TAKSHASHILA INSTITUTION

Hacking Minds, Manipulating Machines

A Primer on Information Warfare

Lokendra Sharma and Nitin Pai

Takshashila Discussion Document No. 2025-13
Version 1.0, June 2025

While information warfare is not new, the Information Age has imparted the former an unprecedented scale and reach. This primer explains the various forms, elements and features of information warfare. It examines the democratic trap and discusses the fundamental conundrum with information warfare – the double-edged sword nature of information power.

Recommended Citation:
Lokendra Sharma and Nitin Pai, "Hacking Minds, Manipulating Machines: A Primer on Information Warfare," Takshashila Discussion Document No. 2025-13, June 2025, The Takshashila Institution.

Executive Summary

While widespread mechanisation, large industrial clusters and increasingly lethal militaries defined the preceding Industrial Age that lasted for more than two centuries, the ongoing Information Age has been about the structuring of human society around the production, consumption and effects of information.

Information warfare is not a feature of the Information Age alone. But the Information Age has imparted the former an unprecedented scale and reach. Using information to influence decisions for achieving political objectives (without necessarily employing physical force) is information warfare.

While all states—including democratic ones—engage in information warfare, authoritarian states are at an advantage when stacked against the democratic ones. Authoritarian states, however, pay an opportunity cost for maintaining a sanitised domestic information environment.

The double-edged sword nature of information power gives rise to a fundamental conundrum: What prevents states which are empowered to safeguard the cognitive autonomy of their citizens from using the same information power against the latter?

This document has been formatted to be read conveniently on screens with landscape aspect ratios. Please print only if absolutely necessary.

Authors

Lokendra Sharma is a Research Analyst with the Takshashila Institution's High-Tech Geopolitics Programme.

Nitin Pai is the Director of the Takshashila Institution.

Acknowledgement

The authors would like to thank Bharath Reddy for valuable feedback.

Table of Contents

I. Introduction

In the wee hours of May 7, 2025, the Indian armed forces struck nine locations inside Pakistan and Pakistan-occupied Kashmir to target terror groups, which have mounted numerous attacks on Indian soil over the last two decades. The immediate cause for Operation Sindoor, however, was the killing of 25 tourists and a local guide in Kashmir's Pahalgam on April 22 by a Pakistan-linked terror group.[1] This led to a series of strikes and counter-strikes by India and Pakistan from May 7 to 10 before an understanding to halt military actions was declared by both sides. Pakistan's response to India's May 7 strike was not just restricted to the land (cross-border shelling) and air domains (drones and missiles) but also involved the information realm. Pakistan's army attempted to foment communal tensions in the Indian state of Punjab by falsely claiming that India was attacking its own Sikh population by launching a barrage of missiles.[2] Pakistan also fabricated claims of inflicting significant damages to Indian airbases like Adampur.[3] The Indian government and the armed forces, on the other hand, refrained from engaging in propaganda and instead focused on domestic information management. India carefully controlled the domestic media cycle on downing of Indian fighter jets by downplaying the same and controlling the information flow about loss of Indian assets.[4]

But it is not just India's western neighbour that engages in information warfare. India's northern neighbour has been more adept at mounting influence operations through a phenomenal social media product created by a Beijing-headquartered company, ByteDance. ByteDance's short-video sharing platform TikTok has more than a billion users worldwide. In June 2020, the government of India had banned TikTok about two weeks after the deadly India-China border clashes in Galwan. TikTok was among the 59 Chinese apps banned on the grounds that these were "engaged in activities which is prejudicial to sovereignty and integrity of India, defence of India, security of state and public order."[5] The comeback of some hitherto banned Chinese apps—following easing of India-China tensions—has led some commentators to wonder whether TikTok would return as well.[6] But even if data concerns associated with TikTok are addressed, issues with TikTok's powerful algorithm would remain: the algorithm could "be potentially used to amplify or de-amplify content to suit ByteDance's (and thereby Chinese Communist Party's) objectives."[7] That the Article 7 of China's 2017 intelligence law requires citizens and organisations to assist with national intelligence work does not help TikTok's case.[8]

China and Pakistan's influence operations directed at India notwithstanding, information warfare is not just an Indo-Pacific matter. It is as much a global concern, from the transatlantic to the transpacific. During the last decade, Russia has mounted disinformation campaigns in the US and Europe to

influence democratic elections. China's TikTok has been a source of alarming concern in the US as well. These developments beg some questions: are authoritarian states at an advantage when it comes to mounting information warfare, as compared to democratic ones? How can democratic states defend against authoritarian ones? How can states be empowered to tackle influence operations, while being prevented from using the same power on their own citizens? How can citizens defend against cognitive threats irrespective of the threat actor?

