Centre for International Governance Innovation

This policy brief is part of CIGI's project on freedom of thought: Legitimate Influence or Unlawful Manipulation?

Find out more at: www.cigionline.org/fot

Policy Brief No. 6 — February 2024

Narrative Dominance, Information Warfare and the Freedom to Think

Nitin Pai

Key Points

- Information warfare involves the use of information to influence political decisions without necessarily using physical force.
- States and non-state actors are engaged in a quest for narrative dominance — to shape the landscape of public opinion in their favour.
- Liberal democracies must protect the individual freedom to think, and cognitive autonomy is a national security objective.
- There is a need for constitutional safeguards to prevent governments from directing information power against their own citizens.

Introduction

Politics is everywhere and on a perpetual quest for narrative dominance. Aphorisms from ancient practitioners of statecraft in Assyria, India and China[1] warn us that the word is mightier than the sword, that the power of knowledge is superior to force and wealth, and that to vanquish the enemy without fighting is the acme of skill. History is replete with the use of cultural power, propaganda, disinformation, deceit and censorship as instruments of policy. Information warfare — the use of information to influence decisions in order to achieve a political objective without necessarily using physical force — is not new. It has, however, become the centrepiece of international politics because we are in the Information Age, an epoch where society is structured around the production, consumption and effects of information.

This policy brief presents a high-level analysis of the external, geopolitical dimension of information warfare and offers recommendations for defence and national security policies for liberal democratic states.

1 The phrase "the word is mightier than the sword" originates in the teachings of the Assyrian royal adviser Ahiqar (circa 700 BCE) (see Matthews and Benjamin 1997). Kautilya, a political adviser in the service of Chandragupta, the founder of the Mauryan empire, places "knowledge power" as the foremost type of power in *The Arthashastra*, a classic Indian treatise of statecraft (see Olivelle 2023, chapter 6, verses 2–33). Similarly, Sun Tzu considers subduing the enemy without fighting as the acme of skill, in *Art of War* (see Kaufman 2012, chapter 3).

About the Author

Nitin Pai is co-founder and director of the Takshashila Institution, an independent think tank and school of public policy based in Bangalore, India. He teaches international relations and public policy at Takshashila's graduate programs. He writes a fortnightly column in *Mint* (livemint.com) called "The Intersection."

Nitin received a gold medal from the National University of Singapore's Lee Kuan Yew School of Public Policy, was an undergraduate scholar at Nanyang Technological University in Singapore, and is an alum of National College, Bangalore. He spent more than a decade at the Singapore government as a policy maker in the technology sector.

He is currently a non-resident senior fellow at the Institute of South Asian Studies at the National University of Singapore, and serves on the board of Jal Seva Charitable Foundation (WaterAid India).

The Pursuit of "Information Power"

Today nation-states, non-state actors, private corporations, social networks and individuals are engaged in a relentless global contest to control narratives and influence people's minds. Information warfare targets "every element in the epistemology of an adversary" (Szafranski 1995). Freedom of thought, therefore, is the bedrock of defence and a crucial aspect of human security. It follows that securing the freedom of thought is a national security objective that states are charged with and responsible for. Freedom of thought is thus both the most fundamental of rights and the most important of interests that governments must secure against external and internal threats.

Recommendations

- → Consider citizens' freedom of thought as a national security objective.
- → Protect the cognitive autonomy of individual citizens, unfettered public discourse and the policy autonomy of its leadership.

Who Will Watch the Watchers?

States pursue narrative dominance by conducting warfare in the information domain. This can be done by manipulating people's thoughts (cognitive warfare), hacking the machines they use to communicate (cyberwarfare) or damaging physical targets (kinetic warfare). Propaganda, for instance, is an example of a cognitive operation, while compromising a country's banking network is a cyberattack. Terrorist attacks, missile tests and military exercises are kinetic operations carried out to achieve psychological objectives. Destruction itself is rarely a political objective. Rather, it is a means of forcefully imposing the destroyer's narrative on the target population. Information warfare employs perceptual or psychological force to target human minds.

States should thus have sufficient information power to prevail over their external adversaries.

