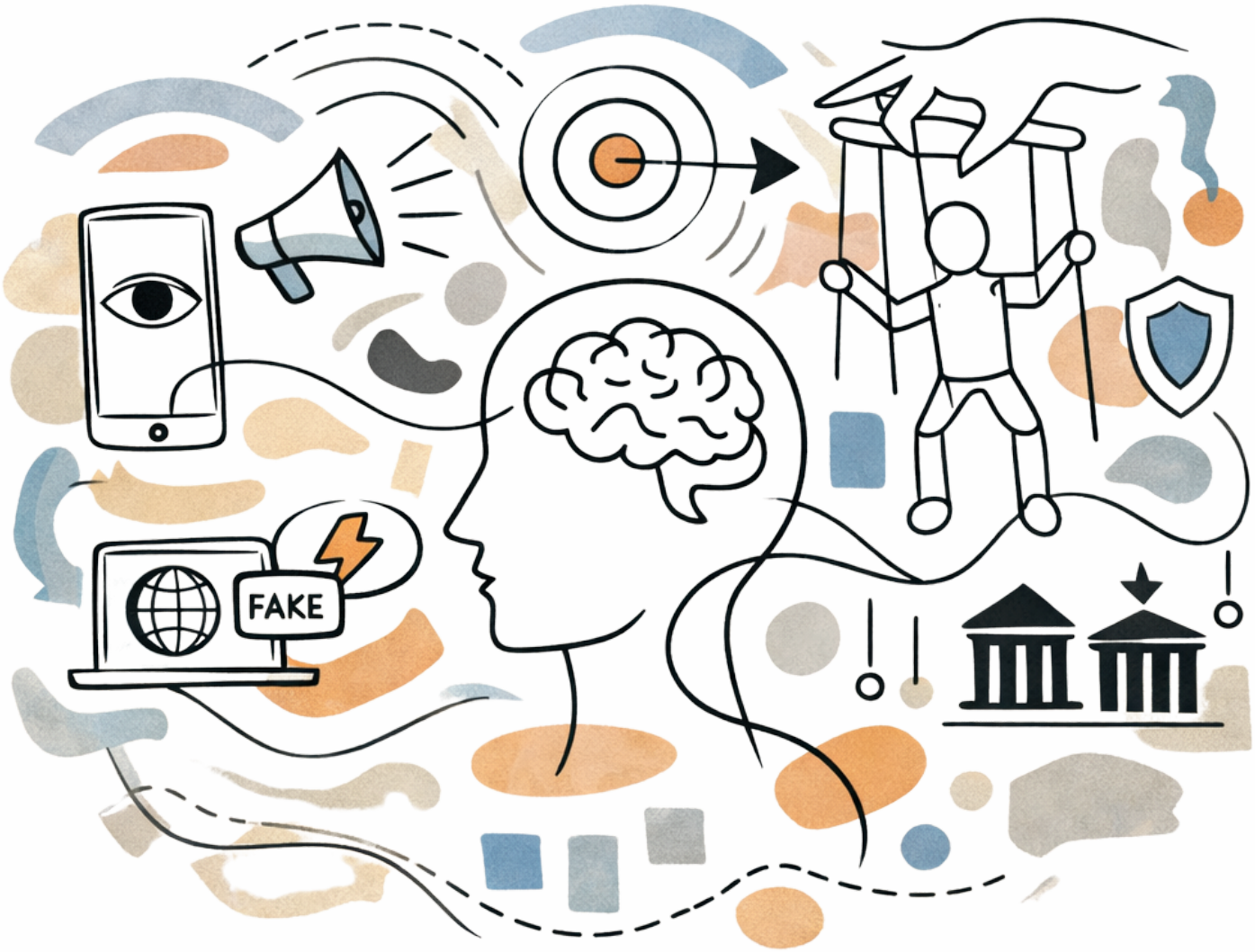


Future Shift Labs

WEAPONISING MINDS

AI, Cyber and Information Warfare in Cognitive Activities

Weaponising Minds

AI, Cyber and Information Warfare in Cognitive Activities

Prepared by

Future Shift Labs

Authors

Mateusz Łabuz & Bhairabi Kashyap Deka

About Future Shift Labs

Future Shift Labs is a strategic research and policy think tank working to build a sustainable, equitable, and digitally resilient future by advancing responsible and ethical applications of artificial intelligence. Established in 2024, the organisation conducts in-depth research and analysis on emerging AI technologies and their societal impact, advocates for inclusive AI governance, and supports strategic consulting, training, and public engagement to strengthen institutional and community capacity. With a focus on fostering collaboration among researchers, policymakers, industry leaders, and civil society, Future Shift Labs seeks to position India as a global leader in digital diplomacy, ethical AI development, and international cooperation on emerging technology challenges

Publication Year: 2026

Future Shift Labs

Opening Message

Nitin Narang
Founder, Future Shift Labs

Conflict in the digital age is no longer confined to borders or battlefields. It increasingly unfolds in the realm of perception; through narratives, algorithms, and the manipulation of trust. The human mind has emerged as a critical strategic domain.

Weaponising Minds: AI, Cyber and Information Warfare in Cognitive Activities reflects **Future Shift Labs'** effort to examine how artificial intelligence, cyber capabilities, and information systems are being integrated into modern cognitive operations. With South Asia as its primary focus, this report highlights how rapid digital adoption, combined with geopolitical and social complexities, has created new vulnerabilities that are often poorly understood and inadequately addressed.

This publication is not an argument for fear, but for preparedness. Democratic societies must recognise cognitive security as a core element of national resilience, addressed alongside technological, legal, and institutional safeguards.

We hope this report contributes to informed policy dialogue and collective action in strengthening societies against manipulation while preserving democratic values.

Opening Message

Mr. Sagar Vishnoi

Director, Future Shift Labs

Modern conflicts are increasingly fought through influence rather than force. They operate below the threshold of open warfare, shaping how people perceive reality, interpret events, and make decisions.

This report examines the convergence of AI, cyber operations, and information warfare in targeting cognition, with a particular focus on South Asia. It demonstrates how blurred boundaries between technology, psychology, and politics enable persistent and scalable influence operations.

By analysing regional case studies and institutional responses, ***Weaponising Minds: AI, Cyber and Information Warfare in Cognitive Activities*** aims to move the discussion from awareness to action. Building cognitive resilience; across institutions, platforms, and society, is no longer optional; it is essential to maintaining stability and democratic integrity.