Information warfare is largely "unseen yet pervasive" and "is more likely to have a deeper impact (both cognitively at individual level, and collectively at societal level)."[9] Therefore, as nation-states become deeply enmeshed in the Information Age, it is pertinent that stakeholders—governments, militaries but also private sector and common citizens—develop an understanding about the various aspects of information warfare to better safeguard their cognitive autonomy.

This discussion document serves as a primer on information warfare and is divided into three parts. The first part focuses on the contours of the Information Age. The second part unpacks information warfare, including its elements and features. The final part examines the democratic trap, as well as discusses the fundamental conundrum with information warfare – the double-edged sword nature of information power.

II. Contours of the Information Age

While widespread mechanisation, large industrial clusters and increasingly lethal militaries defined the preceding Industrial Age that lasted for more than two centuries, the ongoing Information Age has been about the structuring of human society around the production, consumption and effects of information. More specifically, the Information Age has been defined as "[t]he period beginning in the last quarter of the 20th century marked by the increased production, transmission, consumption of, and reliance on information."[10] The proliferation of many different types of computing devices, coupled with technologies to connect them together, heralded the Information Age. This new age not only created new winners and losers in the economic realm (think the internet economy), but also altered the ideas of power and legitimacy in international relations.[11]

Kotasthane and Pai (2023) use "power" in the way Robert Dahl conceptualised it in 1957: "A has power over B to the extent that he can get B to do something that B would not otherwise do." Legitimacy, on the other hand, "requires conformity to a set of rules."

As Kotasthane and Pai (2023) have argued, power has undergone three shifts in the Information Age. First, gaining power in the international system has become more accessible. By "[u]sing information weapons", an actor could directly influence "an adversary's cognitive and decision-making systems".

Second, as the utility of violence reduces in the Information Age, states that can better wield information weapons will enjoy an asymmetric advantage over the others. Third, while the Industrial Age was mostly about nation-states, the Information Age makes non-state actors relatively more powerful. Power does not operate in a vacuum. Power and legitimacy are deeply intertwined. In order to effectively exercise power (or exercise power with less hindrances), that power should be deemed legitimate by other actors in the international system. Therefore, "gaining legitimacy, like power, is a cognitive act." Powerful actors employ narrative dominance—in addition to hard military strengths—to build legitimacy around their actions in an international system that is largely anarchic. State or non-state actors can "easily use the weapons of the Information Age to delegitimise the narratives that old powers might have carefully constructed."[12] Non-state actors are relatively empowered to question the narrative dominance of a powerful actor and even offer alternative narratives.

III. What is information warfare?

Information warfare is not a feature of the Information Age alone. But even as information warfare has been waged for thousands of years, the Information Age has imparted the former an unprecedented scale and reach. Information warfare can be defined as "the use of information to influence decisions in order to achieve a political objective without necessarily using physical force."[13]

There are various forms of information warfare that are popularly known. For example, propaganda uses information to achieve a political goal. Propaganda is intentional, systematic, manipulative dissemination of information to achieve a particular effect in the mind of the targeted person(s). The difference between propaganda and advertising is that the latter is primarily transactional. The former is about wanting people to act in the way you want, and believe in the things you believe. Spreading disinformation, malinformation or fake news in an organised and coordinated manner, with a political goal, are part of propaganda in a broader sense. Espionage or surveillance is another form of information warfare. Further, denial of information or censorship is as much information warfare as propaganda and snooping are. Just as channelling information may be

Disinformation is about deliberately spreading false information; malinformation is about presenting a fact out of its context to mislead; fake news is false information packaged as mainstream news.

information warfare – blocking, changing, moderating, corrupting or interfering with the flow of information too can be information warfare.

