GOA UNIVERSITY
गोंय विद्यापीठ

भारतीय सामाजिक विज्ञान अनुसंधान परिषद्
Indian Council of Social Science Research
शिक्षा मंत्रालय | Ministry of Education

Future Shift Labs

FORUM ON
DIGITAL STATECRAFT

POST EVENT REPORT

About the Report

The Forum on Digital Statecraft 2026 marked a timely intervention at a moment when digital power, cognitive influence, and geopolitical competition increasingly intersect. This report recounts the Forum's core dialogues and research contributions, capturing how experts from defence, academia, diplomacy, and technology interrogated the emerging information order: from cognitive warfare and narrative manipulation to cyber norm-setting and digital sovereignty.

Beyond documenting proceedings, this report reflects on what the rise of information power means for India's strategic future and democratic resilience. It is intended not merely as a record, but as a reference point for researchers, policymakers, and practitioners seeking to navigate the complexities of cognitive security and digital geopolitics in the coming decade.

The Forum served as a platform to present original research on cyber diplomacy, cognitive security, and Foreign Information Manipulation and Interference (FIMI), and to facilitate interdisciplinary conversations that bridged the domains of security, public policy, digital governance, and international affairs. The insights captured in this report have been compiled for policymakers, security practitioners, research institutions, and stakeholders shaping India's digital, diplomatic, and strategic futures.

We were honoured to have Shri Sujeet Kumar, Member of Parliament, and Ms. Revathi Mannepalli, India's Representative to the International Telecommunication Union (ITU), deliver keynote addresses that anchored the discourse within India's shifting strategic and diplomatic priorities in the digital domain.

Our sincere thanks go to all panelists, speakers, moderators, and contributors, and to the research teams whose work grounded the discussions in evidence and strategic clarity. The depth of engagement reflected a shared commitment to enhancing India's preparedness in a rapidly evolving and contested information environment. We are grateful to everyone who made this dialogue both timely and meaningful.

Contributors & Participants

Prateek Joshi · Air Marshal G.S. Bedi (Retd) · Mohd. Ujaley · Dr. Ila Joshi · Dr. Madhukar Shyam · Dr. Ankita Dutta · Dr. Sriparna Pathak · Brig. Anshuman Narang (Retd) · Shantanu K. Bansal · Dr. Kumari Mansi · Ms. Sunanda R. Marak · Purushendra Singh · Dr. Ulupi Borah · Dr. Samir Bhattacharaya · Jyoti Panday · Amrita Choudhury· Subimal Bhattacharjee· Dr. Shahid Siddiqui· Mateusz Łabuz · Bhairabi Kashyap Deka · Sagar Vishnoi · Anhaietaa Puri · Aastha Naresh Kohli · Pranav Dwivedi · Parishrut Jassal · Aşkım Ezo Barol · Alisha Butala · Parul Madan · Vidhi Sharma · Prachi Sharma · Neha Sethi · Sugam Vishnoi · Akanksha Dhanraj · Abir Mahanta · Riya Sandal · Tejasvi Vishnoi

INDEX

Executive Summary

India's strategic and geopolitical position, alongside one of the world's fastest-growing digital ecosystems, has created an increasingly complex and contested information environment. The rapid expansion of Digital Public Infrastructure, widespread internet access, and accelerated adoption of emerging technologies have transformed how information is created, disseminated, and consumed. While these developments have strengthened connectivity and governance, they have also heightened India's exposure to targeted information manipulation, perception management, and cognitive security threats.

To address this evolving challenge, Future Shift Labs convened the Forum on Digital Statecraft as a research-led strategic platform to examine how information warfare, foreign interference, and cognitive influence are reshaping India's security landscape. The forum brought together experts to assess the implications of these threats and explore institutional responses required to safeguard democratic resilience and national interests.

The discussions were anchored in three original research studies. The first examined India's role in shaping global cyber governance and advancing norms related to digital sovereignty and responsible state behaviour. The second analysed the weaponisation of cognition through psychological manipulation and narrative engineering in digital spaces. The third focused on Foreign Information Manipulation and Interference (FIMI), mapping organised disinformation networks and their impact on India's media ecosystem and democratic processes.