We hope this report serves as a catalyst for informed debate and decisive action. In an era where minds are increasingly contested terrain, awareness itself becomes a form of Defence.

About The Authors

Mateusz Łabuz

Visiting Fellow, Future Shift Labs

Mateusz Łabuz is a researcher at the Institute for Peace Research and Security Policy at the University of Hamburg (IFSH). He obtained a PhD title at the Chemnitz University of Technology where he concentrated on deep fakes and synthetic media. He was a career diplomat at the Polish Ministry of Foreign Affairs. He lectures on cybersecurity, artificial intelligence and disinformation at the University of the National Education Commission and the Pontifical University of John Paul II in Cracow. He is a non-resident fellow at the Future Shift Labs and the CEE Digital Democracy Watch. His interest comprises the influence of artificial intelligence on cybersecurity and hybrid threats, as well as emerging trends in the disinformation sphere, including social resilience and cognitive warfare.

ORCID: 0000-0002-6065-2188 | **E-mail:** labuz@ifsh.de

About The Authors

Bhairabi Kashyap Deka

Communications Associate, Future Shift Labs

Bhairabi is a researcher and policy practitioner specializing in cybersecurity policy, cognitive warfare, and the role of non-state actors in cyberspace. She has worked with leading think tanks such as the Observer Research Foundation, where her research has focused on cyber threats, grey zone strategies, and emerging frameworks for AI governance. Her work includes engagement in global multi-stakeholder dialogues, with interactions involving UN officials and policymakers on issues at the intersection of security, technology, and regulation. With prior experience in grassroots policy initiatives at Gunvatta Gurukul under the Quality Council of India, she has also contributed to rural governance and quality-driven institutional reform. She holds a Master's degree in International Relations from Pondicherry University and is deeply interested in security studies and emerging technologies. At Future Shift Labs, she works on strategic communications, research, and AI-driven cybersecurity policy.

Contact: bhairabi@futureshiftlabs.com

Future Shift Labs

Content

Introduction

I. Introduction

In an era of rapid technological advancements, the perception of battlefields must be adapted to new conditions[1]. Nowadays, the battles can be waged through the information infrastructure we use, the screens we scroll, the stories and sources we trust, and the emotions we feel. This shift is changing how warfare can be defined and conducted, and how people could experience it.

Human perception, beliefs, emotions, and the ability to make rational decisions are increasingly being targeted by state and non-state actors[2]. Cognitive[3] activities constitute one of the pillars of the so-called grey zone activities[4]. They are undertaken in peacetime, below the threshold of open conflict and aimed at destabilising the opponents' capabilities without resorting to costly conventional military operations. They are blurring the line between peace and conflict and redefining the very nature of modern warfare[5].

The center of gravity is gradually shifting toward cognitive operations enhanced by the use of cyber- and information warfare. This does not mean abandoning traditional kinetic and conventional military means, as demonstrated by the conflicts in Ukraine and the Gaza Strip, but a development of an additional set of offensive tools. The strategic advantage does not necessarily have to be achieved through the physical destruction of the opponents and their capabilities. The modern forms of warfare can exploit the vulnerabilities of the human mind and information ecosystems, combining or even replacing brute force with psychological pressure or cognitive manipulation[6].

The development of digital technologies, including artificial intelligence (AI), has profoundly transformed the nature of such offensive operations[7]. As a society, we have moved a significant part of our communication and daily activities to the digital sphere. We have submitted to the decisions of algorithms that choose for us what we see and interact with on the Internet. The problem is that they can be easily manipulated or even weaponised to create specific narratives or visions of reality.

Algorithms can analyse vast amounts of data in real time, identify vulnerable social groups and individuals, and precisely select narratives to polarise society. Through big data and sentiment analysis, or behavioural profiling, they allow to create messages that resonate strongly with specific audiences by appealing to their fears, beliefs, experiences, emotions, or exploiting their cognitive biases (i.e., patterns of distorted thinking based on simplified rules of reasoning)[8].

As a result, cognitive operations that previously required significant resources can now be conducted on a mass scale and with increasingly greater precision. They can be also indirectly facilitated by various forms of cyberwarfare and control over the communication infrastructure. For that reason, the boundaries between information warfare, influence operations, and cyberattacks consistently blur, bringing out another field of competition: **the battle over minds**[9].

This report, *Weaponising Minds: AI-, Cyber-, and Information Warfare in Cognitive Activities*, seeks to understand how AI-, cyber-capabilities, and information warfare are increasingly interwoven into strategies of cognitive influence, particularly within the dynamic political and digital landscape of South Asia. It offers actionable policy insights aimed at enhancing societal resilience against these threats, while maintaining democratic norms, privacy rights, and freedom of expression.

South Asia offers a compelling case study for this inquiry. It is a region where rapid digital adoption meets geopolitical and national complexity. Numerous unresolved conflicts in the region provide fertile ground for fueling cognitive activities. Some offensive strategies are already being implemented in South Asia, to the detriment of democratic systems and societies. Others will emerge, especially in cases of systemic weaknesses and unpreparedness to resist new forms of threats.

The diversity in digital maturity, political governance, and societal resilience of South Asian countries provides a rich comparative framework for this study. India serves as our primary reference point as the largest country in the region with the largest resources, and being the most important point of reference for the Future Shift Labs.

The interconnection between tools used in various operational domains requires adapting defensive doctrines. The South Asian countries are currently unprepared for these challenges, whereas understanding the multidimensional threats landscape and their long-term consequences requires collaboration between various stakeholders.

Due to the nature and relevance of these threats, as demonstrated by the case studies analysed below, appropriate solutions should be implemented as soon as possible. The example of India, which, despite its increasing technological advancements, still has significant gaps in approaching cognitive threats, can serve as a point of reference for the countries of the region, while also providing an impulse to strengthen comprehensive national and regional resilience.

The key objectives of the report include:

- Drawing attention to cognitive threats emerging in the digital sphere.
- Highlighting how human perceptions and views are targeted and weaponised to exert pressure and influence.
- Examining how information and AI tools are being used to influence public cognition (e.g., deepfakes, algorithmic amplification, algorithmic bias).
- Highlighting the blurred boundaries between cyber-, information-, and cognitive warfare.
- Identifying factors that increase the vulnerability of South Asian countries to threats in the digital domain.
- analysing regionally-rooted case studies where cognitive activities played an important role.
- Mapping the social and psychological impact of cognitive warfare on vulnerable populations.
- Assessing India's preparedness to cope with challenges in the cyber, information and cognitive spheres.
- Proposing frameworks to raise awareness on the cognitive threats in the region
- Presenting specific recommendations to increase social, political and institutional resilience in regard to cognitive threats.