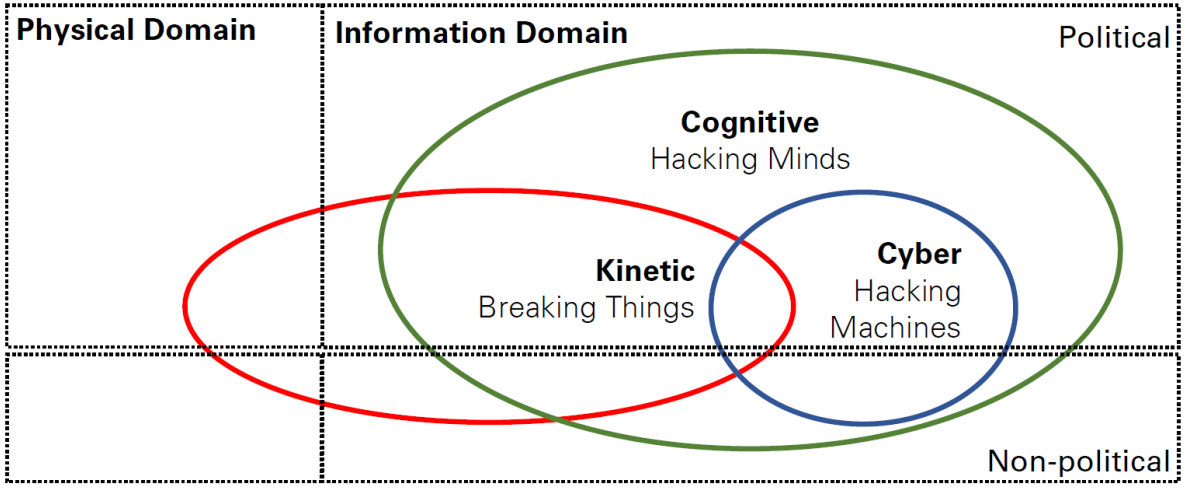
III.1. Elements of information warfare

Information warfare is fundamentally about political ends, though it also operates in the virtual, cognitive realm. As demonstrated in Figure 1, there are three elements of information warfare. The first is cognitive warfare that involves hacking the minds. This can be done through propaganda as described above, or through dedicated influence operations involving the spread of disinformation that targets the very idea of reality. Russian disinformation campaigns in Europe are an example of the same.

Using social media platforms and their algorithms to amplify or de-amplify certain content is also about hacking the mind. While the TikTok case discussed above fits this description, the same can also be held true for X (formerly Twitter). Breaking his promise of keeping Twitter "politically neutral", Elon Musk, who bought the platform in 2022, turned it into an echo chamber for the Make America Great Again (MAGA) movement in the run-up to the 2024 US presidential elections.[14] But Musk's machinations did not just stop at the US borders – from Latin America to Europe, Musk used the X platform to support and amplify right-wing causes.[15] Musk

demonstrated that a powerful social media platform could be wielded as an information weapon in a largely democratic set-up for shaping popular political views domestically and beyond.

Figure 1: The information domain



Source: Conceived and created by Nitin Pai.

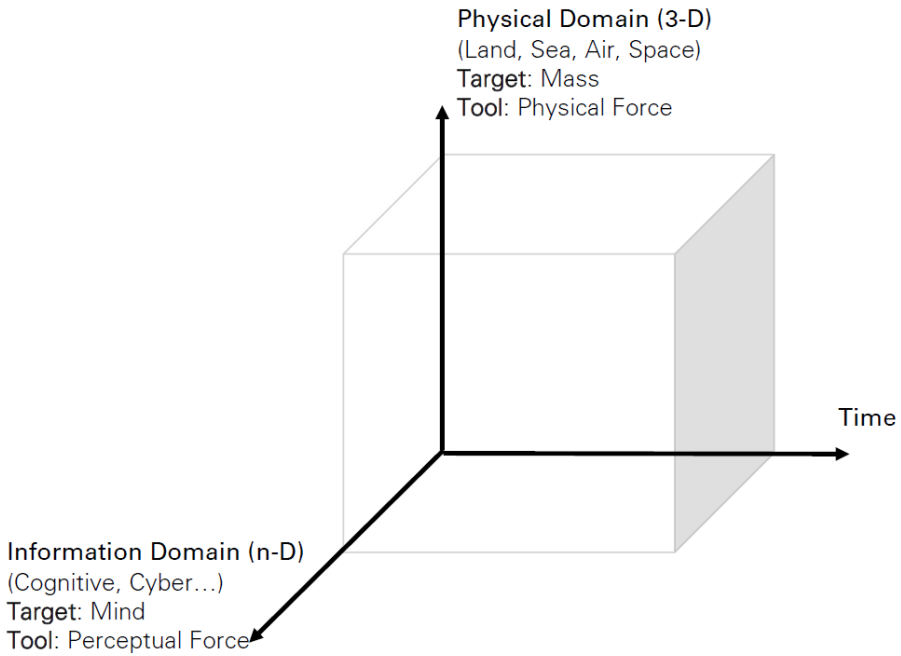
The second element of information warfare is cyber warfare that involves hacking the machines for producing a cognitive effect. China's cyberattack on India's power grid in 2020 is an apt example of the same.[16] Even mounting kinetic attacks (such as a terrorist attack or sabotage) may produce cognitive effects in the targeted population. Attacks can also lie at the intersection of the kinetic, cognitive and cyber elements. For example, the Stuxnet worm

that damaged Iran's nuclear enrichment facility at Natanz involved all three elements – kinetic, cognitive and cyber.

