscience and psychology to enhance its effectiveness. These techniques could profoundly impact decision-making, trust, and performance: providing CW actors an edge in neutralizing their opponents. Such tactics fall under the threshold of traditional warfare, devoid of kinetic activity. Furthermore, neuroscience-related methods lie beyond the scope of current international law, complicating efforts to regulate its use.

Solutions and Recommendations

It is clear that in modern warfare the role of soft power and influence, especially in the cognitive domain, is becoming increasingly important. Continued technological advancements necessitate a greater understanding of CW methods, techniques, and effects. Countering CW operations will become a core aspect of the national security and defense strategies of Canada and its allies. The proliferation of CW highlights the need for Canada and its NATO partners to adopt an assured defense posture which incorporates new counter-strategies and security measures. Such measures are especially required given the wide-ranging harms of CW on society, industry, and against individuals who find themselves targeted by cognitive attacks which bypass traditional military defenses.

An outstanding challenge has been in linking the cognitive (semantic), cyber, and physical domains in a coherent fashion that provides defence-depth and threat reduction. Detecting a compromise of the mind is a difficult task as these compromises occur on a subconscious level. Malign actors take extraordinary precautions to disguise their activities, identity, and methods, often conducting CW through the use of techniques such as back-stopped aliases, non-attributable (untraceable) networks, double fast-flux networking, sock puppets, and semantic botnets. Conventional security doctrine, plans, and standards do not address the tactics used in CW. Cognitive attacks can also "jump air gaps" in every secure network. This means that conventional security measures like walled gardens and firewalls become ineffective. In this sense, CW has no geographic borders or time boundaries.

Conventional approaches to CW view it as a uniquely social problem, when in fact the solution requires multi-domain expertise and capabilities. As the report Reimagining a Canadian National Security Strategy put it, "In the end, we cannot legislate our way out of a misinformation/disinformation problem."[34] Unraveling malicious CW activities requires multisource intelligence and deep analytics supported by talent, technologies, tradecraft, and the ability to operate clandestinely across network and human domains. Countering adversaries requires operational security, stealth and sophisticated ancillary infrastructure. Hence, "*Western militaries must work more closely with [the private sector], social and human sciences [to] help the alliance develop its cognitive warfare [defence] capacities.*"

Intelligence analysis, as a method of collecting, analyzing, and turning information into actionable intelligence, will be key in preventing and combating CW. It can do so in the following ways:

- Creating a database of the most common cognitive warfare tactics and categorizing them by different malign actors;
- Monitoring information sources and their authenticity;
- Using technologies to analyze and verify data authenticity;
- Cooperating with other agencies to share critical information;

However, in the modern age, one cannot effectively detect, defend, or deter cognitive attacks without a strong open-source intelligence program and robust assessment capabilities. Threat hunting, end-entity attribution, and the enumeration of the technical networks behind information campaigns are also necessary before advancing a counter-narrative. The answer to cognitive warfare will be rooted in skilled orchestration of human-led, technology-accelerated analytics consisting of key components[iii]: Building open-source programs within the closed cultures of the intelligence community brings its own challenges: particularly when a mature OSINT industry already exists. In many ways, the private sector played an important role in counter-radicalization, influence, and filtering mis/disinformation on the global stage, at scale, for decades. NATO's adversaries outsource their disinformation and CW operations.

This solution will require a unified platform and a collaborative analytical environment capable of processing big data and common training. Building open-source programs within the closed cultures of the intelligence community brings its own challenges: particularly when a mature OSINT industry already exists. In many ways, the private sector played an important role in counter-radicalization, influence, and filtering mis/disinformation on the global stage, at scale, for decades. NATO's adversaries outsource their disinformation and CW operations. Consequently, solutions must be founded on robust private-public partnerships.

The Alliance must recognize the interlinked dynamics of contemporary conflicts. To counter encroachments into the cognitive domain and guard against tactics such as psychological operations, deception, and electronic warfare, NATO must integrate cyber capabilities to interfere with or control information systems, networks, and data.

National security and societal resilience can be built by embracing a whole-of-society approach, one that combines civilian, economic, commercial, and military vectors. This approach must promote planned data collection, secure data sharing, and effective data management. The diffusion of power, disruptive technology, and the machinations of sophisticated and increasingly belligerent adversaries will generate emergent effects faster than traditional organizations can adapt to them. Solutions will require central orchestration since the issues cut broadly across domains, mandates, and missions.

Policy and legal responses to disinformation and misinformation should be adopted proportionally and with careful consideration. Addressing disinformation must account for competing values, including privacy and fundamental freedoms. In certain instances, digital blocking and takedowns may be warranted.