II. The Architecture of Modern Conflicts

1. A path to cognitive warfare

Understanding contemporary cognitive operations requires distinguishing between concepts that remain undefined or unclear. The use of certain terms can still be controversial, especially due to legal implications they might bring. The concept of warfare seems particularly relevant in this regard, as its application can trigger specific obligations and consequences under international law[10]. One may plausibly advocate for a broader interpretation of warfare that considers the impact of specific actions[11]. On the other hand, an overly expansive definitional delineation risks undermining the clarity and protective function of International Humanitarian Law (IHL)[12]. Consequently, the term warfare, when applied to non-conventional operations, carries some ambiguity. Its use may inadvertently legitimise military responses, which creates natural tension between the evolving nature of conflict and the existing legal architecture. However, this should not be an excuse for not creating better protection for civilians and civilian infrastructure.

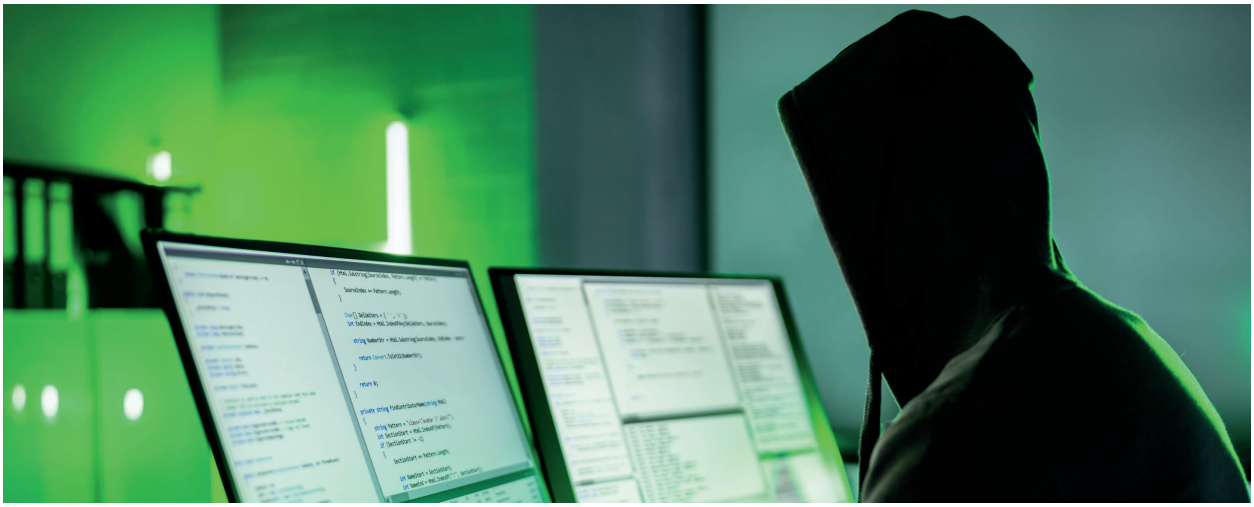
The grey zone activities mentioned earlier exploit these legal imperfections and loopholes, thus making it difficult to qualify specific events, attribute them, hold perpetrators accountable, and adjust the response[13]. Throughout this report we deliberately use the term warfare, seeing it primarily as an emanation of aggressive offensive strategies aimed at gaining a strategic advantage and weakening the adversary, albeit regularly below the threshold of war. Similar nomenclature is used, for example, in reference to cyber warfare or hybrid warfare.

Cyber Warfare

Cyber warfare refers to activities conducted in cyberspace. It includes attacks on digital infrastructure, such as sabotage of IT systems, shutting them down, data theft, ransomware, or disruption of communication systems[14]. In the traditional approach, it is therefore focused primarily on the Information and Communications Technology (ICT) infrastructure.

However, the lack of a universally accepted legal definition and understanding of the term's scope creates uncertainty as to when malicious cyberspace activities can be classified as acts of war under international law. This ambiguity complicates responses and raises justified questions about the applicability of IHL to cyber-activities, which is explicitly postulated by many countries[15].

The threshold that allows for the use of force in response to cyber-attacks remains unclear. The doctrine of NATO countries declares the application of "the full range of capabilities to actively deter, defend against and counter the full spectrum of cyber threats at all times, including by considering collective responses"[16]. However, in practice, countries are cautious about equating cyberattacks with conventional attacks, and they lean on defensive cyber capabilities complemented by offensive cyber capabilities rather than conventional military retaliation.



Information Warfare

Information warfare focuses on information, including its understanding, and interpretation, as a key objective of operations[17]. This influences the selection of means, including manipulating or falsifying information, as well as sabotaging, or controlling the flow of information in order to achieve strategic advantage. It can therefore encompass various forms of information disorders, including propaganda, disinformation, misinformation, censorship, or media manipulation[18]. Although it often employs cyber-tools, physical infrastructure becomes merely an instrument for achieving broader informational and cognitive objectives.

Unlike cyber warfare, which can result in physical consequences in regard to ICT infrastructure, information warfare operates primarily in the cognitive sphere. This Characterisation makes its legal classification even more problematic, as it neither fits within the classic framework of armed conflict nor clearly meets the criteria for the use of force as defined by the United Nations Charter[19]. There is no doubt, however, that malicious operations in the information space can cause significant damage and negatively impact social and systemic stability.

Hybrid Warfare

way are particularly important. Within them, states conduct coordinated actions in many areas - from military, sabotage, cyberattacks, economic pressure, to media disruption - without having to officially declare war[20]. These operations are asymmetrical, remain in a grey zone, and can be collectively referred to as hybrid warfare.

Hybrid campaigns can also use a combination of sabotage of digital infrastructure, disinformation, and psychological operations to gradually undermine the opponent's resilience in the cognitive sphere, or directly force specific actions. Hybridity therefore results from combining different means that can serve to achieve a common goal, which, however, is difficult to capture. This distinguishes traditional from unconventional operations - the adversary's goals remain essentially hidden and can only be analysed in the context of certain deduced meta-goals.

Cognitive warfare

Cognitive warfare can be considered the next stage in the development of influence tools. It indirectly targets ICT infrastructure and information channels, but can also make an impact through physical destruction, i.e., by triggering psychological outcomes. Essentially, it focuses on human consciousness and perception[21]. Cognitive actions target attention, beliefs, and interpretations. Their goal is to change what and how targeted audiences or individuals think. A key tools of this warfare are psychology and impact: currently vastly supported by data, algorithms, and AI, as well as the large-scale use of digital infrastructure.

