

Prototypicality and platformisation in India's CTI ecosystem

Shashank Yadav

shashank.yadav@iitb.ac.in

Sundeep Oberoi

Shishir K Jha

Research Article

Keywords: Information, Organisational Behaviour, Platformisation, Cyber Security Governance, Policy

Posted Date: August 7th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10097172/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Abstract

The governance of cyber security infrastructures increasingly depends on how decision-makers conceptualise their roles and responsibilities within complex threat data-sharing ecosystems. Drawing on two years of qualitative field work that integrated action research and co-design among public and private sector cyber security stakeholders in India, this paper explores how the emergence of cognitive-linguistic prototypes – the firefighter, the smoke-detector, the bystander, and the *Danda* – shapes organisational behaviour and policy reasoning. Using a disinformation pilot as a methodological stress-test, we demonstrate how these metaphorical frames produce distinct biases in the development, standardisation, and adoption of Cyber Threat Intelligence (CTI) platforms. We show that such socio-cognitive framing contributes to inertia in platform development, fragmented coordination, and constrained innovation in national cyber security infrastructures. By linking cognitive-linguistic prototypicality with the material politics of CTI platformisation, the paper also highlights how mental models of governance influence the evolution of data-driven cyber security ecosystems in emerging economies such as India.

1. Introduction

Cyber Threat Intelligence (CTI) platforms are rapidly becoming a key part of national cyber security infrastructures for incident response and information sharing. Platformisation is the process by which threat information is integrated into automated and scalable digital infrastructures. Like all digital infrastructures, these are central to how organisations coordinate activities, share information, and innovate across complex and emerging security contexts. Given the path dependency of information systems, these systems are also undergoing a function creep where the underlying CTI infrastructure and standards are being repurposed to accommodate newer security contexts and challenges, such as the increasing integration of disinformation and generative AIs in our digital information spaces. Because the standardisation and subsequent platformisation of threat data is the backbone of modern cyber defense and intelligence platforms, several global efforts are underway to standardise and express such emerging digital-cognitive threats in a machine-readable manner (Deibler, 2025; OASIS, 2024; StratComCoE, 2022). However, while standard cyber threats have clear technical boundaries and well defined indicators of compromise (a file is either malicious or it isn't), computer based disinformation is "fuzzy" and sits at the intersection of politics and technology. Consequently, this technical-political ambiguity also serves as a methodological stressor to observe how national cyber security organisations and infrastructures accommodate (or resist) more complex and newer socio-technical threats.

This paper uses this ongoing function creep of disinformation as a lens to reveal the underlying mental and institutional models that govern operational logics and practices in the Indian cyber security sector. Specifically, we embedded ourselves within the Indian cyber security sector and asked: how do the cognitive prototypes held by Indian cyber security stakeholders influence the technical standardisation, development, and adoption of CTI platforms when confronted with the function creep of managing

disinformation as a cyber threat? We argue that these cognitive prototypes do more than just shape organisational behaviour, they dictate the degree of digital sovereignty India can exert by normalising certain infrastructural postures that embed proprietary platforms and legacy governance logics into national cyber strategies. The paper is organised as follows. In the next section, we note the scholarship which forms a backdrop to this work. Section 3 then outlines and elaborates our methodological framework. Section 4 introduces the specific cognitive-linguistic agent prototypes we encountered. In Section 5, we discuss the prototypes' implications and interactions with CTI technology stack and offer some insights for national cyber security and innovation ecosystems. Section 6 concludes with final reflections.

2. Theoretical and Conceptual Foundations

Prototypicality generally refers to the human cognitive inclination to classify and comprehend things by relating them to a mental prototype rather than through rigid classifications. Cognitive-linguistic prototyping implies fuzzy boundaries and a gradient scale – meaning categories don't have strict yes/no membership but central "best examples" (prototypes) and graded membership based on similarity to these metaphorically foregrounded best examples. This enables certain actors and objects within a category to appear more (or less) prototypical than others based on context, reflecting a mental "ideal type" for a category. Prototyping and metaphors are distinct but deeply interacting mechanisms, where the former structures the category and the latter reinforces the prototypical features of its members. Because humans inherently try to understand one thing through the lens of another, more familiar thing (Lakoff & Johnson, 2008), these linguistic prototypes function as psychological tools influencing the subconscious, which are deployed both consciously and unconsciously (Lankton, 2020). This greatly serves the human analytical requirement of categorising various social-professional agents and framing organisational behaviours (Niedenthal & Cantor, 1984), especially in the globalised organisational ecology of CTI production/orchestration where markets and public-private symbiosis not only play a defining role but are also a source of significant structural and discursive power (Yadav & Oberoi, 2025).

A substantial body of theoretical work on mental prototypes exists within cognitive sciences (Geeraerts, 1989; Lakoff, 2007), with themes of organisational prototypicality also having been examined (Niedenthal & Cantor, 1984; Schmitt & Branscombe, 2001; Van Knippenberg, 2023). Furthermore, moral categorisations have been known to influence bureaucratic behaviours (Shiff, 2024). However, in cyber security, behavioural categorisations typically have focused on software users (Ertan et al., 2020; Mashiane & Kritzing, 2018; Moustafa et al., 2021), rather than managers and organisational leaders. This is a substantial research gap, as predominant notions of the quality of organisational outcomes, especially under crisis conditions, directly point towards management and leadership (Deming, 2018). In line with this, International Organization for Standardization (2015) explicitly assigns such responsibilities to top management.

In one study, researchers examined behaviours of cyber security personnel in Western Europe (Baltutis et al., 2024), but such researcher-imposed categorisations through survey response clustering do not

capture participants' own self-concept or cognitive-linguistic prototyping. Additionally, the examination of cognitive styles in information systems development and practice has largely concentrated on the narrow, individual-centric information processing (Benbasat & Taylor, 1978; Chae et al., 2020), neglecting how languages and metaphors categorising the world and organisational environments shape institutional decision making.

At the organisational level, software automation infrastructures can often embed those underlying behavioural logics by storing, integrating, and actualising various organisational intents and capacities (Thomas et al., 2014). This platform characteristic further contextualises the continual extensions and customisations of the underlying CTI standards to address novel threats and organisational requirements (Menges et al., 2019; Ussath et al., 2016). Prominent standardisation bodies have acquiesced to this expanding scope of CTI feeds and adopted the same route to expand CTI standards like STIX for integrating data about online disinformation (Minto, 2023). Various national cyber security organisations, including the Indian Computer Emergency Response Team (CERT-In) also rely on same global standards and platform operations for producing and exchanging cyber threat information (CERT-In, 2020). Despite this, there exists an acute paucity of literature studying organisational behaviours surrounding the deployment of CTI infrastructures (Ainslie et al., 2023), with most works focusing on technical implementations and evaluations (Bouwman et al., 2020; de Melo e Silva et al., 2020; Kotsias et al., 2023), and not the psycho-organisational framings which steer the adoption and operations of CTI technologies. Thus, the socio-cognitive mechanisms by which critical organisations and stakeholders conceptualise and implement CTI governance, as well as how they view and align their activities in lieu of their digital information infrastructures, remain less understood and researched.