Ultimately, Canada and its NATO allies must counter CW including through cyber operations, identifying and disrupting disinformation networks. However, allies must be careful not to engage in black propaganda or public disinformation in order to maintain trust and adhere to democratic values.

Conducting a comprehensive investigation and decomposition of a cognitive warfare campaign waged by adversaries against NATO nations involves various crucial components, including intelligence estimation, Intelligence Preparation of the Battlefield/Intelligence Preparation of the Operating Environment (IPB/IPOE), and Target Systems Analysis (TSA) of pertinent hostile influence networks. Additionally, executing comprehensive assessments against NATO military members entails analyzing attack surfaces, assessing resilience, and determining susceptibility to full-spectrum cognitive warfare attacks, culminating in the identification of capability deficiencies.

Bolstering Allied defenses against cognitive warfare threats entails designing, testing, and trialing effective countermeasures, such as counter-influence tactics, cyber deception strategies, threat hunting methodologies, adversarial pursuit techniques, targeting approaches, threat reduction activities, and active cyber defense mechanisms.

Conclusion

In the mid-2000s, former Commandant of the U.S. Army War College Major General Robert H. Scales opined on the future of warfare: “victory will be defined more in terms of capturing the psycho-cultural rather than the geographical high ground.”[35] Revisiting this prediction in 2024 demonstrates the prescience of his statement, emphasized by outgoing Canadian Armed Forces Chief of Defence Staff Eyre on 18 July 24: "Along with the peak threat of war, the other biggest threat to our nation is disinformation. The nature of war remains, in the words of Clausewitz, a contest of human will. But if that will can be affected before the first shot is fired, there is winning without fighting. Our institutions of liberal democracy are under assault with the constant bombardment of conspiracy theories and lies that shape a narrative of distrust and decline. And these are created both within and outside the country. In communist China's three warfare strategic approach, this is called cognitive warfare. Our own institution is being targeted everyday as we see pro-Kremlin trolls tailoring their insidious propaganda to cause maximum harm--in many cases, with fabricated personal attacks". Disinformation is finding increasing purchase as part of the efforts of malicious actors to further their national interests.

The same values that make Western societies strong, openness, multiculturalism, freedom of expression, the free flow of information, also render Western societies vulnerable to cognitive attacks which employ disinformation as a mental trojan horse penetrating the perimeter of the mind and corrupting it from within. Sophisticated information manipulation techniques can wither away at the critical faculties of the citizenry. Disinformation as part of cognitive warfare directly engages with the fears, prejudices, and hatreds of people. In the face of mounting societal polarization, unrest and discord brough on by targeted disinformation, democracies like Canada must dedicate significant resource into education and shaping a public that is informed, resilient, and one that is able to discern fact from fiction through a critical media and skeptical analysis of information.

As media analyst Vasili Gatove has noted, "if the 20th century was defined by the battle for freedom of information and against censorship, the 21st century will be defined by malevolent actors, states or corporations, abusing the right to freedom of information."[36] Governance poses significant challenges as well. In the emerging future, governments must grapple with a currently realities in which power is diffused among blend of state and non-state actors. To uphold the integrity of information and fortify cognitive defences, Canada and its allies should take proactive measures that build collective resilience. The Information Integrity Lab, for its part, is playing an important role by serving as a hub for rigorous analysis and fostering constructive dialogue among leading experts. The multifarious complexities of the modern information landscape require collaboration, innovation, and, especially, informed discourse. Canada and its partners must strive to confront the challenges posed by the proliferation of CW and ensure the preservation of democratic values in a free world.

There is no single bulwark, no outer wall that the state can construct to guard against CW. The defensive walls will have to be psychological ones. Governments ought to engage citizens in thorough digital training that cultivates and sharpens their critical thinking abilities, equipping them to identify and combat disinformation as it comes to them. Proactive strategies not only boost personal resilience but also reinforce societal safeguards against manipulation and deceit. Strong measures, including those described throughout this report, are essential in inoculating populations against mental incursions and to keep democratic societies prosperous, stable, and free.

Acknowledgements

The Information Integrity Lab would like to express its gratitude to Mr. Anvesh Jain and Ms. Mariana Savka for their valuable contributions and feedback to this report.

Notes

[i] In this context, semiotics refers to signs and symbols and their use or interpretation, while iconographies refers to images and their meanings.

[ii] Semantic botnets are automated networks that use AI to create and spread disinformation.

[iii] Including: global Cyber Threat Intelligence (CTI), Open-Source Intelligence (OSINT), Social Media Intelligence (SOCMINT), human experts, active cyber defence, attribution, threat hunting, targeting, and the generation of effects with measurable outcomes.