Cognitive operations are an inherent and increasingly integrated component of hybrid strategies. They complement actions in the physical sphere (e.g., cyber-attacks, sabotage against the critical infrastructure, military operations). They aim for disruption of perceptions, undermining trust in the media and institutions, and ultimately, a change in beliefs of targeted audiences or the decision-makers.

Doctrinal shift

Doctrinal shift

The doctrines of some countries and military alliances increasingly recognise cognitive warfare as a separate and significant dimension of contemporary security. NATO's Allied Command Transformation is developing the Cognitive Warfare Exploratory Concept, which is a part of the Warfare Development Agenda[22]. The strategic assumptions of the concept describe mechanisms for influencing perception, decisions, and behaviour at the societal level. The concept focuses on building cognitive resilience, protecting strategic decisions, and countering information manipulation[23].

Chinese doctrine treats the cognitive domain as a key area of conflict. The People's Liberation Army (PLA) is developing strategies known as the Three Warfares (public opinion, psychological, and legal warfare)[24], which create the foundations of cognitive warfare. The PLA also works on "mind superiority" (制脑权), or cognitive dominance, with the aim of gaining strategic and technological advantage, or "winning the conflict without fighting"[25].

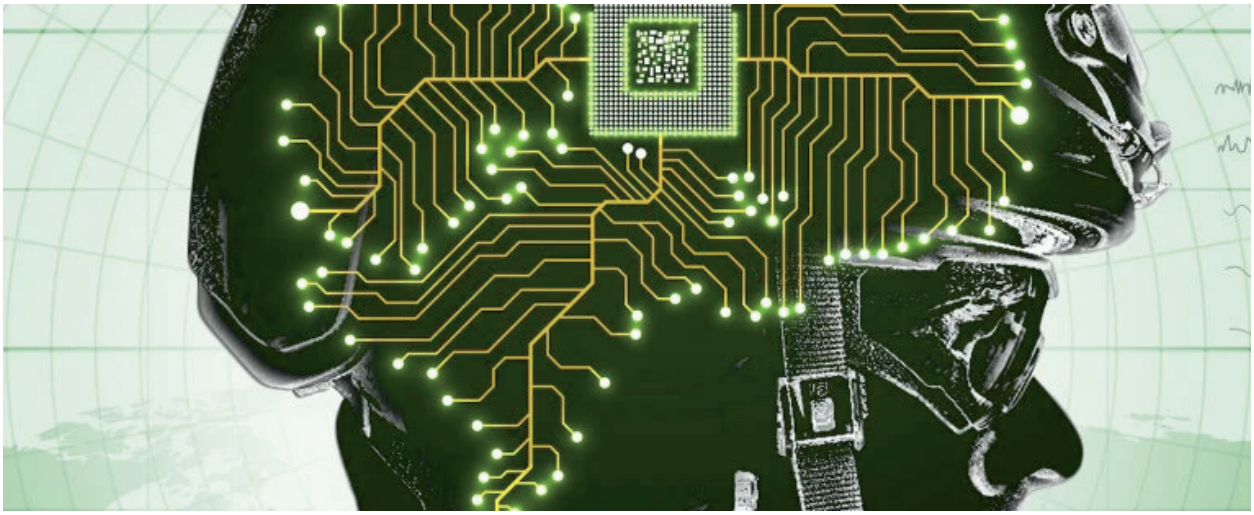


Image Credits : **NATO Innovation Challenge Fall**

In Russia's case, the concept of cognitive warfare has strong historical foundations and is linked, among other things, to Cold War reflexive control, understood as "the process of transferring the basis for decision-making from one opponent to another".[26] Within modern cognitive warfare, Russia combines the use of various communication platforms (media, scientific conferences, diplomatic forums) with various means (information and cyber warfare, sabotage, military exercises)[27]. Importantly, these actions "align with the offensive realist imperative to enhance relative power without direct military engagement"[28].

They also employ various tactics, including: exhaustion, decoy, disintegration, appeasement, intimidation, provocation, overload, suggestion, distraction, and paralysis[29]. Each of these elements weakens the adversaries' cognitive abilities.

India's evolving strategic posture is now acknowledging that future conflicts will not be won by pure kinetic force alone. The Indian armed forces, through their new Joint Doctrine for Multi Domain Operations (MDO)[30], which also refers to shaping perceptions, narratives and the decisions, are beginning to treat the cognitive domain as an integral part of the military activities.

AI in Cognitive Operations

Cognitive operations are not a new phenomenon. Their roots date back to ancient times, when various techniques of propaganda, strategic disinformation, or intimidation were used. The arsenal of solutions has been developed over the centuries, with new technologies gradually being implemented to increase the reach of such operations[31].

ICT infrastructure plays an important role in this respect, creating a field for comprehensive activities. The development of the Internet and social media has enabled activities on a mass scale, with unprecedented precision and speed.

AI-driven algorithms that amplify selected content play an important role in this transformation. The transition from print propaganda, through radio and television, to digital operations has therefore brought about a radical change: today, it is possible to create and target narratives in real time, personalise messages, and automate influence operations based on the behavioural data of millions of users[32]. A key role in these processes is played by the design of an information exchange ecosystem based on social media that aims to amplify content that sparks interest and engagement. Maintaining user attention allows platforms to monetise the users' interest and time spent within the system[33]. For that reason, content that evokes emotions and has high Polarisation potential is prioritised, as it increases the likelihood of interaction. This leads to a feedback loop that drives algorithmic amplification[34].

There is a noticeable opportunistic use of this ecosystem by state and non-state actors, which is also manifested in the weaponisation of AI and its infrastructure. Consequently, AI must also be seen as a tool for exerting influence and means of conducting cognitive activities, and perhaps it is justified to already use the term AI-warfare.

Overlap between all of these spheres

Cyber warfare, information warfare, hybrid operations, and cognitive operations often function as separate analytical categories, but in practice, they increasingly intertwine. Digital technologies, information infrastructure, and psychological tools are used in parallel or complementarily, making the boundaries between these domains increasingly fluid. For example, disinformation operations can simultaneously be part of information warfare, a component of a cyberattack, and an element of a cognitive strategy.

