RAMAIAH UNIVERSITY OF APPLIED SCIENCES | CENTRE FOR NATIONAL SECURITY STUDIES

Cyber Vigilance via Intellectual Diplomacy: Role of Indian Think Tanks in Promoting Cybersecurity

2nd Aug 2025 **Antara Jha**

Introduction

In cyberspace, India's think tanks, intellectual hubs of policy innovation, have transformed South Asia's cyber threat response. Viewing digital challenges through India's civilizational lens, they craft robust cybersecurity frameworks to counter terrorism, radicalization, and disinformation. As vanguards in this asymmetric arena, they develop preventive counter-narratives, positioning India as a key player in global cyber diplomacy.

Track II Diplomacy

Indian think tanks are key players in Track II diplomacy, fostering cyber cooperation beyond official channels. Through strategic dialogues, region-focused policy briefs, and neutral platforms, they address digital threats like ransomware, cyber-espionage, and misinformation. Their efforts drive consensus and lay the groundwork for confidence-building measures, contributing to meaningful progress in bilateral and multilateral cyber relations.

Digital Vigilance

Navigating India's data-driven economy, privacy, surveillance, and data protection are key concerns. Think tanks ethically shape India's digital space, influencing data protection authorities, consent-based governance, and surveillance oversight in legislation and debates. As ethical advisors, they align India's cybersecurity with democratic values, balancing national security and digital rights.

Policy Implementation

India's cyber preparedness has improved through research institutions translating theory into policy. The National Cyber Resilience Matrix quantifies sectoral vulnerabilities, prioritizing critical infrastructure protection. Its impact was clear during an attempted power grid breach, where pre-emptive measures prevented disruptions, safeguarding millions of citizens and businesses reliant on stable power.

Building Initiatives

Policy bodies have proven instrumental in conceptualizing and designing initiatives that strengthen India's cyber defence architecture. The framework for the National Cyber Security Exercise (NCSX), now conducted annually, simulates multi-vector attacks on critical infrastructure. This exercise has evolved to include participants from both public and private sectors, creating an ecosystem of coordinated response that significantly reduces reaction time during actual incidents.

Data Protection Architectures

Research institutions have pioneered context-aware data protection frameworks, balancing privacy and national security. Their initial white papers for India's Personal Data Protection framework strategically included data localization to serve both individual rights and national security. This framework's value is evident in terrorist attack investigations, where local data access helped reveal communication patterns and prevent future plots.

Surveillance Mechanisms

Policy research has played a crucial balancing role in developing oversight mechanisms for surveillance activities. Proposed judicial review frameworks for digital surveillance have influenced amendments to intelligence collection protocols. These models balance robust security measures with constitutional protections, creating a system that maintains democratic values while effectively countering threats.

Indigenous Security Paradigms

Research bodies have excelled in contextualizing cybersecurity concepts within the framework of ancient Indian philosophical traditions. Approaches to digital ethics based on concepts of "Dharma" (righteous duty) and "Ahimsa" (non-violence) have created cybersecurity awareness programs that resonate deeply with Indian cultural values. "Digital Dharma," a culturally resonant curriculum in five states, uses narratives to teach online safety, showing better retention than technical approaches.

Value-Centric Digital Sovereignty

Indian research champions a unique digital sovereignty, blending self-reliance ("Atmanirbhar Bharat") with global connection. This framework, distinct from Western and Chinese models, informs India's cyber diplomacy stance. Its appeal across the Global South is bolstering India's intellectual leadership in this domain.

Critical Infrastructure Protection

Sector-specific programs train workers to detect cyber intrusions, as seen in a curriculum for power sector employees that thwarted reconnaissance attempts on distribution networks. These efforts address the human layer of cybersecurity, vital for national security. The 2020 U.S. Colonial Pipeline attack underscores the need for real-time monitoring, a priority Indian think tanks can adopt to safeguard infrastructure.

Bridging Technical and Policy Domains

Think tanks translate complex threats, like the NotPetya malware, into policy guidance for non-technical policymakers. During a 2024 zero-day vulnerability crisis post-terrorist attack, their rapid analysis enabled swift mitigation, protecting government systems. The International Institute for Strategic Studies' threat assessments offer a methodology for Indian think tanks to enhance predictive capabilities, ensuring proactive defences.

Quantifying National Cybersecurity Posture

India-specific cybersecurity indices quantify national cyber resilience across 16 critical sectors, enabling evidence-based policymaking. By pinpointing resource allocation for maximum security, they identified healthcare data system vulnerabilities weeks before a global ransomware attack. This early warning facilitated preventive measures, safeguarding patient data in major medical institutions.

Improving International Cybersecurity Rankings

India's strategic research and targeted policy recommendations significantly improved its global cybersecurity ranking, advancing seven positions in the ITU Global Cybersecurity Index. Enhanced legal and technical infrastructure boosted investor confidence in India's digital economy and strengthened its stance in international cyber diplomacy, marking substantial progress beyond mere numerical gains.