It is only fitting that the nomenclatures of cyber security practice themselves are steeped in metaphorical reasoning, drawing from rich biological and spatial equivalences that deeply shape the security realities of cyberspace (Betz & Stevens, 2013). However, by implicitly reframing technology policy problems in terms of things that feel more "commonsensical", metaphors can also quietly remove the rhetorical resources of opponents and alternate socio-technical architectures (Branch, 2021) – affecting the material, normative, and conceptual aspects of digitisation (Larsson, 2017). For emerging economies with limited resources like India, such invisible and informal policy agenda-setting could mean embarking on long term suboptimal trajectories of technological development which remain unchallenged and accepted as the natural order. Because this prototypicality influences the emerging AI and disinformation threat data infrastructures within the national cyber security ecosystems – impacting the corresponding standardisation and formulation of socio-technical policies and practices – the absence of research on cognitive-linguistic prototypicality in cyber security scholarship within India's digital sector, or even globally, represents a critical oversight.

3. Researching India's Cyber Security Information Infrastructures

To investigate how cognitive prototypes steer the technical and strategic evolution of India's cyber security landscape, this research followed a multi-phased, two-year design and action research trajectory

(2023–2025). This longitudinal and immersive approach was necessitated by the 'fuzzy' nature of digital-cognitive threats as well as cognitive-linguistic models, which traditional snapshot-based methods fail to capture. Following an inductive analytical approach, we identified patterns and recurring metaphors through field notes made over this sustained longitudinal engagement. We observed that participants consistently used a shared vocabulary to refer to roles and responsibilities within the cyber security ecosystem, invoking terms such as “firefighters” and “bystanders”. We treated these recurring self-descriptions as indicators of shared role-based mental models. The “*Danda*” prototype, in contrast, was not a self-description but derived from repeated references to enforcement and authority oriented logics in participants’ accounts of governance.

The study began in early 2023 with the development of a foundational CTI model for social bots, facilitating technical engagements with global stakeholders including the DISARM Foundation and OASIS. By late 2023, the research transitioned to the Indian national context, initiating a series of consultations with CERT-In leadership, industry actors, and stakeholders from the Bureau of Indian Standards (BIS). This culminated in 2024 with the development of a STIX-compliant 'Communications' specification and an immersive co-design pilot involving longitudinal interactions with high-level stakeholders (N = 28) from the Indian cyber security community and IIT Bombay’s Trust Lab. Concluding in mid-2025, these interactions provided the empirical 'stress-test' necessary to formalise the cognitive-linguistic prototypes. By observing how these actors adapted existing infrastructures to accommodate the non-binary threats of disinformation, we were able to surface the underlying mental models, or prototypes, that otherwise remain invisible in 'business-as-usual' technical operations. In this process, we also helped prepare our stakeholders’ CTI infrastructures to better integrate disinformation-oriented threats in their cyber situation awareness pipelines.

A breakdown of these stakeholders is offered in the Table 1 below. All participants were senior information technology professionals who engaged voluntarily with us based on their professional interest in the research, which was limited to their vocational experience with CTI software deployment and standardisation. Participants were informed about the nature of the study and their right to withdraw at any stage. No personal data was collected during discussions, and no audio/video recordings were made or stored. The research did not pose any risks from study procedures, did not involve any vulnerable populations, medical data, or bio-safety concerns, and was accordingly assessed as minimal risk by the institutional review board. We have further maintained confidentiality by anonymising participants’ specific inputs and aggregating/generalising quotes in the paper.

Table 1
CTI Stakeholder/Participants Breakdown

Stakeholder Type	Percentage	Key Representations	Role/Expertise
C-Level Cyber Security	43%	CISOs/CIOs	Strategic cyber security leadership, organisational decision-making on CTI governance and policy direction
Management Leaders	21%	SOC Managers, Threat Intelligence Leads, Cyber security product/operations managers	Business, marketing, and operational management of CTI platforms
Developers/Analysts	11%	SOC developers, security analysts, CTI platform engineers	Technical development, CTI integration, threat analysis, software and infrastructure implementation
Government Stakeholders	25%	Leadership from CERT-In and BIS	National cyber security coordination, standardisation, regulatory and policy engagement

4. Prototypicality in India's CTI Ecosystem

Understanding the diverse roles assumed by decision-makers and organisations in emerging cyber security contexts, such as AI-driven disinformation, is essential to inform policymaking and analysis. Our work revealed that many policy actors perceived themselves as occupying structurally rigid roles within India's national cyber security ecosystem, interpreting their technical-regulatory environment primarily through the lens of managing security incidents and meeting political or business expectations. This constrains institutional adaptability to address non-conventional threats, narrowing the scope of proactive threat mitigation and socio-technical innovations, while reinforcing siloed, compliance-driven modes of cyber security governance.

Drawing a parallel with an urban fire response, our participants frequently described themselves and other stakeholders as firefighters, bystanders, or smoke detectors. We have further added to this set of roles by identifying an additional regulatory agent prototype, which our discussants and collaborators often referred to as the *Danda*. These prototypes function as both cognitive and analytical tools – they enable actors to rationalise and contextualise their actions within the broader environment while also facilitating the interpretation and anticipation of others' behaviours. In both respects, these cognitive-linguistic prototypes operated as implicit anchors that shaped the direction and scope of our stakeholders' actions. We elaborate on each of these prototypes in turn.

4.1. Firefighters

Primarily, the firefighter prototype actor is focused on being able to react quickly to incidents and address immediate threats. Owing to the expectation of managing real-time crises, actors adopting this mental model often justify inaction on non-immediate matters which are outside their perceived crisis thresholds. Even health workers during the COVID-19 pandemic were described as firefighters (Semino, 2021); however, when internalised as a basis of self-concept, such prototyping transcends rhetoric to become a cognitive framework guiding real-world behaviour, fostering a crisis-driven governance rationality in information systems and security. Consequently, by grounding actions in emergency logics, this prototype prioritises short-term remediation over long-term infrastructural strategy, contributing to policy inertia in platform development and public-sector innovation.

Prototypical firefighters such as the cyber security Incident Response Teams, typically engaged with data breaches, ransomware, and other malware incidents, extend this firefighting rationality to their interpretation of technical CTI standards – particularly when addressing ambiguous threats such as online disinformation. Since disinformation lacks the immediacy of a “raging fire,” actors tend to defer action, leading to prolonged uncertainty and stagnation in technology strategy and decision-making. This was evidenced during our interactions when a national cyber security leader described bot-driven disinformation as being on his “radar,” yet admitted to lacking the “bandwidth” to address it – indicating that organisational resources remained absorbed by containment and recovery efforts against the more conventional cyber threats.