Additionally, since 2022, the European Union has been using the term FIMI (Foreign Information Manipulation and Interference), emphasizing not only the disinformative aspect of information manipulation but also comprehensive influence operations. However, this term is too narrow to encompass all the elements mentioned above. It should be assumed that they constitute interlocking sets of activities whose common element (or the superset) is the pursuit of strategic goals and gaining advantage.

This overlapping nature of such operations creates new challenges for legal classification, institutional response, and building societal resilience - particularly in situations below the threshold of open armed conflict. Therefore, it is necessary to develop integrated analytical models and multi-layered Defence strategies that take into account the complexity of the contemporary security environment. The following summary groups threat areas and operational mechanisms. Specific examples of their applications will be presented in the next section dedicated to case studies from the South Asia region.

Image Credits : **LikeWar (DC Launch) The weaponisation of Social Media**

2. Operational Mechanisms

State and non-state actors employ diverse strategies targeting infrastructure, information and its distribution, and the perception of reality on the opponents' side. They try to undermine citizens' trust in institutions, erode social cohesion, fuel Polarisation, undermine morale, and generate cognitive chaos that makes it difficult to distinguish fact from fiction. The following list is a sample enumeration of operational mechanisms that can be used in cognitive activities. It is not intended to be exhaustive, especially since the number of tactics is constantly growing, and many of them can be freely combined. However, it gives an overview of the means already used in cognitive activities.

weaponisation of social media and behavioural data

Social media platforms are a tool for collecting, aggregating, and analysing user behavioural data, which can lead to shaping their opinions and decisions[35]. This data is used for precise audience profiling and segmentation, enabling crafting tailored messages that resonate with audiences and individuals.

As a result, adversaries can conduct long-term influence campaigns tailored to the individual characteristics and vulnerabilities of target groups by leveraging easily accessible infrastructure. Moreover, the increasing weaponisation of social media platforms gives adversaries easy access to millions of users who spend an increasing amount of time within systems characterised by a high level of interaction and immersion. Just exposure to the source creates particular vulnerability.

Examples: Cambridge Analytica used Facebook data to target specific audiences with political advertisements during the 2016 US presidential election. During the 2024 crisis in Bangladesh, social media algorithms amplified radical content, pushing curious young users toward conspiracy theories and violent ideologies - subsequently this aligned platform engagement goals with the objectives of extremist recruiters.

Strategic Use of Controlled Platforms

Platforms controlled by a state or corporate entity enable management of information flow and content moderation in the operator's interests. This allows for the systematic promotion of specific narratives and restricting access to content that contradicts the intended purpose. This type of mechanism fosters a homogenous information environment, susceptible to long-term opinion shaping.

Examples: TikTok's algorithms favouring specific content. Limiting the sources to right-wing circles only, to provide information for AI algorithms used on the Truth Social [36].

Image Credits : **Joanna Chan**

Algorithmic Amplification

Recommendation algorithms amplify messages by prioritising content that aligns with the desired narrative. Increasing reach and frequency of exposure causes audiences to perceive the message as the dominant version of reality. AI enables the automation and scaling of influence campaigns at unprecedented speed. Language models and data analysis systems enable the creation of personalised content and the prediction of audience responses, enabling continuous and adaptive actions.

Example: The widespread of deepfakes featuring Bollywood celebrities endorsing political parties in India that have been circulated online in 2024 and reached the audiences due to the vast interest of users multiplied by algorithms spotting that interest[37].

Image Credits : **Gerd Leonhard**

Targeting Echo Chambers and Information Bubbles

Information bubbles or echo chambers might be described as "an epistemic environment in which participants encounter beliefs and opinions that coincide with their own"[38] or "seek and interpret information in a way that confirms preconceptions"[39]. Closed information spaces foster the consolidation and radicalisation of views through constant exposure to content that aligns with the recipient's beliefs. Targeting messages to such environments increases Polarisation and further isolates social groups by exploiting so-called "conformation bias".

Example: In 2024, Bangladesh witnessed a massive spread of targeted disinformation with misleading and exaggerated claims about attacks against Hindus in the region[40].

Pre-emptive Influence and Narrative Seeding

Online psychological operations involve deliberately shaping public opinion by introducing narratives before a real event occurs. Preemptive narrative seeding allows for expanding in the information space and preparing audiences for a specific interpretation of the facts[41]. Such actions reduce the adversary's ability to effectively engage in counter-narratives.

Example: In 2018, in Pakistan bloggers were accused of blasphemy and labelled as traitors[42]*. The campaign was well strategised, due to the religious and cultural significance of blasphemy and treason; they were falsely pre-emptively targeted, which shaped a whole conversation against them.*

Disinformation and Misinformation

Disinformation, understood as deliberate spreading of false or manipulated information in order to achieve specific goals, is a fundamental tool of cognitive warfare, aimed at changing audiences' perceptions of reality. Blurring the line between truth and falsehood hinders rational decision-making. This process often combines emotional elements with the apparent credibility of sources.

In contrast to disinformation, misinformation is not a conscious process - it involves repeating false or manipulated information as a result of lack of knowledge or awareness. At the same time, it is an important factor driving the impact of disinformation.

Example: False claims on social media in regard to how India captured Pakistani cities during the clashes in May 2025[43]. Dis- and misinformation was mainly spread through X, provoking further tensions between the two countries.

Image Credits : **United Nation SDG**

Influencer Manipulation & Covert Influence-as-a-Service

The use of influencers, both overt and covert, to disseminate specific narratives that align with the interests of cognitive operators. These activities involve funding, rewarding, bribing, or blackmailing individuals with significant social media reach to seemingly organically promote selected content, thus influencing public opinion and shaping perceptions of events. This mechanism is particularly effective in environments with low information resilience, where the authority and popularity of individuals have a strong influence on audiences.

Example: In May 2025, Indian authorities uncovered a business woman, referred to as "Madam N", who recruited social media influencers from India - they were paid and asked to propagate destabilising content[44].

Image Credits : **Fordham Center for Cybersecurity**.

Bot networks and Coordinated Inauthentic behaviour

Bot networks are used to disseminate content and artificially boost its popularity on mass-scale. The coordinated activities of multiple accounts can create the illusion of spontaneous support by exploiting cognitive biases, such as “social proof”. This increases social pressure and shapes the perception of “majority opinion”.

Trolls are individuals or automated accounts that deliberately provoke, deceive, or disrupt online discussions. They are used to manipulate public perception by spreading disinformation, sowing discord, and amplifying divisive narratives across digital platforms. They exploit emotional triggers to weaken trust, polarise societies, and influence decision-making.