Building Regional Leadership

India has established itself as the intellectual hub for cybersecurity expertise in the region. A Regional Cyber Capacity Building Program has trained over 1,000 officials from neighbouring countries, creating a network of security professionals who share India's perspective on cyber norms and best practices. This initiative has strategically positioned India as the natural leader in regional cybersecurity cooperation, advancing both security and diplomatic objectives simultaneously.

Shaping Global Frameworks

Indian research bodies shape India's stance on global cyber norms, providing detailed policy inputs for UN cybersecurity groups. Their recommendations blend India's civilizational values with strategic autonomy, promoting responsible state behaviour. This resonates with developing nations, balancing digital sovereignty and global cooperation without alienating partners, ensuring India's perspective influences emerging international frameworks.

Cyber Diplomacy and Capacity-Building Leadership

India has established itself as a leader in cyber capacity-building initiatives across the Global South. The "Digital Security Partnership" program has implemented training and infrastructure development projects in twelve countries across Africa and Southeast Asia, extending India's cyber influence while strengthening diplomatic relationships. This work exemplifies the concept of "intellectual diplomacy," where India's thought leadership translates into tangible international partnerships that advance national security interests.

Think Tanks as Technology Watchdogs

Indian intellectual institutions proactively scan emerging technologies like quantum computing, autonomous systems, and synthetic biology for security implications. Identifying vulnerabilities, such as quantum threats to encryption, they drive investments in quantum-resistant cryptography. This strategic foresight positions India ahead of many developed nations in mitigating risks and leveraging advantages from transformative technologies.

Ethical Frameworks for AI Security

India-specific frameworks for applying artificial intelligence in national security contexts balance security effectiveness with constitutional principles. These guidelines have been incorporated into procurement requirements for AI systems used by intelligence agencies. This work has positioned India as a leader in responsible AI development—a strategic advantage as international norms around these technologies are still evolving.

Countering Digital Radicalization

Groundbreaking research on digital radicalization processes specific to the South Asian context has mapped the online ecosystem of extremist content, identifying key intervention points where counter-narratives can be most effectively deployed. This research directly informed the disruption of digital recruitment networks following the discovery of their connection to physical attacks, demonstrating how intellectual analysis translates into operational security outcomes.

Deepfake Detection and Countermeasures

Pioneering methods to detect and counter synthetic media used in disinformation campaigns have been developed. This technology identified manipulated evidence circulated following border incidents, preventing escalation based on falsified information. This capability has become increasingly crucial as synthetic media becomes more sophisticated and accessible to malicious actors seeking to manipulate public perception around security events.

Intellectual Firewalls: Translating Policy to Practice

India has tailored cybersecurity frameworks to its diverse socioeconomic context, adopting a tiered approach to security requirements. This strategy accommodates varying digital literacy and resource availability, ensuring effective and practical measures across urban financial hubs and rural cooperatives embracing digitalization, balancing robust protection with accessibility in India's complex digital landscape.

International Cyber Diplomacy

Through bilateral frameworks, like the Indo-Singapore Cyber Security Response Team, think tanks enhance India's ability to track transnational threats, such as terrorist financing via cryptocurrencies. Their multilateral strategies in UN forums combat terrorist use of the internet, reinforcing India's diplomatic stature. The EU's cyber diplomacy toolbox offers lessons for expanding collaborations.

Multilateral Engagement Strategies

Sophisticated strategies for India's engagement in multilateral cybersecurity forums have established India as a pivotal player in international cyber diplomacy. Position papers have informed India's contributions to UN processes on cybersecurity norms, ensuring that India's perspectives are effectively represented in emerging global frameworks. India's cyber diplomatic efforts have been particularly effective in establishing consensus on combating terrorist use of the internet.

Adapting International Best Practices

The Colonial Pipeline ransomware attack revealed vulnerabilities applicable to Indian energy infrastructure, despite differing architectures. Post-Ukraine power grid attacks, India's power systems adopted enhanced authentication protocols across twelve state electricity boards. The Brussels Airport breach prompted India to integrate cyber-physical security monitoring at airports, thwarting a similar coordinated attack at a major Indian airport.

Developing Indigenous Solutions

India's focus on indigenous cybersecurity solutions has built domestic capabilities, lessening reliance on foreign tech and tackling unique challenges. The "Digital Sovereignty Roadmap" guides this self-sufficiency. Its value was proven when global supply chain issues after international conflicts disrupted foreign hardware access, but Indian institutions following the roadmap-maintained operations with homegrown alternatives.

Conclusion

Indian think tanks are the unseen architects of national cybersecurity, addressing digital threats like radicalization, coordination, and disinformation. Beyond safeguarding digital assets, they shape South Asian cyber norms through intellectual diplomacy, bolstering India's security, regional stability, and global cyber governance. These cerebral sentinels convert tech complexities into policy, build capacity, foster cooperation, and secure India's digital future.