However, this brings up a fundamental conundrum: How do we ensure that they do not abuse this power to influence their own citizens? The old challenge of *quis custodiet ipsos custodes* (translated as "who will guard the guardians?" or "who will watch the watchers?") has acquired new salience in contemporary society. A state that succeeds in making its citizens believe in false propaganda not only violates the rights of its citizens, but also — to the extent it diverges from reality — creates the conditions for instability, upheaval and, in the extreme, its own demise. The experiences of the Soviet Union, Mao-era China and the Communist bloc during the Cold War are instructive and warn us of putting unchecked information power in the hands of the state.

If democratic societies escaped the fate of their authoritarian counterparts in the twentieth century, it may be because their political structures dispersed power and instituted checks and balances that proved to be effective enough. Government's legitimate need to use information power to inform, protect, educate and persuade citizens must, therefore, be constrained by constitution, statute and structure in its exercise.

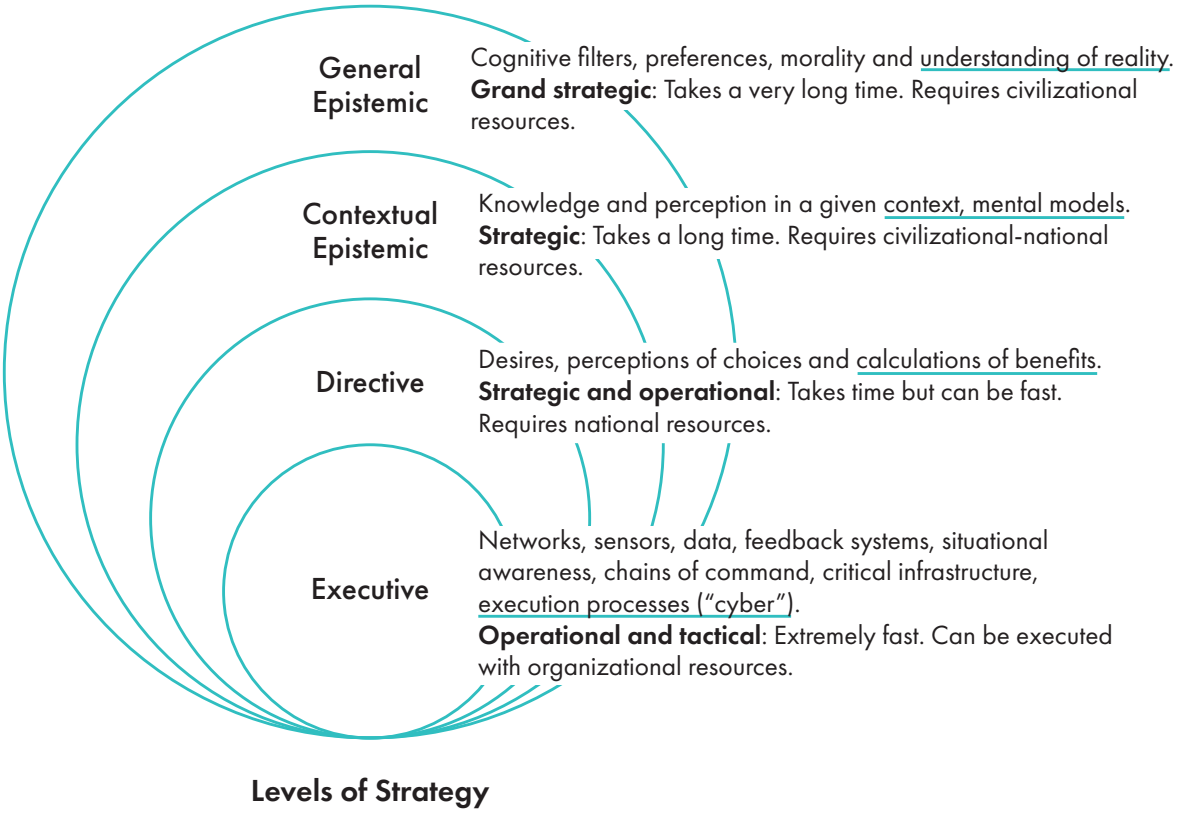
Recommendation

→ Construct structural safeguards against governments' directing of information power against their own citizens and ensure institutional checks and balances to prevent abuse.