The recurring issue of limited organisational “bandwidth” is prevalent among actors embodying the firefighter prototype, often constrained by how their Key Result Areas (KRAs) and Key Performance Indicators (KPIs) are defined. This reflects a degree of cultural transfer from private-sector management practices into government settings. As standardisation and R&D in India typically fall outside most industry actors’ KPIs and KRAs, such tasks are readily dismissed as “not my job.” Even regarding participation in our experimental pilot, several respondents cited limited “bandwidth,” using the term as a euphemism for workload pressures and the continual negotiation of responsibilities within the cyber security ecosystem. Consequently, even when KPIs, KRAs, or R&D agendas exist, immediate firefighting imperatives within platform infrastructures tend to override longer-term or non-crisis priorities. As a senior cyber security advisor who had worked with several ministries and law enforcement agencies remarked – *CERT-In are the guys government calls after an incident for breach analytics and forensic requirements, they wouldn’t have the resources or even will to parse unstructured digital media artifacts spreading online for an early warning system* – highlighting a fundamental cognitive obstacle where disinformation is treated as an ‘incident’ in the sociopolitical sense, but it does not resemble the kind of post-incident, contained response work which defines the firefighters’ operational reality.

This prevailing firefighting orientation within public-sector cyber security organisations also reflects how political leadership conceptualises the role, scope, and strategic value of cyberspace governance. National cyber security firefighters simultaneously function as bystanders in global standardisation processes, implementing externally developed norms within domestic contexts. Nonetheless, the limited resources available to these actors warrant an acknowledgment. When cyber security leaders cite a lack

of “bandwidth,” it typically denotes team – or department-level resource constraints, which in turn serve as justification for de-prioritising standardisation and innovation. Given the widespread recognition of cyber security’s strategic importance among policymakers and in public discourse, a critical question arises regarding why there are still bureaucratic hesitations and obstacles in the flow of resources to firefighters?

The answer, unexpectedly, lies in the often obscured but inherently strategic intent driving cyber security operations. As has also been noted by leading cyber security experts (Anderson, 2001), cyber security, only in the ideal world, is practiced for the altruistic goals of safeguarding the citizen-users or their activities and digital data and footprints. In the real-world, the actual flow of resources happens only to reduce any potential business liability and political hazards. Once we take this correspondence between resource allocation, and the potential cyber risks and liabilities from disinformation that could be actually felt at the political level, and juxtapose that in government with the bureaucratic subordination of the scientific rationale (focused on building and creating) to the rationale of the policeman (focused on arbitration and enforcement) in a highly technical field – we come to better understand why our cyber security leaders can do little but prototype themselves as firefighters in a chaotic techno-regulatory environment dominated by enforcement rather than innovation.

4.2. Smoke Detectors

In cyber security, the prototypical smoke-detectors are the quintessential CTI providers, expected to monitor the cyberspace and detect threats and malicious activities in a proactive manner, propagating the corresponding threat data as alerts through dedicated platforms, and keeping the integrity of information products and communications. The *raison d’être* of this actor surrounds the act of detection – to the extent that, when presented with a CTI schema for disinformation, several SOC solution providers immediately asked whether an algorithm or plug-in for detection was available.

Many automated security systems integrate heuristic and machine learning models that supplement and perform similar detection roles, while external vendors and actors also supply CTI as a commercial/non-commercial product. Smoke-detectors’ strong data-centric orientation often drives their deeper involvement in data standardisation and platform capability development – *we will workout with CERT-In and then if you like take this up with OASIS for formal standardisation* – as a platform vendor with significant monitoring and detection orientation explained to us during a technical discussion. However, smoke-detectors generally remain detached from concerns about how firefighters use their threat data in the real-world, or from broader ethical and human-interest considerations, being grounded in the acquisition and processing of threat data. From the vantage point of disinformation or social engineering automation, the experience of this prototype underscores how the political economy of data circulation can restrict the capacity of states and institutions to establish collaborative cyber security infrastructures.

Cyber security smoke detection, particularly in areas such as disinformation and social media analytics, operates within a crowd-sourced, distributed, and industry-driven ecosystem. Public-sector firefighters

primarily depend on multiple, often competing, sources of commercial CTI and automated analytics platforms, reducing incentives for in-house development or maintenance of such systems. Given the limited availability of commercial CTI services from Indian providers, knowledge transfer and spillover to the domestic cyber security sector have been minimal. Consequently, national cyber security organisations face a dilemma between meeting their immediate need for ready-to-use intelligence products, and fostering a domestic CTI industry. Emerging local players in this market must therefore compete not only with established international vendors but also with a firefighting rationality that offers them neither policy protection nor developmental incubation. Notably, consistent with the graded nature of these prototypes, firefighters tend to engage in detection functions to a significantly lesser extent than specialised CTI providers. *He has the gun, just tell him who to fire on* – as a private sector cyber security stakeholder once quipped to us about his government counterpart – *but don't ask him to go scouting for threats himself*.

Moreover, public organisations often delegate the data mining and social threat detection to obscured third parties due to the reputational risks associated with public surveillance and communications monitoring. We gradually learnt from one of the API providers we reached out to procure online social data that some of the Indian government agencies were already their clients, although potentially unbeknownst to each other, and unsurprisingly none of our stakeholders admitted to such existing arrangements either. The cultural influence of Western privacy norms has made even the acknowledgment of scraping or analyzing publicly available social media content politically and ethically sensitive, often triggering hasty and politically reactive regulatory responses (Jung & Kwon, 2024). As a result, governments seeking such capabilities for security and law enforcement purposes like to maintain plausible deniability, relying on a competitive yet niche market of prototypical smoke-detectors to fulfill these arguably contentious functions.

Smoke-detectors also encounter substantial entry barriers in addressing digital-cognitive threats due to restrictive API pricing structures imposed by data merchants. Such pricing functions as a form of infrastructural gatekeeping, determining which actors can participate in the disinformation-focused CTI ecosystem. The current social network API frameworks consolidate knowledge and power through monetisation models that impose rate limits on free tiers – such as those offered by platforms like Meta – while tiered pricing structures create unequal data access. At the highest tiers, costs are often determined through extended negotiations and can reach millions of dollars, merely for automated access to publicly available content, rendering social smoke detection highly exclusionary (Stokel-Walker, 2023; Voorhees, 2023). As a result, the high-volume, high-velocity data requirements of disinformation CTI production grant API providers disproportionate leverage over which organisations can operate as social smoke-detectors. Furthermore, despite being ostensibly machine-to-machine interfaces, commercial API integrations typically also necessitate extensive human interaction for sales, technical support, and customised pricing, particularly with the niche vendors.