Endnotes

1 Kimberly Underwood, "Cognitive Warfare Will Be Deciding Factor in Battle," SIGNAL Magazine, Aug. 2017.
2 Shay, Shaul. "Between Kiev and Venice the cognitive warfare and the Biennale of Venice." Security Science Journal, vol. 3, no. 2, 31 Dec. 2022, pp. 101–117
3 Kuperwasser, Y., & Siman-Tov, D. "The cognitive campaign: Strategic and intelligence perspectives." Tel Aviv: Institute of National Security Studies, 2019.
4 Ottewell, Paul. "The Disinformation Age: Toward a Net Assessment of the United Kingdom's Cognitive Domain." Expeditions with MCUP, 2022.
5 du Cluzel, Francois, "NATO Cognitive Warfare, a Battle for the Brain", NATO Allied Command Transformation. 2020.
6 Pappalardo, David. "'Win the War Before the War?': A French Perspective on Cognitive Warfare." War on the Rocks, Jul. 2022.
7 Pomarantsev, Peter, "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money", Institute of Modern Russia, 2014
8 "Cognitive Warfare: Strengthening and Defending the Mind", NATO Allied Command Transformation 2023.
9 Rutheford, Nicholas "About mis-disinformation, its potential impacts, and the challenges to finding effective Countermeasures", Information Integrity Lab, Feb. 2023.
10 Ken Klippenstein, Lee Fang. "Leaked Documents Outline DHS's Plans to Police Disinformation." The Intercept, Jul. 2023
11 Chan, Kelvin. "TikTok Bans Deepfakes of Young People as It Updates Guidelines", Associated Press News, 22 Mar. 2023, apnews.com/article/tiktok-china-cybersecurity-data-privacy-595f9ae7c0a1fc22f0b285cede6bd67c.
12 Canadian Security Intelligence Service, "Foreign Interference Threats to Canada's Democracy", 2021.
13 Government of Canada, "RT and RT France can no longer be distributed by Canadian television service providers", March, 2022.
14 Russia Today, "Distribution", https://www.rt.com/about-us/distribution/.
15 Orr Bueno, Caroline. "Russia's role in the far-right truck convoy." The Journal of Intelligence, Conflict, and Warfare, vol. 5, no. 3, 31 Jan. 2023.
16 Kolga, Marcus, "Russia's threat to Canadian democracy and the Arctic: Marcus Kolga", MacDonald-Laurier Institute, Apr. 2022.
17 Orinx, K. Tanguy Struyede Swielande. "China and Cognitive Warfare: Why Is the West Losing?" Bernard Claverie; Baptiste Prébot; Norbou Beuchler;François du Cluzel. Cognitive Warfare: TheFutureof Cognitive Dominance.,NATO Collaboration Support Office, pp.8, 1-6, 2022
18 Momani, Besma "International Security: Canada's Role in Meeting Global Threat", Center for International Governance Innovation", 2021.
19 "Chinese State Interference in Canada's 2021 Election." DisinfoWatch, Sept. 2021, disinfowatch.org/chinese-state-interference-in-canadas-2021-election/.
20 du Cluzel, Francois, "Cognitive Warfare", NATO Innovation Hub, 2020.
21 Ibid du Cluzel
22 Marsili, Marco. "Guerre à la Carte: Cyber, information, cognitive warfare and the metaverse." Applied Cybersecurity & Internet Governance, vol. 2, no. 1, 28 Dec. 2023.
23 Shay, Shaul. "Between Kiev and Venice the cognitive warfare and the Biennale of Venice." Security Science Journal, vol. 3, no. 2, 31 , pp. 101–117,Dec. 2022.
24 Claverie B., B. Prébot, N. Buchler and F. Du Cluzel. Cognitive Warfare
25 Government of Canada, "Defending Canada against cognitive warfare", Nov. 2021.
26 Ibid Government of Canada
27 Government of Canada, "Our North, Strong and Free: A Renewed Vision for Canada's Defence" Apr. 2023.
28 Ibid "Our North, Strong and Free: A Renewed Vision for Canada's Defence"
29 Government of Canada, "Cyber Attribution for the Defence of Canada", 2023.
30 House of Commons of Canada, "Standing Committee on National Defence", Feb. 2024.
31 Faiswal, Kasirye, "The Importance of Needs in Uses and Gratification Theory." Advance. May. 2022.
32 Baker, Eva, et al. International Encyclopedia of Education. 3rd ed., Elsevier Science, 2010.
33 Vaccari, C., & Chadwick, A. "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News" Social Media + Society, 6(1), 2022.
34 Shull,Aaron,Wark,Wesley, "Reimagining a Canadian National Security Strategy", Center for Internation Governance Innovation, Dec 2021
35 "The 21st Century Game-Changer: Cognitive Warfare", NATO Joint Warfighting Center, 2023.
36 Ibid Pomarantsev

Infolab.uOttawa.ca
Labinfo.uOttawa.ca