The Information Domain

It is possible to visualize the cross-section of the information domain as consisting of four concentric strategic levels: the general epistemic, the contextual epistemic, the directive and the executive. This framework is represented in Figure 1.

Figure 1: The Framework of the Information Domain



Source: Author.

Bolstering the General Episteme

The all-encompassing outermost level of the information domain concerns the **general episteme**,[2] a society's understanding of reality, the validity of knowledge, the legitimacy of methods of acquiring knowledge, its basic values and social norms. Influencing societies at this level takes a long time and is a civilizational enterprise. For instance, the basket of related ideas of individual rights, liberal democracy and free markets arose from the Enlightenment. Those ideas first shaped Western societies and then spread across the globe over a period of three centuries. General epistemic change takes place very slowly, in fits and starts and with reversals along the way. The rate of information flows do affect the pace. Relatively rapid changes are possible if contexts are conducive and information networks pervasive. Communism and fascism gestated for decades before making rapid strides in the favourable aftermath of the First World War, and on the back of radio communication and air travel.

The general epistemic layer is important because it aligns societies at the deepest levels: to create shared narratives is also to ensure that the shared narrative is dominant.

The present time is witnessing several simultaneous general epistemological contestations. First, the geopolitical ascendance of the People's Republic of China and the closed information order it promotes challenge the free and open model extant in democratic countries. The closed model requires vast resources to be expended in censorship, surveillance, propaganda and narrative control but is attractive to authoritarian regimes because it strengthens their hold on power. Second, people around the world have responded to the advent of the global Information Age either by doubling down on ethnic or socially constructed identities, or by trying to transcend them.[3] Third, common global challenges such as climate change are calling the world's geopolitical structure into question, given the inability of the world's governments to achieve the cooperation necessary to stave off existential threats. These new contestations do not replace the traditional political, religious and ideological competition but add to them.

Liberal democracies can best defend themselves by strengthening their commitment to the foundational values underlying their success. Political communities organized around reason, liberty, equality, rule of law and openness have survived and outperformed the alternatives for more than three centuries. A long view of history suggests that given a choice, people will prefer openness and freedom.

Recommendations

- → Strengthen commitment to being and promoting free and open societies. Education, media and social norms must encourage free inquiry, reason and pluralism.
- → Defend a free and open global information order: counter illiberal political regimes and prevent unaccountable private corporations from acquiring political power.[4]

Securing Contextual Epistemes

The envelope of a society's views on a particular subject constitutes a **contextual episteme**. Perceptions, public attitudes and mental models are shaped by traditions, institutions, economic and social structures, and sources of information. Influencing societies at this contextual epistemic level is a strategic enterprise and requires national resources and long durations of time. The range of Indian public opinion on Russia's 2022 invasion of Ukraine derives from narratives of Cold War history, public perception of India's own relations with Russia, analogies to India's political considerations and society's response to Western, Russian and other international media coverage. Despite President Vladimir Putin's egregious violation of international law and naked military aggression, and Indians' consumption of news from, overwhelmingly, Western media, not to mention the relatively small propaganda effort by Russia, many Indians are sympathetic to the

2 The word *episteme* refers to valid knowledge and understanding. *Merriam-Webster.com Dictionary* defines it as "intellectually certain knowledge" (www.merriam-webster.com/dictionary/episteme).

3 See Fukuyama (2018) and Mounk (2023) on the resurgence of identity politics and attempts to overcome its limitations, respectively.

4 At the time of writing, the global information order is dominated by a few private corporations at the infrastructure, operating system and platform levels. While the content and services market is more competitive, these providers rely on underlying infrastructure that is a lot less competitive. Unlike the market for goods, concentration in information markets does not arise so much from entry barriers as from strong network effects. As this market power translates to political influence, it is in the public interest to prevent its accumulation.

Russian cause (Frisbie and Moskowitz 2023). The shadow of the Cold War narrative (when India relied on the Soviet Union's backing at the UN Security Council), its dependence on Russian arms imports, and skepticism over the West's motives could account for the apparent contradiction.