III.2. Blurring lines between physical and information domain

It is possible to conceptualise any contemporary conflict as playing out over multiple domains and dimensions. For instance—in the physical domain—a conflict could play out over land, sea, air or space with the target of physical force being mass. At the same time—in the information domain—perceptual force could be used to target the minds of an adversary's population (or decision-making elites) through cognitive or cyberattacks. But these are not clear distinctions. There may be overlaps, and an attack in the physical domain (such as aerial bombardment of the capital city of an adversary) may be intended more for the cognitive effects as opposed to just the quantum of destruction.

Figure 2: The multi-domain, multi-dimensional nature of conflict



Source: Conceived and created by Nitin Pai.

The Russia-Ukraine war that has been ongoing since early 2022 has played out in a multi-domain, multi-dimensional manner, involving both the physical and information realm. Russia and Ukraine have not just duelled over the land, sea, air and space domain, but also mounted cognitive and cyber warfare over the years. The initial "special military operation" launched by Russia in February 2025 was at the intersection of the physical and the cognitive. The Russian military embarked on an ambitious march towards the Ukrainian capital city Kyiv that aimed at browbeating Ukrainians into submission, not by unrestrained violence, but by sheer display of overwhelming military might of the invading forces.

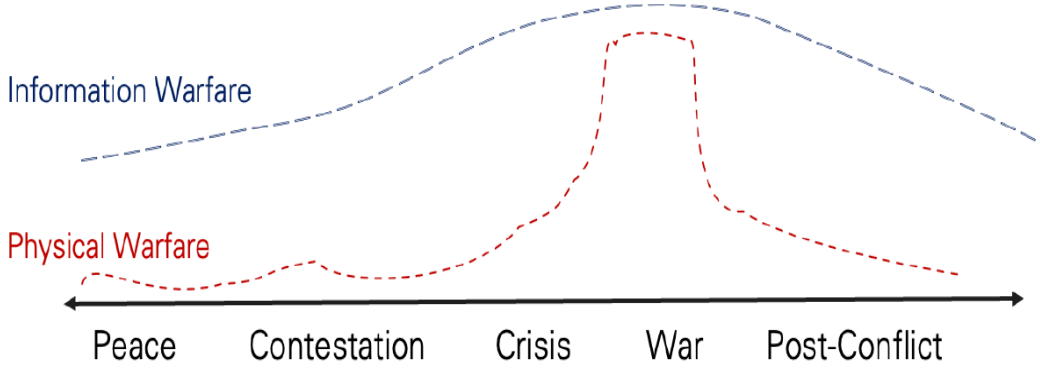
That the initial Russian strategy did not work in face of Ukrainian resistance and (subsequent) military assistance by the United States and partner countries is not relevant to the current argument.

III.3. Information warfare does not always need a war

War is an event. It has a beginning and an end. Waging war is warfare. The act of engaging in war is warfare. However, a party could be engaged in warfare without being in war. For example, Pakistan has been engaged in sub-conventional warfare (that is, below the threshold of war) with India through state-sponsored terrorism. The continuity argument holds more so for information warfare, which, as showcased in Figure 3, maintains a relatively high baseline even during peacetime as well as periods of

contestation, crisis and post-conflict. Physical warfare, however, peaks during a war while staying relatively low otherwise (notwithstanding sub-conventional warfare).