Example: In 2024, Researchers exposed bot networks and coordinated inauthentic behaviour in favour of the Awami League in Bangladesh during the ongoing election campaign in that country[45]

Deepfakes

Deepfakes are advanced AI-generated image and audio technologies that enable the creation of realistic yet false materials. They can undermine the credibility of leaders, institutions, or accounts of events, or even create events that never actually occurred. The use of such content exacerbates information chaos and erodes trust[46].

Example: Deepfakes of Pakistani Prime Minister Shehbaz Sharif were spread during the Indian-Pakistani conflict in May 2025.

Use of Synthetic Personas

Creating and maintaining false digital identities that exist online ad hoc or for extended periods of time in order to gain credibility and trust among targeted audiences. Such synthetic personas can act as journalists, analysts, social activists, influencers, or ordinary users, and their task is to gradually introduce and amplify narratives favourable to the entities conducting cognitive operations. The level of realism of these accounts, supported by advanced AI techniques, makes them difficult to identify and neutralize.

Example: In May 2025, during the Indian-Pakistani conflict AI-generated synthetic personas were commonly used to spread false information[47].

Cognitive Load Manipulation and Information Saturation

Cognitive overload of recipients with large amounts of information reduces their ability to critically analyse content. In conditions of information saturation, manipulative narratives can be more easily transmitted. This mechanism deliberately exploits the limited capacity of attention and working memory[48].

Examples: Publishing contradictory reports during the COVID-19 pandemic on a mass-scale to confuse and fatigue audiences. Publishing numerous false narratives on the Indian-Pakistani conflict in May 2025 that saturated information space of both sides.

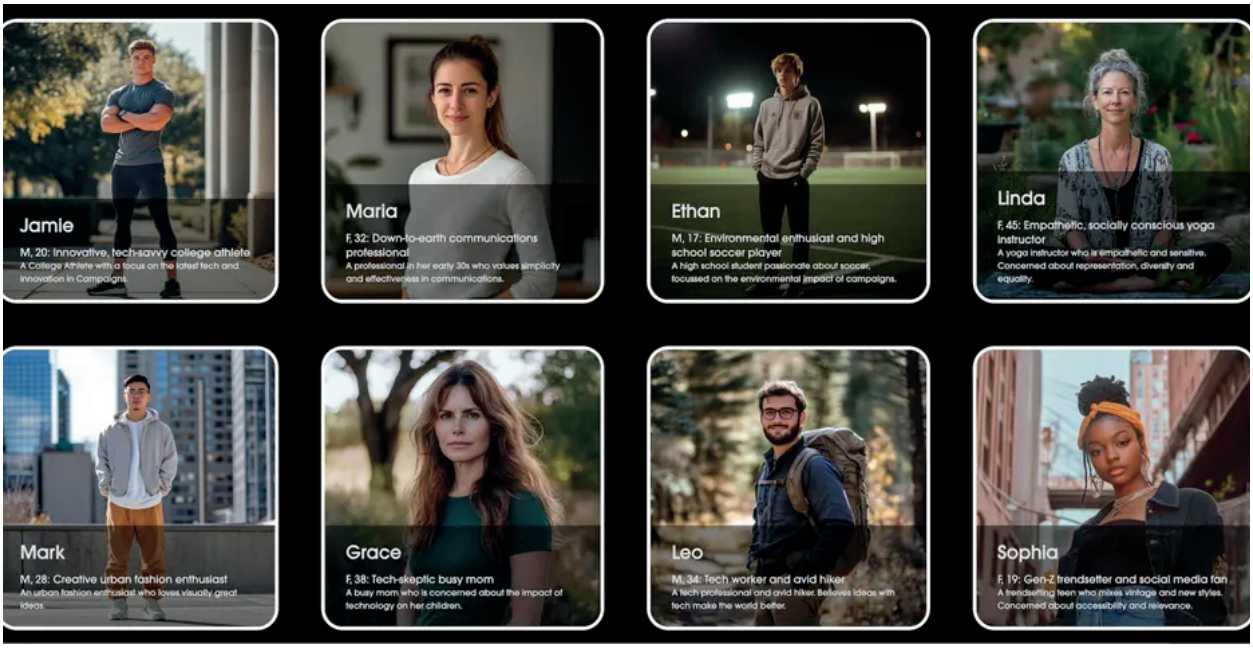


Image Credits : **Synthetic personas developed by Rehabai.ai**

Cognitive Chaos

Deliberate generation of contradictory, variable, and multi-threaded messages leads to informational disorientation. In a state of cognitive chaos, recipients lose their ability to develop a coherent picture of the situation. This results in decision-making paralysis and susceptibility to external interpretive cues.

There is also potential for spamouflage or barrage jamming campaigns by creating hundreds slightly modified versions of the same message and distributing them among the recipients. The analysts of the French Policy Planning Staff and Institute for Strategic Research depicted a fictitious scenario of creating twenty versions of the same speech by altering only parts of the original audio track. Dissemination of all of them simultaneously would "hide the authentic version in the confusion"[49].

Example: The spread of multiple, mutually exclusive versions of events following the shooting down of MH17 in 2014. Saturation of the information space with contradictory information, in particular regarding Russian aggression against Ukraine or Indian-Pakistani conflict in May 2025.

Emotion engineering and affective targeting

analysing audiences' emotional responses allows for tailoring messages to evoke desired emotional states. Using emotions like fear, anger, or enthusiasm amplifies the narrative's impact. This type of influence bypasses rational decision-making processes, directly targeting motivational mechanisms[50].

Example: During the 2024 political unrest in Bangladesh, disinformation campaigns were supposed to raise emotions and trigger communal tensions, as was shown in the case of spreading false narratives about genocide on Hindus[51].

Image Credits : The Guardian

Narrative laundering

The process of introducing false or manipulated narratives into the information space by publishing them on seemingly credible sources, such as niche portals, think tanks, or expert forum members, before they reach the mainstream. This mechanism aims to give disinformation the appearance of authenticity and independent origin, increasing its effectiveness and resistance to debunking. For this purpose, portals impersonating local media and suggesting better understanding of the topic and closeness to the audience may be used. Such media might be referred to as "pink-slime journalism"[53].

Example: False narratives were seeded in the Indian-Pakistani conflict 2025[54], where regional blogs and news sites played a role of original sources. Then the national media amplified these news - a dominant narrative was built out of fabricated stories.