The contextual epistemic layer is of primary importance in information strategy because of its relevance to contemporary policy. Public opinion can now be effectively changed fast enough to achieve practical political goals — especially where the context, target audience, time frame and purpose are sharply defined. The effect might not be long-lasting, and indeed, it need not be. If public opinion on an issue can be influenced until, say, an election is concluded, the investment in contextual epistemological operations will deliver sufficient benefits.

Recommendations

- → Promote free and competitive media, and prevent the concentration of narrative power.
- → Promote technology ecosystems that are built on open protocols, open standards and open source that are less likely to concentrate market power.
- → Invest in "information health" (which must be considered an aspect of public health) through school curriculum interventions and public awareness programs.[5]
- → Enact legislation that allows governments to designate information sources as foreign political actors and requires these actors to be so identified in all communications.

Protecting Decision-Making Autonomy

The desires, choice perceptions, benefit calculations and intuitions of the policy-making elite constitute the **directive level** of the information domain. This level is important because a country's elite makes most of the substantive decisions that affect both the targeted and the targeting society. To continue with the previous example, India's foreign policy positions on the Russia-Ukraine war are the political resultant of elite actors in its political establishment, and may not reflect public opinion. Influencing the decision-making elite requires a far more targeted effort, directed at groups such as politicians who desire to be re-elected, civil servants who fear adverse outcomes, military leaders conscious of their organizational interests, business leaders who wish to protect their economic interests, and other interest groups that see external events from the perspective of promoting their domestic power.

The directive layer is amenable to relatively rapid changes, and successful influence operations may see results in the time frame of weeks or months. This renders the directive layer the primary operational theatre of information warfare. The operations process can be conceptualized as a loop, consisting of observation, orientation, decision and action (OODA) (Boyd 2018). Targeting the adversary's (or partner's) OODA loop is the focus of information operations at the directive level.

Defence at this level rests in diversity and resilience. The greater the diversity of opinion the decision makers have access to, the broader their assessments, window of feasible options and estimates of benefits. Deconcentrating decision making and building resilience into the system will reduce vulnerabilities.

Recommendations

- → Reconstitute political leaders' advisory to promote independence, diversity of background, expertise and opinion.
- → Disperse high-level decision making across government, with coordination among agencies rather than via a unified chain of command, to ensure diversity.
- → Embed public consultation in legislative and policy-making processes.
- → Adopt and strengthen instruments such as India's Right to Information Act, 2005, and the United States' Freedom of Information Act (and practices such as the mandatory declassification of public records).

Securing Cyberspace

The networks, sensors, data, feedback systems, chains of command and operating procedures that turn decisions into practical action constitute the **executive level** of the information domain. This level is mostly about the machines and the networks that interconnect them and also

5 Information health would include critical thinking skills, reasoning, media literacy, public communication norms, etiquette, and so forth.

includes the people who directly operate them. Most of what is termed as cyber falls into this category. Cyberwarfare — or the hacking of machines — is highly technical. It does not serve a political purpose in and of itself but is a tactical component of information warfare.

The first line of defence against attacks on the executive layer has been cybersecurity — software, hardware and practices to safeguard devices and networks from being compromised. The responsibility for cybersecurity falls predominantly on the end-users. However, user-provided cybersecurity is effective only to a point, and cannot secure large-scale infrastructure, much less a nation's entire information sphere.

Due to the externalities involved, cybersecurity is also a public concern, but the target surface is so vast that it is impossible for the state to secure every vulnerable point. Consequently, cybersecurity cannot be achieved without offensive cyber operations, where the fight is taken to the attacker, and strategies such as deterrence, compellence,[6] reward and punishment are employed (Smeets and Lin 2018).

Successful cybersecurity and cyber defence require cognitive superiority, technology and skill. The technological and operational aspect of defending against the hacking of machines is beyond the scope of this policy brief. From a freedom of thought perspective, there is an important consideration. While many cyberwarfare capabilities can be imported, states have an interest in achieving a high degree of self-reliance in the development and use of the cyber arsenal. Developing this self-reliance requires a force of people who not only have skills at the cutting-edge technologically but are also mentally agile. Cognitive strength forms the bedrock of cyber defence.