Figure 3: Information warfare versus physical warfare



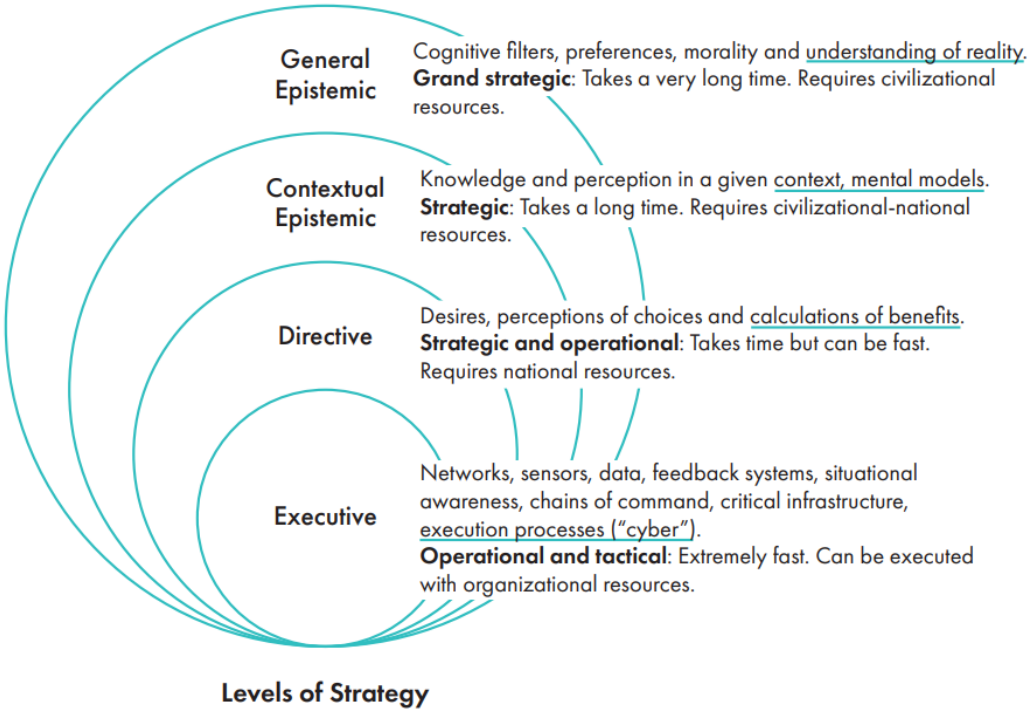
Source: Conceived and created by Nitin Pai.

III.4. Levels of strategy in information warfare[17]

The information domain can be broadly divided into four levels. The outermost layer, and the one which is most consequential, is the general epistemic layer. This is where a society's understanding of reality forms and manifests (think enlightenment values, how China views its place in the world). Influencing the general epistemic layer of a society is a very long-term matter requiring civilisational resources. The second-outermost layer is the contextual epistemic, which is about knowledge and perception in a particular context (that is, a society's views on a particular subject, say immigration). Influencing societies at this level requires national level resources in a long-time frame. How decision-making elites of a society think about their desires, perceive choices and calculate benefits constitute the third layer of the information domain – the directive layer. This layer is where most of the information operations are targeted at. Influencing this layer, while requiring national level resources, can yield relatively faster results. The last level is executive (or cyber). This layer is about networks, sensors and a host of systems that translates thoughts in the upper layers into actions. Influencing this layer is done through cyberattacks. One way to look at these layers is that a largely physical layer sits at the bottom; moving up across the information layers is directly proportional to an increase in abstraction. The

greater the abstraction, the more difficult and time consuming an influencing endeavour is, albeit more rewarding at the same time.

Figure 4: Levels of strategy in the information domain



Source: Nitin Pai (2024)[18]

IV. The democratic trap and the fundamental conundrum

In an international system that is largely anarchic, power and legitimacy in the Information Age derive partly, if not wholly, from narrative dominance. Narrative dominance not just domestically, but also internationally. While all states—including democratic ones—engage in information warfare, authoritarian states are at an advantage when stacked against the democratic ones. Authoritarian states, such as China and Russia, have installed a heavily censored domestic information environment while taking advantage of the relatively freer information flows in Western societies such as that of the United States. By sanitising their own information environment, authoritarian states maintain narrative dominance domestically. But by mounting information operations, including disinformation campaigns in the West, authoritarian states attempt to undermine core democratic narrative about the integrity of elections.[19]

Across the Atlantic, Russian President Vladimir Putin has been wielding his own information weapons to partly avenge the fall of the Union of Soviet

Socialist Republics (USSR). In the late 1980s and early 1990s, the colossal Soviet Union comprising 15 constituent soviet socialist republics including Russia unravelled. Internal contradictions and weakness of the Soviet system have often been cited as among the reasons for the collapse of the USSR and the end of the Cold War.[20]

But the Cold War was a contest among super powers mostly in the Industrial Age.

In the ongoing Information Age, which began towards the end of the 20th century and accelerated in the 21st, equations have changed. What was once the strength of Western democracies—a free press and relatively free flow of information—might have just become a weakness.[21] Perhaps no one understood this better than President Putin, who, amid the commercial and open vision backed by the US, citizen rights vision backed by the EU and the paternal and controlling approach backed by China, pushed for his own vision for the internet – the Moscow spoiler model.[22] This model involved mounting disinformation campaigns with the end-goal of causing more polarisation in the targeted polity. But more importantly, Russian information operations attacked the very idea of reality; that is, what is real and what is not, what could be trusted and what could be not.