Framing

Interpretive frames determine how the audience perceives a given phenomenon. By choosing context, metaphors, and emphasis, facts can be reinterpreted without distorting them. Framing is a subtle yet effective tool for shaping opinions and emotions.

Example: During the 2022 Sri Lankan economic crisis the government media framed protesters as funded by the foreign agitators while the opposition media framed them as patriots[52]. Russia consistently uses the term "special operation" to describe its aggression against Ukraine.

Memetic Warfare

It uses simple, sharable forms of content to quickly shape narratives in a simplified way. Memes are viral in nature and convey emotional and ideological messages in ways that are difficult to neutralize. Memetic warfare combines humor with propaganda and cognitive associations, increasing message acceptance[55].

Example: ISIS's meme campaigns on social media, designed to attract young recruits worldwide. Following the capture of Indian pilot Abhinandan's comment, slogan "the tea was fantastic" went viral and became a meme; Pakistanis widely used it online to mock India[56].

Slopaganda

It refers to low-quality AI-generated content that can be produced in masses. It is often characterised by poor reasoning, factual inaccuracies, or emotional manipulation that aims to exploit cognitive biases and instill a particular point of view. It uses AI's ability to produce vast amounts of content quickly, thus spreading disinformation or biased narratives with minimal effort and costs.

Example: Bangladesh's elections in 2024 faced media and influencers opting for cheap AI tools to create deepfake-style propaganda[57] .

Grooming of Large Language Models

Large language models (LLMs) are playing an increasingly important role in shaping the information environment. Control over content generation mechanisms and the ability to manipulate them create new threat vectors with significant potential to impact cognitive processes and the formation of attitudes and beliefs.

Grooming should be seen as gaining long-term impact on LLMs by providing manipulated training content, which allows for subtle shaping of their responses. This process can gradually shift the system's ideological or thematic profile, potentially generating content that supports specific strategic goals. This technique is particularly dangerous due to difficulty in detecting it after the training process is complete[58].

Example: Russian Pravda Network systemically publishes large amounts of pro-Kremlin content in open repositories to be included in future training of language models[59].

Semantic Manipulation and Language Engineering

Deliberate changes in the meaning of words, phrases, and linguistic structures influence how audiences perceive concepts and reality. Prolonged use of this mechanism can lead to a redefinition of values, norms, and facts. This constitutes a profound interference in culture and social consciousness.

Example: Russia describes the Ukrainian government and forces as "Nazis". In May 2024, Pakistan named its military response to India's Operation Sindoor as "Operation Bunyanum Marsoos", part of a broader campaign called "Marka-e-Haq" (Battle of Truth).

Cyber-attacks to Trigger Psychological Implications

Cyberattacks can be designed to have a psychological impact, in addition to their technical impact. Defacing government websites, or using distributed denial of service (DDoS) or ransomware attacks against public institutions undermines the sense of security. This reinforces the belief that state or Organisation is weak and cannot ensure the proper protection[60].

Example: Hackers altering the content on the Indian government websites to cause additional fear during the Indian-Pakistani conflict in May 2025.

Cyber-physical Attacks to Trigger Psychological Implications

Integrated attacks on physical infrastructure and digital systems can escalate public anxiety. Disruptions in energy, water, or transportation supplies act as a catalyst for panic. This mechanism undermines the fundamental sense of stability and predictability of the environment.

Example: The cyberattack on Ukraine's power grid in 2015 which caused power outages for hundreds of thousands of residents.

Image Credits : **Supplied/ ABC News: Jarrod Fankhauser**

Cross-Domain Triggering Attacks

Concentrated, coordinated operations combining actions in the physical world with their amplification in the information space. Small incidents - such as limited military clashes, infrastructure sabotage, or staged events - are immediately publicized and amplified in digital media to provoke disproportionate social or political reactions. This mechanism amplifies the psychological impact of small-scale events, destabilising the adversary without the need for extensive military action.

Example: Indian-Pakistani conflict saw an AI-generated disinformation and physical military clashes supplemented with cyberattacks, which in turn led to psychological impact and fuelled the spread of fabricated stories[61].

Case Studies from South Asia

III. Case Studies from South Asia

1. Specificity of the South Asia Region

The South Asia region - including India, Pakistan, Bangladesh, Sri Lanka, Nepal, Bhutan, and the Maldives - can be characterised by strong bilateral and internal tensions, low information resilience, widespread use of digital technologies, and deep social, religious, ethnic, and identity divisions. These factors create favourable conditions for conducting cognitive operations, which increases regional vulnerability.

At this point, however, significant campaigns have been recorded primarily in India and Pakistan, which is linked to the long-standing conflict over Kashmir. In other countries of the region, there is a growing trend of using disinformation, which is vastly amplified by the algorithms of social media platforms.

They facilitate the spread of false or manipulated content and fuel social unrest. However, due to the characteristics of the region, we see significant threats and weaknesses, which will be described below, and need to be comprehensively addressed by the individual countries and through transnational cooperation.

Complex geopolitical and conflict landscape

The region is characterised by long-standing, unresolved territorial and religious conflicts (e.g., India-Pakistan over Kashmir, ethnic tensions in Sri Lanka, separatism in Bangladesh and Nepal), which create fertile ground for various types of threats. Cyberattacks and information operations are often an integral part of hybrid conflicts here - not only as auxiliary activities, but as tools of direct psychological and strategic influence to further fuel existing tensions.

Digital expansion without adequate cognitive safeguards

South Asia is experiencing rapid growth in the number of internet and smartphone users - India is now the world’s second-largest digital market. However, this growth has not been accompanied by the development of digital literacy, data protection, or critical thinking skills. Many countries in the region lack information security policies, and public debate continues to focus mainly on technical aspects, overlooking the impact of narrative manipulation on the democratic systems and national security.

Social vulnerabilities

Religious, caste, ethnic, and class divisions - characteristic of countries such as India, Sri Lanka, and Bangladesh - are often used as vectors for information operations to fuel social Polarisation. Disinformation and emotional manipulation have a particularly strong impact on societies that often lack the tools to verify information and are characterised by numerous vectors of social divisions. Trainings in media literacy, AI and digital ethics, fact-checking activities, and content verification are marginal or absent in education systems. Moreover, South Asia is home to a wide range of stakeholders, from digitally literate urban youth to rural populations with limited digital literacy, making it a region highly susceptible to cognitive threats. Understanding how these communities engage with information ecosystems is vital.