Recommendation

→ To enable national self-reliance in the cyber workforce, education systems, work cultures and social norms must promote free inquiry and thought.

Conclusion

To the extent information warfare reduces violence and bloodshed, it may be seen as an indicator of human progress. Achieving one's goals through persuasion and influence can be one of the most civilized forms of conducting politics. A fair contest where contenders use facts, logic and reason to persuade a free, open-minded audience is an ideal way for a society to settle its affairs. Evidence from cognitive sciences, however, puts a dampener on such hopes. The human mind has both intuitive and reasoning faculties, and the former are in the driver's seat (Kahneman 2011). Also, our opinions and decisions are far more socially influenced than it was previously believed (Haidt 2012). As a result, our cognitive makeup is susceptible to biases and manipulation. The human mind is vulnerable. The collective is even more so.

Constitutional and statutory safeguards can help protect the freedom to think within a country's domestic context. International relations, however, are conducted in an anarchy. There are no rules of the game and, even if there were, no means to ensure fair play. While international law can help at the margin, states have little choice but to engage in information warfare to protect their citizens' freedom to think.

6 *Compellence* refers to a coercive move that attempts to make an adversary behave in a certain way.

Works Cited

Boyd, John R. 2018. "Appendix: The OODA Loop." In *A Discourse on Winning and Losing*, edited by Grant T. Hammond, 383–86. Montgomery, AL: Air University Press. www.jstor.org/stable/resrep19552.13.

Frisbie, Sonnet and Scott Moskowitz. 2023. "India in Between: Modi's Delicate Dance of Diplomatic Moderation Offers Risks and Rewards." Morning Consult, January 17. https://pro.morningconsult.com/analysis/india-diplomatic-moderation-offers-risks-and-rewards.

Fukuyama, Francis. 2018. *Identity: Contemporary Identity Politics and the Struggle for Recognition*. London, UK: Profile Books.

Haidt, Jonathan. 2012. *The Righteous Mind: Why Good People Are Divided by Politics and Religion*. London, UK: Penguin Books.

Kahneman, Daniel. 2011. *Thinking, Fast and Slow*. London, UK: Penguin Books.

Kaufman, Stephen F. 2012. *Art of War: The Definitive Interpretation of Sun Tzu's Classic Book of Strategy*. Clarendon, VT: Tuttle.

Matthews, Victor A. and Don C. Benjamin. 1997. "*The Teachings of Ahiqar.*" In *Old Testament Parallels: Laws and Stories from the Ancient Near East*. Mahwah, NJ: Paulist Press.

Mounk, Yascha. 2023. *The Identity Trap: A Story of Ideas and Power in Our Time*. London, UK: Penguin Books.

Olivelle, Patrick. 2013. *King, Governance, and Law in Ancient India: Kautilya's Arthasastra*. Oxford, UK: Oxford University Press.

Smeets, Max and Herbert S. Lin. 2018. "Offensive Cyber Capabilities: To What Ends?" In *2018 10th International Conference on Cyber Conflict: CyCon X: Maximising Effects*, edited by T. Minárik, R. Jakschis and L. Lindström, 55–72. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence Publications. https://ccdcoe.org/uploads/2018/10/CyCon_2018_Full_Book.pdf.

Szafranski, Richard. 1995. "A Theory of Information Warfare: Preparing for 2020." *Airpower Journal* 9 (1): 56–65. www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-09_Issue-1-Se/1995_Vol9_No1.pdf.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director and General Counsel Aaron Shull
CIGI Senior Fellow and Project Co-Leader Susie Alegre
Director, Program Management Dianna English
Program Manager Jenny Thiel
Publications Editor Lynn Schellenberg
Senior Publications Editor Jennifer Goyder
Graphic Designer Abhilasha Dewan

KONRAD ADENAUER STIFTUNG

This policy brief was made possible thanks to the financial support of the Konrad-Adenauer-Stiftung (KAS) Canada.

For publications enquiries, please contact publications@cigionline.org.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org