Although Putin's information operations have targeted countries such as Germany, Britain and Estonia over the past decade,[23] arguably the most consequential target has been the United States. In the lead up to the 2016 US presidential elections, Russia engaged in what has been described as a case of information warfare.[24] At the heart of Moscow's Project Lakhta[25] was the now disbanded,[26] St. Petersburg-based Internet Research Agency (IRA) that employed an army of bots on social media platforms such as Facebook and Twitter (now called X). The disinformation campaign attempted to polarise voters and diminish their trust in the US electoral processes. Cognitive warfare went hand in hand with cyber warfare when the Russian intelligence agency, Main Intelligence Directorate of the General Staff (popularly known as GRU), hacked the emails of Democratic presidential nominee Hillary Clinton and subsequently spread them via Wikileaks.[27] The Republican presidential nominee Donald Trump made Clinton's emails one of his central election planks. In the years following Trump's victory in the 2016 elections, separate investigations launched by Special Counsel Robert Mueller, Department of Justice, the intelligence community, and the Republican-led Senate Select Committee on Intelligence reached a similar conclusion: Russia interfered in the 2016 elections.[28] The Senate report found that the Russian campaign attempted to help Trump's presidential campaign, and also showcased evidence of contacts between Trump campaign officials and those linked with the Kremlin.[29]

It is one thing to say that Russia tried to help Trump clinch the presidency. But can Trump's victory be partially attributed to Putin's information operations? An influential 2023 study in *Nature Communications* "did not detect any meaningful relationships between exposure to posts from Russian foreign influence accounts and changes in respondents' attitudes on the issues, political polarization, or voting behavior."[30] But as the authors themselves acknowledge, this study focused narrowly on social media posts on Twitter; they did not look at the interference in its totality across social media platforms, involving not just posts but also the media (image, video) shared, cyber actions (Clinton email hack) and second-order effects (the impact of the news of Russian interference among US citizens, irrespective of how successful the IRA campaign was). As a 2022 paper looking at second-order impact notes, "it has become clearer that knowledge of the precise direct impact of the R-IRA is likely to remain elusive."[31]

It is not as if authoritarian states enjoy an asymmetric advantage without any cost. Implementing a domestic firewall that filters external content, and manning an iterative information sanitising socio-technical system for domestically generated content has a significant opportunity cost. Because "[i]f China didn't expend so much political, financial and human energy on firewalls, censorship and surveillance, it is likely to have been a far richer, more innovative and vibrant society by now."[32]

How should democracies respond to the threat from authoritarian states in the information domain? Empowering the regimes in power to wield information weapons is riddled with a conundrum: what stops these democratically elected regimes from not using the same information weapons against their own citizens to further their goals, such as staying in power or fulfilling ideological missions of their partisan voter-bases? What prevents governments or private companies (such as Elon Musk's X) in democratic setups from wielding indiscriminate information power domestically? Constitutional safeguards is one obvious answer, but is it enough to provide cognitive security? After centuries of warfare, nation-states developed professional armies and security forces to secure the physical (political) borders. But nation-states, especially of the democratic kind, have not yet figured out how to secure the cognitive borders from threats – both internal and external.

V. References

[1] "Operation SINDOOR: Forging One Force." Press Information Bureau, May 18, 2025. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2129453; Ashiq, Peerzada. "The Resistance Front: New face of terror." The Hindu, April 27, 2025. https://www.thehindu.com/news/national/the-resistance-front-new-face-of-terror/article69495443.ece

[2] Sidhu, KBS. "Pakistan tried hard to instigate Sikhs against India during Operation Sindoor." The Print, May 17, 2025. https://theprint.in/opinion/pakistan-khalistan-propaganda/2628681/

[3] "PM Modi poses in front of S-400 missile system at Adampur Air Base days after Pakistan claimed it was destroyed." Times of India, May 13, 2025. https://timesofindia.indiatimes.com/india/pm-modi-poses-in-front-of-s-400-missile-system-at-adampur-air-base-days-after-pakistan-claimed-it-was-destroyed/articleshow/121134748.cms

[4] Peri, Dinakar. "Operation Sindoor objectives achieved; losses are part of combat but pilots are back home, says IAF." The Hindu, May 11, 2025, https://www.thehindu.com/news/national/operation-sindoor-objectives-achieved-losses-are-part-of-combat-but-pilots-are-back-home-says-iaf/article69564934.ece

[5] "Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order." Press Information Bureau, June 29, 2020. https://pib.gov.in/PressReleseDetailm.aspx?PRID=1635206&reg=3&lang=1

[6] Pareek, Priya. "Many banned Chinese apps make comeback in India: Will TikTok return?" India Today, February 12, 2025. https://www.indiatoday.in/india/story/many-banned-chinese-apps-make-comeback-in-india-will-tiktok-return-2678684-2025-02-12; Chawake, Anurag. "Banned Chinese apps like Xender and TanTan are back, but TikTok is still missing." Indian Express, February 13, 2025. https://indianexpress.com/article/technology/tech-news-technology/banned-chinese-apps-xender-tantan-shein-back-tiktok-missing-9829795/