Among established smoke-detectors in cyber security, disinformation-related CTI is generally regarded as less valuable than other, higher-volume and higher-value threat intelligence data. Our interactions

often revealed that stakeholders organise their workflows and business models around tactical and operational intelligence needs, with disinformation treated primarily as a strategic concern. Consequently, only the largest platforms with sufficient “bandwidth” tend to integrate such strategic CTI, like online disinformation, into their dashboards and are more inclined to engage in its early standardisation efforts. Depending on client requirements, some vendors do embed some social communications monitoring within their data loss prevention tools, but typically avoid addressing influence operations or bot-driven narratives. These concerns are instead delegated to the marketing or reputation management teams, who rely on a separate ecosystem of platforms (Ziegler & Skubacz, 2012) largely detached from cyber security operations and concerns.

For private-sector cyber security teams, disinformation-related threats and technologies are typically peripheral concerns. This weakens their incentives to coordinate with any internal social smoke detection teams engaged in real-time, data-driven brand and reputation monitoring – thus both mutually also acting as bystanders to the other. As a result, online influence tracking tools are developed and marketed primarily for business users in marketing departments, remaining disconnected from IT and security procurement workflows. Consequently in the domain of social engineering CTI, smoke-detection often suffers from poor intra-organisational interoperability.

Professionals with expertise in disinformation monitoring – commonly found in public relations or advertising – lack the technical vocabulary of IT teams and have limited understanding of cyber security infrastructure's potential role in countering bot-driven manipulation. This results not in a clean division of labor, but rather a fragmented overlap where capabilities and responsibilities relevant to online influence tracking exist across business and security functions, yet remain embedded in distinct workflows and procurement logics which operate with different analytical frameworks and operational priorities. A high-level technical security planner who had advised several governments on both cyber security as well as influence operations equated this organisational experience with the interoperability issues he encountered in the tactical integration of online propaganda and deception planning within armored military operations. This misalignment steers how organisations’ disinformation risks are technologically defined and acted upon. Thus, while the firefighters maintain a procedural isolation from CTI standardisation, their smoke-detector counterparts are characterised by a corporate form of bureaucratic fragmentation that similarly hampers organisational preparedness to innovate and develop non-conventional threat mitigation standards.

4.3. Bystanders

As the fragmentation of smoke detectors also suggests, the prototypical bystanders choose to stand near the site of the fire and watch, sometimes offering a cheer and sometimes documentation. The bystander prototype does not engage directly with the cyber threat environment, preferring instead to observe from a safe distance, even document, analyse and recommend the practices and standards of firefighters and smoke-detectors. This can include an organisation’s executive management, Standard Development Organisations (SDO), policymakers, users, and even the auxiliary third-parties and consultants. For cyber security operations, this is a peripheral, but often complex and critical function

whose responsibility (given the multiplicity of bystanders and SDOs) is presupposed to be diffused in the environment. And given that baseline diffusion of responsibility, there can emerge an externalisation of the firefighters' CTI standards requirements – as has been the case with the passive adoption of global CTI standards and practices in various local cyber security environments.

In India, BIS exemplifies the bystander prototype through its institutional identity as the national SDO. Unlike the American National Standards Institute, which evolved over a century of bottom-up industrial initiatives and became embedded in national policymaking (Agnew, 1928), BIS originated through a top-down legislative process in 1986 that merely rebranded the earlier Indian Standards Institution – created post-independence via state intervention in 1947 (Bantu et al., 2020). Thus, while in the US technical standards have emerged to harmonise voluntary industrial practices, BIS has historically operated within a state-driven top-down model, leading to a "waiting for instructions" or "checkbox" mentality that hinders frontier local technological innovation for emerging security contexts. Eventually, this produces specifications designated as national standards by default, irrespective of their practical adoption or sectoral relevance.

The bystander prototype, in this context, functions as a cognitive frame that prioritises compliance over operational agility. This distinction is central to the organisation of corporate networks in bystander work. During our discussions, a key BIS member noted the risk of letting industry take the wheel in IT standardisation – because then, *they start conflicting and competing with each other*. Clearly, the BIS mandate and organisational control over cyber security standards development in India could suffer with a shift from writing specifications to a mere coordination and conflict resolution paradigm, possibly also making this cyber security bystander less contingent in the scheme of national influence in global (particularly transnational) organisations. While BIS does take inputs and requests from industry member committees, it is not particularly encouraging of industry initiative in and of themselves, and thus also is a passive enforcer of the prevailing local institutional status-quo of top-down state-led IT standards development, thus occasionally overlapping with the *Danda* prototype.

The bystander prototype typically does not act on cyber security needs proactively – it responds only when formally mandated, following which it establishes committees and procedural mechanisms to draft specifications or guidelines. Upon asking why had they not considered contributing to emerging security platform standards, BIS officials pointed that they had received no such requests from concerned government authorities – who operate on a firefighting rationale. Standardisation work in these contexts involves a blend of development, negotiation, and adoption processes. However, the bystander's prototypical disposition limits both entrepreneurial initiative in promoting standards' adoption and active engagement to advance national interests in industry-led standardisation. Positioned as a bystander to the operational realities of cyber security production, India's national SDO thus often adopts globally dominant designs with minimal contextual adaptation and without much consideration of local security theater specific requirements. Given the political nature and sensitivities of online and automated disinformation, it is deemed better to avoid active and overt public engagement in corresponding technical standardisation.

The bystander approach to cyber security standardisation – treating it primarily as a bureaucratic exercise in specification drafting rather than as a process of sustained market negotiation, transnational consensus-building and adoption, reflects an administrator–policeman rationality rooted in top-down control. Within this model, industry and civil society are seldom treated as equal partners. Such institutional insularity from operational realities can foster an illusion of technological maturity, prompting premature regulation and misinterpretation of emerging innovations. This dynamic contributed to significant policy fluctuations surrounding the development and adoption of Large Language Models in India (TN Tech Desk, 2024) – a pertinent technology to online information cascades. By framing governance in terms of procedural compliance and maintaining an observational stance, bystanders tend to endorse and import global standards rather than shape them – thereby perpetuating structural dependency and constraining domestic innovation.

4.4. *Danda*

The *Danda* is an institutional prototype (unlike the previous three social ones) which conceptualises governance as the exercise of authority through coercive enforcement and punishment. Literally denoting a rod or staff, it carries distinct political connotations. As articulated by Chanakya in the Arthashastra, *Danda* represents the sovereign authority and the prerogative to punish (Rangarajan & others, 1992). Similarly, the Manusmriti also describes the *Danda* as the supreme instrument of rule over the population (Meena, 2005), positioning it as the ultimate emblem of stately power.