Background

IIndia's rapidly evolving digital ecosystem presents both strategic opportunities and vulnerabilities, particularly in the domains of information, cyber, and cognitive security. The Forum on Digital Statecraft convened experts from defence, academia, technology, and policy to examine India's information environment, focusing on strategic, cognitive, and diplomatic challenges.

The sessions highlighted India's emerging role in global cyber governance, norm-setting, and digital diplomacy, with discussions emphasising the importance of harmonised policy, multi-stakeholder engagement, and human-centric AI to bridge global divides. Cognitive warfare was explored as a critical threat vector, with insights on how disinformation, algorithmic amplification, and perception manipulation target individuals and societal trust. Case studies, including the India-Pakistan conflicts of 2025 and Operation Sindoor, illustrated the operationalisation of foreign information manipulation and the need for preemptive, resilience-focused strategies.

Key recommendations emphasised strengthening institutional capacities, developing comprehensive cognitive resilience toolkits, fostering digital literacy, and reducing dependence on foreign platforms. The Forum underscored the importance of a coordinated, evidence-based approach to safeguard national security, societal trust, and India's leadership in shaping a stable and secure regional information environment. By situating information challenges within a geopolitical and technological context, the event laid the groundwork for actionable policy and strategic preparedness in the coming decade

Objectives of the Forum on Digital Statecraft – 2026

India's evolving digital ecosystem presents both strategic opportunities and vulnerabilities. The nation's vast social media user base, rapid technological adoption, and shifting media landscape have created conditions where cognitive manipulation, information operations, and organized influence campaigns can exploit societal fractures. Recognizing this, the Forum on Digital Statecraft aims to strengthen India's resilience against the weaponization of information, while positioning the country as a leader in shaping global norms around cyber governance, AI, and responsible technology use.

The event sought to:

1. Present interdisciplinary research mapping India's information warfare landscape, including domestic and cross-border cognitive threats, AI-enabled manipulation, and strategic disinformation campaigns such as FIMI.

2. Identify vulnerabilities in national security, societal trust, and institutional preparedness, highlighting challenges posed by reliance on foreign infrastructure, digital divides, and rapid technology diffusion.

3. Facilitate structured engagement between policymakers, defence and security agencies, academia, technology experts, and civil society to foster coordinated responses.

4. Generate actionable recommendations to enhance cognitive resilience, preempt disinformation, and reinforce India's role in international digital governance, regional stability, and strategic norm-setting.

By integrating evidence-based insights with policy foresight, the Forum emphasized a holistic, proactive approach to India's information security, ensuring societal trust, institutional strength, and global influence in the coming decade.

CORE PROCEEDINGS

Chief Guest's Address – Ms. Revathi Mannepalli, India's Representative to the International Telecommunication Union (ITU)

In her address, Ms. Revathi Mannepalli underscored the centrality of information to national security and governance in the digital era, noting that power today is no longer exercised solely through physical force but through influence over information and perception. She emphasised the need for India to strike a careful balance between openness and security, highlighting that traditional sectoral boundaries are dissolving as governments, industry, and society increasingly operate within interconnected digital ecosystems.

Ms. Mannepalli also reiterated that India approaches digital governance with a service-oriented ethos rather than a purely commercial motive. She stressed that defending cyberspace can no longer remain the responsibility of governments alone, as cyber threats do not exist in isolation and often cut across domains. Concluding her remarks, she highlighted that information warfare ultimately targets people and human behaviour, amplifying its impact, and that government frameworks can succeed only when society is aware, engaged, and acts collectively.

Session 1: India's Cyber Governance Diplomacy and Global Norm-Shaping Role

The panel explored India's evolving role in global cyber governance from political science and international relations perspectives, focusing on the intersections of policy, power, and people, and considering what India can contribute to the international digital architecture.

Key Interventions

- Mr. Subimal Bhattacharjee opened the session by noting that India's influence in digital forums remains limited compared to the US, China, and Russia, and emphasised the need for internal harmonisation to strengthen norm-setting efforts. He highlighted the importance of understanding geopolitics around critical minerals, semiconductors, AI, and the broader digital ecosystem.