[7] Sharma, Lokendra. "Why India should keep out TikTok in the age of information warfare." Moneycontrol, March 13, 2025. https://www.moneycontrol.com/news/opinion/why-india-should-keep-out-tiktok-in-the-age-of-information-warfare-12963472.html

[8] Additionally, there have also been reports of ByteDance's linkages with the Chinese Communist Party. See: Mohan, Geeta. "How China's Intelligence Law of 2017 authorises global tech giants for espionage." India Today, July 27, 2020. https://www.indiatoday.in/news-analysis/story/china-national-intelligence-law-2017-authorise-companies-espionage-india-1705033-2020-07-27; Girard, Bonnie. "The Real Danger of China's National Intelligence Law." The Diplomat, February 23, 2019. https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/; Soo, Zen. "Former ByteDance executive says Chinese Communist Party tracked Hong Kong protesters via data." AP, June 7, 2023. https://apnews.com/article/tiktok-china-bytedance-user-data-d257d98125f69ac80f983e6067a84911; Ye, Josh. "TikTok ban bill: What we know about Tiktok's Chinese owner." Reuters, March 16, 2024. https://www.reuters.com/technology/what-do-we-know-about-tiktoks-chinese-owner-bytedance-2024-03-15/

[9] Sharma, Lokendra. "Looking beyond privacy and platform governance: A case for reorienting public discourse in India." Moneycontrol, October 10, 2024. https://www.moneycontrol.com/news/opinion/looking-beyond-privacy-and-platform-governance-a-case-for-reorienting-public-discourse-in-india-12839176.html

[10] Igwe, C. Frank. "Third Places in the Blackosphere." Encyclopedia of Information Science and Technology, Second Edition, edited by Mehdi Khosrow-Pour, IGI Global, 2009, pp. 3745-3749. https://doi.org/10.4018/978-1-60566-026-4.ch597

[11] Kotasthane, Pranay, and Nitin Pai. "Interrogating Power and Legitimacy in the Information Age from an Indian Perspective." Power, Legitimacy, and World Order, edited by Sanjay Pulipaka, Krishnan Srinivasan, James Mayall, Routledge India, 2023. 189-197. https://doi.org/10.4324/9781003385233

[12] Ibid.

[13] Pai, Nitin. "Narrative Dominance, Information Warfare and the Freedom to Think." Centre for International Governance Innovation, Policy Brief No. 6, February 2024. https://www.cigionline.org/static/documents/FoT_PB_no.6.pdf

[14] Ingram, David. "How Elon Musk turned X into a pro-Trump echo chamber." ABC News, October 31, 2024. https://www.nbcnews.com/tech/social-media/elon-musk-turned-x-trump-echo-chamber-rcna174321; Swenson, Ali, and Chris Megerian. "Elon Musk uses his X ownership to be a mouthpiece for Trump narratives and his White House position to push his priorities." PBS, February 6, 2025. https://www.pbs.org/newshour/politics/elon-musk-uses-his-x-ownership-to-be-a-mouthpiece-for-trump-narratives-and-his-white-house-position-to-push-his-priorities; Bond, Shannon, and Bobby Allyn. "2 years in, Trump surrogate Elon Musk has remade X as a conservative megaphone." NPR, October 25, 2024. https://www.npr.org/2024/10/22/nx-s1-5156184/elon-musk-trump-election-x-twitter

[15] Silva, João da, and Vanessa Buschschlüter. "Top Brazil court upholds ban of Musk's X." BBC, September 3, 2024. https://www.bbc.com/news/articles/crkmpe53l6jo; Taylor, Adam, Jeremy B. Merrill, and Adrián Blanco Ramos. "How Elon Musk used X to amplify Germany's far right ahead of election." The Washington Post, February 23, 2025. https://www.washingtonpost.com/world/2025/02/20/musk-germany-election-afd-x-twitter/

[16] Sanger, David E., and Emily Schmall. "China Appears to Warn India: Push Too Hard and the Lights Could Go Out." New York Times, February 28, 2021. https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html

[17] This section is adapted from: Pai, Nitin. "Narrative Dominance, Information Warfare and the Freedom to Think." Centre for International Governance Innovation, Policy Brief No. 6, February 2024. https://www.cigionline.org/static/documents/FoT_PB_no.6.pdf

[18] Ibid.