More colloquially, the *Danda* is also the weapon of choice for the swathes of police constabulary in India, and thus a ubiquitous mediator of the common man’s everyday experience of the state on the street. The dominant narrative of the Indian independence movement itself has been built significantly around accounts of non-violent Gandhian protesters confronting British *lathi*-charges, however, many of the same coercive institutional structures that had been subject to critique were retained post-independence with little to no transformation (K. S. Subramanian, 2021). In the contemporary context, the National Security Council Secretariat, the apex coordinating body for cyber security in India, occupies a position that reflects both residual coercive logics along with a bystander orientation for coordinating the firefighting and smoke-detection functions across the government.

Cyberspace, with its transnational infrastructures and reliance on algorithmic governance and “best practices,” appears to call for less coercive modes of security governance. Yet, the *Danda* retains its historical and institutional significance, acquiring even newer meanings and applications. As a senior firefighter put it, he *could just shut down social media and force those companies to comply* with a swing of *Danda*, suggesting that he does not really need to commit time and resources for online media monitoring and response standards despite acknowledging the growing scale and sophistication of automated social engineering threats. The key insight here is the *Danda* driving enforcement logic as a substitute for capability-building. It thus continues to embody the traditional policing rationality while also emerging as both an impediment to and an organiser of scientific rationality – each playing a critical role in national cyber security. While this reinforces the state’s regulatory authority, it

simultaneously constrains the governance landscape by framing information infrastructures primarily through the lens of enforceability rather than adaptability or collaboration.

Another firefighter we interviewed, who had quite successfully managed a major ransomware incident at one of India's largest power sector organisations, attributed his effectiveness to being granted complete freedom to "use his *Danda*". In this context, *Danda* served as a metaphor for both personal skill and managerial authoritarianism. This perspective reflects the policing mindset that views the *Danda* – with its connotations of fear and coercion – as universally effective. By equating governance with punishment, this logic privileges compliance enforced through punitive authority, thereby constraining opportunities for co-creation and collaborative infrastructuring, and reinforces hierarchical, top-down approaches to CTI standards, practices and policies. While the *Danda* remains readily and immensely useful for its punitive functions, having led to stricter rules around the reporting of cyber incidents or heavy financial penalties for the breach of personal data protections – it fails to create a positive incentive structure for mobilising stakeholders towards long term goals that are not a compliance burden.

Consider the case of India's National Cyber Security Policy, unveiled in 2013 (MeitY, 2013), whose proposed update has remained in draft form for years despite significant changes in the technological landscape. Its structural inertia reflects a persistent deadlock between the *Danda* and the bystanders – the bystanders wait for the *Danda* to provide a mandate, while the *Danda* prioritises enforcing incident control over developing technology roadmaps. Interestingly, the 2013 document had envisioned participation of industry in cyber security standardisation, but the overlapping framings of *Danda* with prototypical cyber security stakeholders, especially the bystanders, have kept this implementation restricted. Here, BIS tends to prioritise its role as government's quality control arm by acting as a 'conformity assessment agency' – as an official emphasised, *this is where they derive much of their revenue from* – thus deriving its organisational validation more effectively from wielding the *Danda* and not the adoption of its technical outputs.

Within the organisation of national cyber security, the *Danda* also serves functional purposes for the scientific bureaucracy by shaping practices in vendor management, public–private collaboration, or breach reporting and assessment work. The ready availability of *Danda* arguably also inclines such stakeholders towards fulfilling their immediate needs for finished CTI products over the co-development of a domestic industry, a pattern which could be reflective of high-technology public procurement practices in the wider defense sector (Kundu, 2021) and not just in the CTI or cyber security policymaking. Our observations indicate that policing and scientific rationalities in cyber security are not exclusive to their respective institutional domains. Even ostensibly scientific organisations may pivot from creation and innovation toward enforcement and policy control – enabled by wielding the *Danda*. This tendency has several historical precedents in the evolution of India's computing and technology ecosystem (C. Subramanian, 1992).

The prototypicality of *Danda* lies in its status as an institution so diffused with Indian polity and administration that its manifestations, whether material, legal, spiritual, or organisational, often defy characterisation other than just being a variant of the *Danda*. Most importantly, the pervasive influence of this institutional prototype has limited the adoption of CTI as a potential tool of global soft power (Yadav & Oberoi, 2025) – for neither the firefighters nor the bystanders can meaningfully engage with the strategic possibilities of CTI without potentially trespassing in the eyes of the *Danda*. In contrast, smoke-detectors tend to treat CTI's strategic dimensions as commercial and marketing opportunities, introducing some further analytical complexities into stakeholders' cyber situational awareness (Oosthoek & Doerr, 2021). Following the Machiavellian notion that a ruler is only as good as the quality of his counsel, it may be surmised that democratic political leadership often remains insufficiently attuned to the global techno-politics underlying CTI production and dissemination. Under the influence of the *Danda*, CTI production and orchestration is thus framed narrowly as an operational necessity rather than as a strategic instrument requiring collaboration with pool of non-state technical expertise. Moreover, the inherent contestations surrounding disinformation in democratic contexts obscure bureaucratic and political visions for its CTI development – as illustrated by the Trump administration's recent stance toward disinformation research (Kelley, 2025). In this sense, the prototypical *Danda* frequently positions itself on the wrong side of innovation.

In fact, all of the social-psychological identities in India's professional cyber security management circles are shaped in relation to the *Danda*. Upon asking the question – *who am I and what am I doing* – the firefighter, the smoke-detector, and the bystander would come to reformulate the question to anchor their activities in congruence with the requirements of avoiding the *Danda*, becoming its attendant keeper, or both if their circumstances and fortunes are favorable. It is thus, that the social and organisational behaviours which emerge from interactions between the three social prototypes and the fourth institutional prototype, have been found to contour the socio-technical ecology of governing emerging threat information in the Indian cyber security sector.

5. Discussion

As noted earlier, the social prototypes discussed here are not fixed or mutually exclusive. A firefighter acts as a bystander in standard-setting environment, while a smoke-detector could assume a firefighting role when its own digital infrastructure is threatened. At the systemic and national levels, however, Indian cyber security ecosystem consistently reflects these three social prototypes, each interacting with the structural dynamics of technological evolution and the overarching institutional prototype of the *Danda*. While we have been fortunate to encounter and observe these through the prism of the emerging landscape of disinformation and automation, we concur that these are but universal prototypes in a chaotic organisational environment where software and cyberspace meet the existential rigidities of security operations.

Ostensibly, disinformation related CTI remains a peripheral component within CTI platform infrastructures – an experimental add-on being shaped by competing political–security blocs seeking to

standardise it to their advantage. The boundaries and social protocols governing automation in this domain remain ambiguous for most prototypical actors, owing to the inherently political and subjective character of disinformation threats. Nonetheless, our observations indicate that disinformation has emerged as a distinct feature in intelligence software and a potential source of competitive differentiation and market advantage among existing CTI platform vendors.