- Mr. Purushendra Singh described India's pivotal moment in leveraging human-centric AI to bridge North–South divides, revive multilateral institutions, and foster collaboration over bloc-building.

- Dr. Shaid Siddiqui cautioned that India must address the non-traditional risks of AI, given its limited strategic influence.

- Ms. Amrita Choudhury highlighted India's multi-stakeholder approach and stressed building government capacity to effectively tackle emerging challenges.

- Dr. Ulupi Borah emphasised semiconductors and processors as the "new oil," noting India's efforts through initiatives like Project Shakti to enhance civilian and military capabilities.

- Ms. Jyoti Pandey observed that India's ambitions in the digital domain are constrained by digital sovereignty debates and imbalances in multi-stakeholder frameworks.

- The discussion concluded with insights from Dr. Samir Bhattacharya, underscoring the need for strategic coherence and international engagement.

SESSION 2: WEAPONISING MINDS – AI, CYBER, AND INFORMATION WARFARE IN COGNITIVE ACTIVITIES

Presentation: Weaponising Minds – AI, Cyber, and Information Warfare in Cognitive Activities

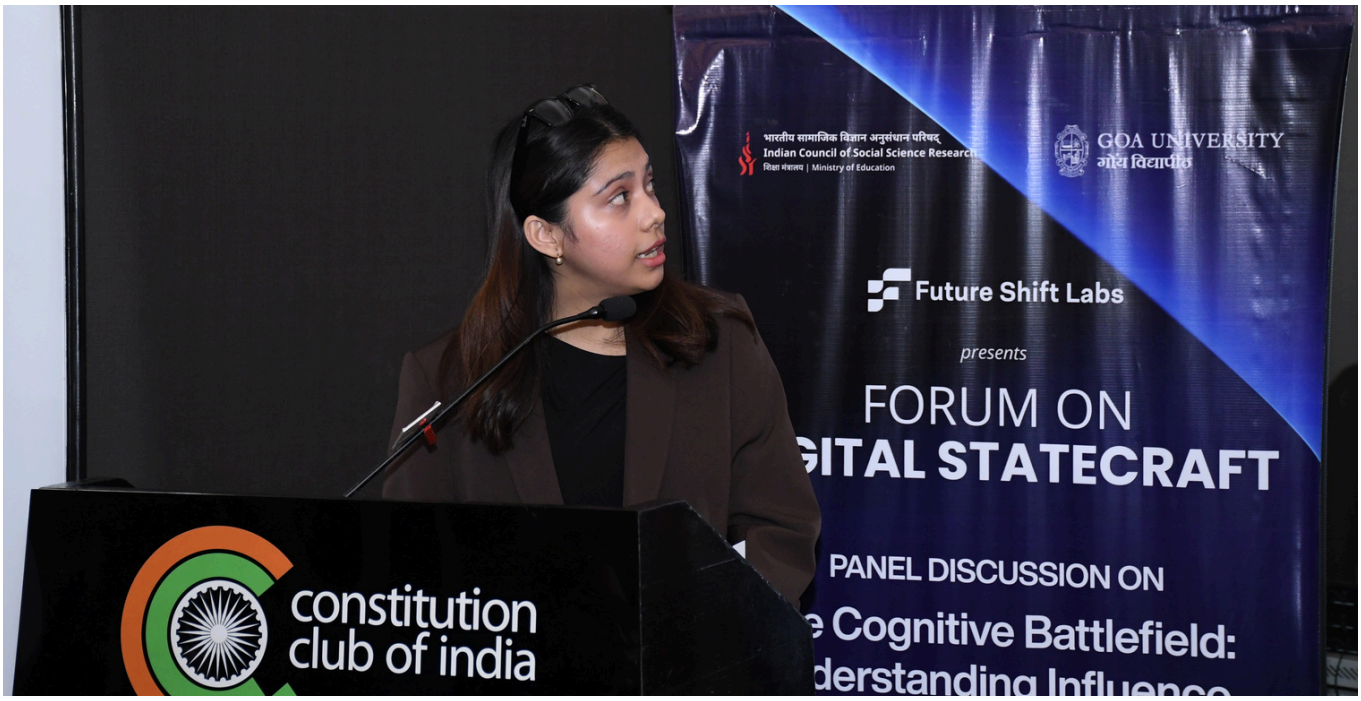
Mateusz Łabuz opened the session by framing the modern battlefield, noting that contemporary conflicts increasingly target human perception, beliefs, and decision-making through digital and information infrastructures. His research analyses how AI, cyber capabilities, and information warfare interweave into cognitive influence strategies, with a particular focus on South Asia.