[19] Kotasthane, Pranay, and Nitin Pai. "Interrogating Power and Legitimacy in the Information Age from an Indian Perspective." Power, Legitimacy, and World Order, edited by Sanjay Pulipaka, Krishnan Srinivasan, James Mayall, Routledge India, 2023. 189-197. https://doi.org/10.4324/9781003385233

[20] Kalashnikov, Anthony. "Differing Interpretations: Causes of the Collapse of the Soviet Union." Constellations 3, no. 1 (2012): 75–86. https://doi.org/10.29173/cons16289; Sakwa, Richard. "The Soviet Collapse: Contradictions and Neo-Modernisation." Journal of Eurasian Studies 4, no. 1 (2013): 65-77. https://doi.org/10.1016/j.euras.2012.07.003

[21] Rosenbach, Eric, and Katherine Mansted. "Can Democracy Survive in the Information Age?" Belfer Center for Science and International Affairs, October 2018. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/CanDemocracySurvive_0.pdf

[22] O'Hara, Kieron, and Wendy Hall. Four Internets: Data, Geopolitics, and the Governance of Cyberspace. University of Oxford, 2021. https://doi.org/10.1093/oso/9780197523681.001.0001

[23] Wesolowski, Kathrin, and Tetyana Klug. "Fact check: Russia's influence on Germany's 2025 election." DW, February 18, 2025. https://www.dw.com/en/russian-disinformation-aims-to-manipulate-german-2025-election/a-71664788; Ruy, Donatienne. "Did Russia Influence Brexit?" Center for Strategic and International Studies, July 21, 2020. https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit; Teperik, Dmitri. "Disinformation networks of pro-Kremlin proxies in Estonia and their fostering of anti-government sentiment among the Russian speaking community: the case of anti-vaccination narratives in the online space." GLOBSEC, 2022. https://www.globsec.org/sites/default/files/2022-02/Disinformation-networks-of-pro-Kremlin-proxies-in-Estonia.pdf

[24] "Russian National Charged with Interfering in U.S. Political System." US Department of Justice, October 19, 2018. https://www.justice.gov/archives/opa/pr/russian-national-charged-interfering-us-political-system; Wojnowski, Michał. "U.S. Democracy as the target of Russian Secret Services." Warsaw Institute. 2021. https://warsawinstitute.org/wp-content/uploads/2021/07/RS_06-2021_EN.pdf

[25] Hanlon, Bradley. "Target USA: Key Takeaways from the Kremlin's "Project Lakhta"." The German Marshall Fund of the United States. https://www.gmfus.org/news/target-usa-key-takeaways-kremlins-project-lakhta

[26] Greenberg, Andy, and Andrew Couts. "Security News This Week: Russia's Notorious Troll Farm Disbands." WIRED, July 8, 2023. https://www.wired.com/story/russia-internet-research-agency-disbands/

[27] Nakashima, Ellen, and Shane Harris. "How the Russians hacked the DNC and passed its emails to WikiLeaks." Washington Post, July 13, 2018. https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html

[28] "Fact Sheet: What We Know about Russia's Interference Operations." The German Marshall Fund of the United States. https://www.gmfus.org/news/fact-sheet-what-we-know-about-russias-interference-operations

[29] Mazzetti, Mark. "G.O.P.-Led Senate Panel Details Ties Between 2016 Trump Campaign and Russia." New York Times, August 18, 2020. https://www.nytimes.com/2020/08/18/us/politics/senate-intelligence-russian-interference-report.html

[30] Eady, Gregory, et al. "Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behavior." Nature Communications 14 (2023): 1–11. https://doi.org/10.1038/s41467-022-35576-9

[31] Ross, Andrew RN, Cristian Vaccari, and Andrew Chadwick. "Russian meddling in US elections: How news of disinformation's impact can affect trust in electoral outcomes and satisfaction with democracy." Mass Communication and Society 25, no. 6 (2022): 786-811. https://doi.org/10.1080/15205436.2022.2119871

[32] Pai, Nitin. "We have a historic opportunity to shape tomorrow's world order." Mint, May 1, 2024, https://www.livemint.com/opinion/columns/we-have-a-historic-opportunity-to-shape-tomorrow-s-world-order-11682879640606.html

The Takshashila Institution is an independent centre for research and education in public policy. It is a non-partisan, non-profit organisation that advocates the values of freedom, openness, tolerance, pluralism, and responsible citizenship. It seeks to transform India through better public policies, bridging the governance gap by developing better public servants, civil society leaders, professionals, and informed citizens.

Takshashila creates change by connecting good people, to good ideas and good networks. It produces independent policy research in a number of areas of governance, it grooms civic leaders through its online education programmes and engages in public discourse through its publications and digital media.