But one may ask here, what does it really mean to platformise the CTI? In our interactions, some senior firefighters have questioned the need for dedicated CTI platforms, suggesting that threat information could just as easily be shared via WhatsApp or email. However, the rationale for platformisation rests on three interrelated dimensions – situational awareness, automation, and interoperability. To platformise CTI is, therefore, to bridge the gap between human and computational capacities in processing cyber security data, rendering threat intelligence operationally manageable at the speed and scale demanded by contemporary globe spanning digital information systems.

Given the centrality and dependency over CTI platform infrastructure to meet the organisational remit in cyber security, the infrastructural platform is often able to exercise an “architectural leverage” over the wider socio-technical ecology of an organisation (Thomas et al., 2014). Managing this infrastructure, however, is harder than it looks for a firefighting organisation, and thus a delegation of control occurs to a dedicated vendor who can take ownership of various standards driven platform engineering tasks, leaving the firefighters more time to think about and respond to “the smoke” than building and then managing the CI/CD of their smoke-detection systems. This accords to the actors actually controlling the infrastructuring process an invisible but pervasive sort of control over platform capabilities. This leverage translates into a subtle yet not-insignificant asymmetry of control, one that cannot be easily contested within the prototypical modes of governing the cyber security ecology.

The policy consequences of this dynamic can be discerned from the broader societal effects produced by contrasting variants of platform engineering practices. In cases where multi-homing architectures prevail – and where actions are guided more by scientific rationality than by self-imposed prototypicality – the resulting digital infrastructures tend to generate their own communities of practice (Magalhães, 2011; Pipek & Wulf, 2009). These communities quite organically incentivise and nurture those technology actors who are capable of assuming paradiplomatic roles in transnational cyber security environments, thus promoting local influence in global environments.

This is exemplified by the developers and public-private ecosystems surrounding CTI platforms such as the Malware Information Sharing Platform (MISP) and OpenCTI, which have catalysed new research directions and product development initiatives (Dalamagkas et al., 2024), even international techno-security architectures over computer based disinformation (EEAS, 2023). On the other hand, reliance on proprietary or closed CTI platform infrastructures to fulfill public sector cyber security requirements tends to erode opportunities for software multi-homing, as platform vendors are naturally reluctant to open their “black boxes” to scrutiny or experimentation by civil society actors and red teams. This consolidation of infrastructural control away from prototypical stakeholders of cyber security not only

limits transparency but also narrows the developmental imagination of cyber security organisations. However, because the imagery of fighting fires in itself imbibes a certain authority and heroic self-image, it establishes a natural legitimacy of the ways prototypical cyber security organisations in India are addressing their technological contexts, which is appropriately under the "temporal squeeze" (Charteris-Black, 2017) of fire where immediate action always overrides the wider national techno-economic and digital-industrial alternatives.

Multi-homing in CTI platformisation, consequently, can be understood to operate at two distinct levels. The first where a firefighter like CERT-In maintains access to and interoperability across multiple competing CTI platforms, while being a bystander to their development. The second where elements of the platform's infrastructure are made accessible to external developers and open-source communities for experimentation, adaptation, and "hacking". The latter, as demonstrated by several prominent CTI platforms originating from public-sector (Ghura, 2023), fosters innovation, transparency, and collective problem-solving qualities that proprietary architectures often suppress in favour of commercial secrecy and vendor lock-in opportunities. The latter sort of multi-homing typically manifests in societies with better integrated regulatory and technical universes, gradually cultivating a homegrown and mature CTI sector (Jesus et al., 2023).

Because firefighters are largely driven by a procurement-oriented mentality, focused on acquiring immediate technological solutions to their smoke-detection needs, they seldom engage in the long-term infrastructural politics of the global cyber security norms, standards and governance – which are increasingly becoming a domain of their vendors (Fairbank, 2019; Hurel & Lobato, 2018). Consequently, the main contest for digital sovereignty unfolds between two divergent systems of infrastructural organisation – the platform-owned closed ecosystem, and the community-of-practice oriented open ecosystem. Prototypicality subtly privileges the former by reinforcing dependency on proprietary infrastructures and thus shifting the locus of control away from digital sovereignty, capacity-building, and participatory standard-setting.

The implications of prototypicality are visible in how questions of platform control and openness are negotiated. Concerns about constraining foreign platform power (Fratini et al., 2024) appear to have limited influence on organisational rationalities which are driven by their cognitive prototypicality. Inadvertently, most firefighters, especially within the private sector, find themselves operating inside insular and fragmented information systems, constrained by limited interoperability and access barriers. Many private-sector participants in our study deplored the closed nature of government CTI platforms, which makes the consumption and contribution of threat data unduly difficult. This sentiment was largely consistent across organisational types. Several participants unequivocally advocated for the establishment of a national CTI sharing infrastructure built on open-source foundations. Such a platform, they argued, could serve as the "ground-truth" architecture for cyber security collaboration – an accessible digital commons where emerging CTI standards requirements and practices could be developed, tested, and refined in practice.

The fragmentation and interoperability constraints described above can be traced to a broader misalignment in the objectives and preferences of prototypical agents, as summarised in Table 2. This resonates with van Dijck, Poell & de Waal’s account (2018) of the “platform society”, where infrastructures embed particular logics of power. Within the Indian cyber security ecology, the firefighter and the *Danda* embody reactive and coercive governance logics focused on control, enforcement, and incident response. In contrast, the smoke-detector and the bystander enact anticipatory surveillance and procedural dependency, emphasising monitoring and compliance rather than creative infrastructuring.

Stakeholders’ reliance on prototypical framings obfuscates the fact that CTI standards are both logical infrastructures as well as global public policies, which is complicated by the status-quo orientation of our prototypical actors. The commonly experienced technological lock-in and switching costs with respect to the legacy IT systems can thus also be inadvertently transferred over to the public policy domain, even though the policymakers themselves may not be accustomed to thinking about code as policy or policy as code yet. In our view these misalignments allude to a deeper problem of high-level stakeholders in cyber security sector of not seeing themselves as primarily software engineering based organisations. Software is just the beast they are forced to deal with in order to carry out their prototypical expectations and avoid the *Danda*.