Łabuz highlighted emerging cognitive threats, the weaponisation of perception, and the use of AI tools such as deepfakes and algorithmic amplification. He underscored the blurred boundaries between cyber, information, and cognitive warfare, and examined vulnerabilities, regional case studies, social impacts, and India's preparedness. His interventions concluded with recommendations to enhance resilience against cognitive threats. Łabuz emphasised the importance of understanding warfare across four domains: cyber, information, hybrid, and cognitive.

Indian Perspective

Bhairabi Kashyap Deka provided the Indian perspective, illustrating the India–Pakistan Conflict of May 2025, during which both sides employed intense information operations with cognitive manipulation. She explained that disinformation in this context aimed not merely to mislead, but to disrupt cognitive processes, induce disorientation, and manipulate perception.

Deka concluded with key recommendations for building cognitive resilience, including comprehensive strategies combining law, politics, education, technology, and international cooperation; strengthening institutions and public trust; developing social resilience through critical thinking and digital literacy; fostering regional collaboration; and positioning cognitive resilience as a pillar of 21st-century security.



Panel Discussion: The Cognitive Battlefield: Understanding Influence Architecture, Social Fractures & Vulnerabilities in India's Information Space

The presentation was followed by a panel discussion moderated by Mr. Prateek Joshi, who highlighted that humans have long been strategic targets, exploited by both state and non-state actors, and noted that reliance on foreign infrastructure compromises data sovereignty.

Key Discussion Themes

- Air Marshal G.S. Bedi emphasized that while cognitive warfare is historically longstanding, technology has introduced new methods of influencing the mind subtly and persistently, differentiating it from traditional propaganda which is more easily identifiable.

- Mohd Ujaley pointed out that cognitive warfare extends beyond individual states, with tactics including media shutdowns, internet control, and social media manipulation to shape public behaviour.

- Dr. Ila Joshi discussed how the sheer volume, repetition, and unverified nature of information can influence perception, noting that India's widespread mobile access and cheap internet make it particularly vulnerable, especially given the digital divide between urban and rural areas.

- Dr. Madhukar Shyam stressed that technology-enhanced cognitive warfare spreads like an epidemic and underscored the importance of individual awareness, citing cases like Jamtara and Lumbini.

The panel concluded that India must shift from "debunking" to "pre-bunking" misinformation, develop its own cognitive resilience toolkit, and reduce dependence on foreign media platforms.

Session 3: FIMI Disinformation Threat: Operation Sindoor & India's Response
Presentation by: Ms. Sunanda R. Marak

Ms. Sunanda R. Marak, author of the research report "Mapping Pakistan's Foreign Information Manipulation and Interference (FIMI) Disinformation Operations Against India: The Expanding Role of Foreign Media and X Influencers in the Wake of Operation Sindoor," opened the session with a detailed presentation of her study.

The report focuses on Pakistan's FIMI campaigns against India following the Pahalgam attack (April 2025) and during Operation Sindoor (May 2025), highlighting Islamabad's strategic objectives and its collaboration with China, Turkey, and Azerbaijan in orchestrating disinformation. The research adopted the EU framework to understand Pakistan's overt and covert operations against India.
Marak outlined the study's objectives: mapping Pakistan's FIMI ecosystem, analysing objective and operational goals, examining Tactics, Techniques, and Procedures (TTPs), evaluating the role of foreign media and social media influencers, and providing recommendations for India's countermeasures.

She identified Pakistan's operational goals, which include delegitimising India's counter-terrorism efforts, portraying India as the aggressor, exploiting religious and ethnic divides, and undermining the reputation of the Indian military and key defence platforms like the Rafale fighter jets.