Table 2
How prototypical agents in India approach the platformisation of CTI data

Installed	Firefighter	Smoke-Detector	Bystander	<i>Danda</i>
Base	Prefers	Prefers	Indifferent	Incentivises
	On-premises	Cloud-native		On-premises
Platform Engineering	Prefers	Prefers	Indifferent, but	Incentivises
	Closed Source	“Inner Source”	cheers for Open-Source	Closed Source
Social API	Prefers	Faces API Pricing	Indifferent	Indifferent
Management	Third-party curation	Limitations		
CTI	Automation	Monetisation	Indifferent	Limits
Data	Orientation	Orientation		Processing
Software	Bureaucratic	Agile	Indifferent	Formally indifferent, informally bureaucratic
Lifecycle Management				

6. Closing Remarks

This paper has shown how cognitive-linguistic prototypicality shapes the governance and platformisation of CTI infrastructures by anchoring stakeholder expectations in metaphorical roles such as the firefighter, smoke-detector, bystander, and the *Danda*. While our empirical focus was disinformation and the Indian cyber security ecosystem, the broader implication is that digital policy outcomes are not only institutional or economic, but also socio-cognitive. Governance metaphors channel how actors perceive their responsibilities, the urgency of action, and the legitimacy of particular infrastructural solutions. These findings highlight how cognitive prototypes function as informal, stabilising frameworks shaping organisational behaviour and the direction of CTI infrastructural development.

For debates in platform governance and digital policy, this suggests that policy inertia and fragmented coordination cannot be explained solely by regulatory design or power asymmetries. They also arise from the mental models through which stakeholders enact governance. Prototypicality therefore helps account for why cyber security policy often defaults to crisis-driven or enforcement-oriented logics, and why anticipatory, collaborative forms of digital infrastructure development – as may be required to address AI-generated disinformation and online information cascades – are hard to create and sustain. In particular, we have noted here how cognitive-linguistic prototypes, both social as well institutional, fabricate the reality of cyber security management as analogous to the management of a raging urban fire incident, with potentially deep technological and policy implications in long-term. Understanding these cognitive orientations is therefore essential for any effort to reform CTI infrastructures and enable more coordinated and innovative cyber security ecosystems.

Declarations

Disclosure of Interest

We declare that we have no competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Disclosure of Funding

No funding was received.

Author Contribution

S.O. reviewed the manuscript and provided supervision along with S.J. S.Y. conceptualized, conducted the investigation, did writing and editing.

References

1. Agnew, P. G. (1928). Work of the American Engineering Standards Committee. *The ANNALS of the American Academy of Political and Social Science*, 137(1), 13–16.
2. Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security*, 132, 103352. <https://doi.org/10.1016/j.cose.2023.103352>
3. Anderson, R. J. (2001). Why information security is hard—An economic perspective. *Seventeenth Annual Computer Security Applications Conference*, 358–365.
4. Baltuttis, D., Teubner, T., & Adam, M. T. P. (2024). A typology of cybersecurity behavior among knowledge workers. *Computers & Security*, 140, 103741. <https://doi.org/10.1016/j.cose.2024.103741>
5. Bantu, B., Fatima, A., Parelli, K., Manda, P., & Bayya, S. R. (2020). The bureau of indian standards act, 2016-an overview. *International Journal of Drug Regulatory Affairs*, 8(1), 1–4.
6. Benbasat, I., & Taylor, R. N. (1978). The impact of cognitive styles on information system design. *Mis Quarterly*, 43–54.
7. Betz, D. J., & Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialogue*, 44(2), 147–164.
8. Bouwman, X., Griffioen, H., Egbers, J., Doerr, C., Klievink, B., & Van Eeten, M. (2020). A different cup of TI? The added value of commercial threat intelligence. *Proceedings of the 29th USENIX Conference on Security Symposium*, 433–450.
9. Branch, J. (2021). What's in a Name? Metaphors and Cybersecurity. *International Organization*, 75(1), 39–70.
10. CERT-In. (2020). *Annual Report*. Ministry of Electronics and Information Technology (MeitY).
11. Chae, H.-C., Koh, C. E., & Jeon, M. (2020). Can Cognitive Style Predict Adoption of an Emerging Technology?: A Study of Cognitive Style and Its Influence on the Perception of a New Technology. *International Journal of Technology and Human Interaction*, 16(1), 18–35. <https://doi.org/10.4018/IJTHI.2020010102>
12. Charteris-Black, J. (2017). *Fire metaphors: The discourse of awe and authority*. Bloomsbury Academic.
13. Dalamagkas, C., Asimopoulos, D., Radoglou-Grammatikis, P., Maropoulos, N., Lagkas, T., Argyriou, V., Sargsyan, G., & Sarigiannidis, P. (2024). AI4COLLAB: an AI-based threat information sharing platform. *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, 783–788.
14. de Melo e Silva, A., Costa Gondim, J. J., de Oliveira Albuquerque, R., & García Villalba, L. J. (2020). A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence. *Future Internet*, 12(6), 108. <https://doi.org/10.3390/fi12060108>
15. Deibler, D. (2025, April 23). Strengthening Digital Resilience. *DAD-CDM Open Project*. <https://dad-cdm.org/strengthening-digital-resilience/>
16. Deming, W. E. (2018). *Out of the Crisis, reissue*. MIT press.

17. EEAS, E. E. A. S. (2023, May 31). *Trade and Technology Council Fourth Ministerial – Annex on Foreign information manipulation and interference in third countries* | EEAS.
https://www.eeas.europa.eu/eeas/trade-and-technology-council-fourth-ministerial-%E2%80%93-annex-foreign-information-manipulation-and_en
18. Ertan, A., Crossland, G., Heath, C., Denny, D., & Jensen, R. (2020). Cyber security behaviour in organisations. *arXiv Preprint arXiv:2004.11768*.
19. Fairbank, N. A. (2019). The state of Microsoft?: The role of corporations in international norm creation. *Journal of Cyber Policy*, 4(3), 380–403. <https://doi.org/10.1080/23738871.2019.1696852>
20. Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. *Digital Society*, 3(3), 59.
<https://doi.org/10.1007/s44206-024-00146-7>
21. Geeraerts, D. (1989). *Introduction: Prospects and problems of prototype theory*.
22. Ghura, B. S. (2023). *Scaling & Automating Cyber Threat Intelligence (CTI) Operations with Free and Open-source Software (FOSS)*.
23. Hurel, L. M., & Lobato, L. C. (2018). Unpacking cyber norms: Private companies as norm entrepreneurs. *Journal of Cyber Policy*, 3(1), 61–76.
24. International Organization for Standardization. (2015). *ISO 9001:2015 Quality management systems – Requirements*. International Organization for Standardization.
25. Jesus, V., Bains, B., & Chang, V. (2023). Sharing is caring: Hurdles and prospects of open, crowd-sourced cyber threat intelligence. *IEEE Transactions on Engineering Management*, 71, 6854–6873.
26. Jung, W. K., & Kwon, H. Y. (2024). Privacy and data protection regulations for AI using publicly available data: Clearview AI case. *Proceedings of the 17th International Conference on Theory and Practice of Electronic Governance*, 48–55.
27. Kelley, A. (2025, April 18). *NSF begins terminating select grant funding*. NextGov.Com.
<https://www.nextgov.com/policy/2025/04/nsf-begins-terminating-select-grant-funding/404698/>
28. Kotsias, J., Ahmad, A., & Scheepers, R. (2023). Adopting and integrating cyber-threat intelligence in a commercial organisation. *European Journal of Information Systems*, 32(1), 35–51.
<https://doi.org/10.1080/0960085X.2022.2088414>
29. Kundu, O. (2021). Risks in defence procurement: India in the 21st century. *Defence and Peace Economics*, 32(3), 343–361.
30. Lakoff, G. (2007). Cognitive models and prototype theory. *The Cognitive Linguistics Reader*, 130–167.
31. Lakoff, G., & Johnson, M. (2008). *Metaphors we live by*. University of Chicago press.
32. Lankton, S. (2020). What Milton Erickson said about being Ericksonian. *American Journal of Clinical Hypnosis*, 63(1), 4–13. <https://doi.org/10.1080/00029157.2020.1754068>
33. Larsson, S. (2017). *Conceptions in the code: How metaphors explain legal challenges in digital times*. Oxford University Press.

34. Magalhães, R. (2011). *Infrastructure and infrastructuring as a bridge between information systems design and organization design*. CIEO-Research Centre for Spatial and Organizational Dynamics, University of ...
35. Mashiane, T., & Kritzinger, E. (2018). Cybersecurity behaviour: A conceptual taxonomy. *IFIP International Conference on Information Security Theory and Practice*, 147–156.
36. Meena, S. L. (2005). Relationship between state and dharma in Manusmriti. *The Indian Journal of Political Science*, 575–588.
37. MeitY. (2013). *National Cybersecurity Policy*. Government of India.
38. Menges, F., Sperl, C., & Pernul, G. (2019). Unifying Cyber Threat Intelligence. In S. Gritzalis, E. R. Weippl, S. K. Katsikas, G. Anderst-Kotsis, A. M. Tjoa, & I. Khalil (Eds.), *Trust, Privacy and Security in Digital Business* (Vol. 11711, pp. 161–175). Springer International Publishing.
https://doi.org/10.1007/978-3-030-27813-7_11
39. Minto, M. B. (2023, November 16). OASIS Mobilizes Open Source Community to Combat the Spread of Disinformation and Online Harms from Foreign State Actors. *OASIS Open*. <https://www.oasis-open.org/2023/11/16/oasis-defending-against-disinformation-dad-cdm/>
40. Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology*, 12, 561011.
41. Niedenthal, P. M., & Cantor, N. (1984). Making use of social prototypes: From fuzzy concepts to firm decisions. *Fuzzy Sets and Systems*, 14(1), 5–27.
42. OASIS. (2024). *Charter for the OASIS DAD-CDM Open Project*. OASIS Open.
43. Oosthoek, K., & Doerr, C. (2021). Cyber Threat Intelligence: A Product Without a Process? *International Journal of Intelligence and CounterIntelligence*, 34(2), 300–315.
<https://doi.org/10.1080/08850607.2020.1780062>
44. Pipek, V., & Wulf, V. (2009). Infrastructuring: Toward an integrated perspective on the design and use of information technology. *Journal of the Association for Information Systems*, 10(5), 1.
45. Rangarajan, L. & others. (1992). *The arthashastra*. Penguin Books India.
46. Schmitt, M. T., & Branscombe, N. R. (2001). The Good, the Bad, and the Manly: Threats to One's Prototypicality and Evaluations of Fellow In-Group Members. *Journal of Experimental Social Psychology*, 37(6), 510–517. <https://doi.org/10.1006/jesp.2001.1476>
47. Semino, E. (2021). “Not Soldiers but Fire-fighters” – Metaphors and Covid-19. *Health Communication*, 36(1), 50–58. <https://doi.org/10.1080/10410236.2020.1844989>
48. Shiff, T. (2024). Moral Logics of Bureaucratic Indifference. *Annual Review of Law and Social Science*, 20(1), 1–15. <https://doi.org/10.1146/annurev-lawsocsci-041922-032616>
49. Stokel-Walker, C. (2023, March 10). Twitter's \$42,000-per-Month API Prices Out Nearly Everyone. *Wired*. <https://www.wired.com/story/twitter-data-api-prices-out-nearly-everyone/>
50. StratComCoE, N. (2022, November 29). *Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM.'*

<https://stratcomcoe.org/publications/foreign-information-manipulation-and-interference-defence-standards-test-for-rapid-adoption-of-the-common-language-and-framework-disarm-prepared-in-cooperation-with-hybrid-coe/253>

51. Subramanian, C. (1992). *India and the computer: A study of planned development*. Oxford University Press, Inc.
52. Subramanian, K. S. (2021). *Political violence and the police in India*. Sage Publications.
53. Thomas, L. D., Autio, E., & Gann, D. M. (2014). Architectural leverage: Putting platforms in context. *Academy of Management Perspectives*, 28(2), 198–219.
54. TN Tech Desk. (2024, March 3). *AI Models Need To Get Indian Govt Approval Before Deployment*. Times Now. <https://www.timesnownews.com/technology-science/ai-models-need-to-get-indian-govt-approval-before-deployment-article-108176335>
55. Ussath, M., Jaeger, D., Cheng, F., & Meinel, C. (2016). Pushing the Limits of Cyber Threat Intelligence: Extending STIX to Support Complex Patterns. In S. Latifi (Ed.), *Information Technolog: New Generations* (Vol. 448, pp. 213–225). Springer International Publishing. https://doi.org/10.1007/978-3-319-32467-8_20
56. Van Dijck, J., Poell, T., & De Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford university press.
57. Van Knippenberg, D. (2023). Developing the social identity theory of leadership: Leader agency in leader group prototypicality. *Social and Personality Psychology Compass*, 17(4), e12739. <https://doi.org/10.1111/spc3.12739>
58. Voorhees, J. (2023, May 31). Reddit Quotes Extraordinarily High API Pricing to Apollo Developer. *MacStories*. <https://www.macstories.net/linked/reddit-quotes-extraordinarily-high-api-pricing-to-apollo-developer/>
59. Yadav, S., & Oberoi, S. (2025). Situating Power in Cyber Threat Knowledge. *Digital Society*, 4(1), 12. <https://doi.org/10.1007/s44206-025-00169-8>
60. Ziegler, C.-N., & Skubacz, M. (2012). Towards Automated Reputation and Brand Monitoring on the Web. In C.-N. Ziegler, *Mining for Strategic Competitive Intelligence* (Vol. 406, pp. 109–119). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-27714-6_6

Footnotes

1. Structured Threat Information eXpression
2. Organisation for Advancement of Structured Information Standards
3. Security Operations Center