Concluding her presentation, Marak emphasised that Pakistan's information warfare is a sustained one, though the mediums and methods have evolved from traditional to digital media. She stressed that FIMI poses significant threats to India's national security, foreign policy, and societal cohesion, and recommended a whole-of-society approach, with cognitive deterrence becoming a core national priority to counter disinformation effectively.

Panel Discussion: The Foreign Hand in the Digital Age
Lessons from Operation Sindoor for Strengthening India's Information Defences

Moderated by Dr. Kumari Mansi, the panel examined how Pakistan's strategic use of disinformation during the Pahalgam attack and Operation Sindoor exemplified contemporary information warfare targeting India.

Key Interventions

- Brig. Anshuman Narang provided a detailed analysis of India's strategic foresight during Operation Sindoor, illustrating how Pakistan institutionalised narrative warfare to influence public opinion. He highlighted the role of Chinese influencers in amplifying Pakistani narratives, particularly to portray their defence platforms, such as the JC-10, as superior to India's Rafale jets. He stressed the importance of "pre-bunking" false narratives rather than reactive debunking to mitigate their impact effectively.

- Dr. Sriparna Pathak emphasised that disinformation campaigns are increasingly used by states to gain strategic advantage. She cited the Galwan clash as a case where China tested its ability to spread misleading narratives, which India successfully countered through timely exposure of false information, and highlighted Chinese TTPs.

- Dr. Ankita Dutta explained the EU FIMI framework and how it is applicable to Pakistan's information warfare against India. She underscored that FIMI represents a shift from traditional military confrontation to non-kinetic strategies, requiring awareness, institutional resilience, and collaborative efforts across the state and society to protect information integrity.

- Mr. Shantanu K. Bansal highlighted that India is actively engaged in the information warfare landscape, noting that narrative building is an ongoing process without definitive victory or defeat. He stressed the need for a robust offensive and structural strengthening of India's communication strategies to ensure its perspectives are heard on international forums and social media.

The panel concluded with the shared view that proactive resilience, rather than crisis-driven responses, is essential, and that the effectiveness of information defence ultimately depends on a well-informed and prepared population.

LOOKING AHEAD

The Forum underscored that India is entering a new phase in which information, cognition, and technology are no longer peripheral to strategy; they are central to it. The rise of influence operations, AI-enabled manipulation, and foreign information interference suggests that the defining contests of the coming decade will play out as much in the cognitive domain as in conventional or cyber domains. This shift places new demands on institutions, on knowledge systems, and on how societies negotiate trust and perception.

Several themes emerged with clarity:
First, institutions built for the analogue era will require updating. Information threats cut across policy, security, diplomacy, and society in ways that do not map neatly onto existing bureaucratic boundaries. Cognitive security, disinformation response, and strategic communication will need structured attention rather than ad-hoc or reactive measures.

Second, the responsibility for information security no longer rests solely with the state. Platforms, media, research institutions, civic organisations, and industry all play a role in shaping the informational environment in which citizens form judgments and beliefs. The conversations at the Forum made clear that national resilience will depend on whether these actors can work in concert rather than in isolation.

Third, India has an opening to shape emerging norms in international forums. As debates accelerate on cyber governance, responsible AI, and FIMI standards, India's voice will matter; not only as a large digital market, but as a country attempting to balance sovereignty, openness, and democratic values. The groundwork laid at the Forum points to the possibility of India contributing frameworks rather than merely reacting to those set elsewhere.

Future Shift Labs intends to carry this work forward. Over the coming year, we will deepen our research on cognitive security, FIMI, and digital diplomacy; expand capacity-building programmes; and work with domestic and international partners on education, documentation, and analytical infrastructure. Several threads initiated during the Forum are now moving into more sustained research tracks and institutional collaborations.

The conversations were not an end point, but the beginning of a longer process. The cognitive era presents challenges that are complex and ongoing, but it also offers India the opportunity to define its own strategic posture in the information space. What emerges from this work; across government, academia, civil society, and industry; will shape how India protects its democratic spaces and how it positions itself in the international digital order.