Level of strategic resilience

In recent years, some countries in the region, especially India, have begun to develop instruments to counter information warfare. Initiatives such as the Fact Check Unit at the Ministry of Information and Broadcasting in India[62], cyber Defence doctrines, and cooperation with digital platforms to remove disinformation content have emerged. However, these are preliminary measures and are not yet widespread throughout the region

2. Case studies from the region

Below we present selected case studies covering South Asian countries that illustrate the application of strategies that had significant cognitive impact, or can be directly described as cognitive warfare

Case Study 1: India-Pakistan conflict (2025)

During the escalation of the border conflict between India and Pakistan in May 2025, both sides engaged in an intense information war with a strong cognitive component. Disinformation was used on a mass-scale by both sides and it took various forms, from factually false content distributed in the media (including official broadcasting) to audio-visual content produced by AI.

Footage unrelated to events from May 2025 was repeatedly spread and subsequently misattributed. False claims about the outcome of air strikes were disseminated on social media, reaching millions of users (single post on X on alleged bombing of port in Karachi by India reached at least 2 million users)[63]. Archival recordings of explosions and air crashes were used by both sides, including those in the port of Beirut (disseminated by India as frontline footage), or the attack on Srinagar Airbase (disseminated by Pakistan as the outcome of airstrikes)[64]. Photos and footage from the Gaza Strip were also used. At least some of the footage was aired on national TV by both sides.

Deepfake technology was used to produce a fake speech by Pakistani Prime Minister Shehbaz Sharif, in which he supposedly admitted military defeat. The material was distributed via anonymous accounts on X, Telegram, and WhatsApp, causing confusion[65]. In another AI-generated video Director General of Pakistan's Inter-Services Public Relations (ISPR), Ahmed Sharif Chaudhry, allegedly reported losing some of the fighter jets[66].

Simultaneously, the official account of Pakistani ISPR shared doctored or false clips, presenting them as authentic footage depicting fights in Kashmir region, e.g., the footage from video game Arma III[67]. Various false claims were additionally fueled by authentic and inauthentic social media accounts[68].

Information campaigns were reinforced by cyberattacks aimed at sowing panic and increasing chaos. One key example was a series of defacements of military and local government school websites in India, emblazoned with propaganda messages of psychological intimidation. This was accompanied by claiming the access to military information by Pakistani sources: intended to undermine citizen morale and the credibility of Defence institutions[69]. Both Pakistani and Indian hacking groups engaged in cyber retaliation.

This tactic used by both sides aimed to destabilize public opinion, sow uncertainty, and provoke emotional reactions from citizens. The aim of these operations was not merely to spread falsehoods, but to interfere with the cognitive processes of society through shock, disorientation, and manipulation of perceptions of reality. At a time of particular tension, exerting psychological pressure served, on the one hand, to weaken the enemy and, on the other, to strengthen one's own propaganda activities and reinforce the morale of its own citizens.

Cyberspace activities are a litmus test in this regard. According to analysts, Pakistan, supported by hackers and hacktivists from Turkey, Bangladesh, Malaysia, Indonesia, and China, conducted massive attacks on India's critical sectors. A significant portion of these attacks were strictly military in nature, designed to target infrastructure used for military operations[70].

However, attacks such as DDoS and website defacements had a strong psychological impact. Furthermore, "sources allege that the attackers' primary goals were to cause reputational damage to India on the international stage and to extract classified data, particularly information related to missile development programs"[71].

The aforementioned reputational damage is also an important cognitive factor that can counteract external mobilisation, including support from allies and public opinion outside the involved country.

Image Credits : **MOD, INDIA**

Image Credits : AI Generated Content

Case Study 2: Reinforcement of socio-ethnic divisions in India by Pakistan (2023-2025)

Between 2023 and 2025, Pakistan actively developed a strategy based on fuelling socio-ethnic conflicts in India. The ISPR, operating as the Pakistani military's media arm, intensified polarizing narratives aimed at both Pakistani citizens and audiences in India. Some of the actions were part of the Pakistani "bleeding India with a thousand cuts" strategy, which involves dispersed attacks that cumulatively weaken and destabilize India over time[72].

This design was also witnessed in the April 2025 Pahalgam attack, where militants allegedly affiliated with Pakistan-based groups targeted Hindu tourists[73]. By picking up victims due to their religious beliefs and forcing them to recite religious verses before execution, the attackers deliberately sought to inflame communal sensitivities, deepen Hindu-Muslim mistrust, and trigger Polarisation. The objective was not simply physical terror but also cognitive and social disruption. This calculated exploitation of socio-religious division long formed under Pakistan's strategy for a proxy war illustrates how external actors used targeted violence as a psychological weapon to destabilize India.

These operations constitute an example of Weaponising identity: religious and ethnic identity has been transformed into a tool of strategic destabilization in particularly vulnerable areas.

Case Study 3: Bots in Indian-Pakistani conflicts (ongoing)

The social media platform X has increasingly functioned as a digital extension of the India-Pakistan conflict, as disinformation was heavily shaped and coordinated with inauthentic activity. Research combining sentiment analysis of tweets with Speech Act Analysis (a way to conceptualize speech as an action examining the intent or purpose behind speech[74]), shows that discussions about India-Pakistan relations on X are largely negative. The online platforms activities often mirror the polarised narratives of Pakistani media and are amplified by bots and trolls networks that impact diverse content during times of geopolitical tension.

The studies of coordinated bot activity confirm that both India and Pakistani nationalist or state-aligned groups deeply automated or semi-automated accounts during crises[75].

Image Credits : **FORBES**

For instance, during the 2019 Pulwama-Balakot episode and later clashes thousands of bot-driven tweets flooded Twitter with hashtags such as #Indiastrikesback and #PakistanZindabad. These campaigns recycled old visuals, manipulated algorithms, and manufactured a sense of consensus by making certain narratives appear more popular than they actually were. This strategy leveraged the principles of social proof: when users see a message trending widely, they are more likely to trust and adopt it regardless of its accuracy.[76]

Case Study 4: Disinformation against ethnic minorities in Sri Lanka (2019)

After the 2019 terrorist attacks, Sri Lanka has seen an increase in cognitive operations targeting the minority communities in that country. Some of these activities may have been home-grown. In response to the acts of terror, numerous fake news stories were circulated about further alleged attacks planned by the Muslim community. Manipulated or recycled images or footage were used to document these false claims[77].

The consequences were immediate and tangible: numerous attacks on companies and institutions run by minorities, boycotts, and in some cases, physical violence[78]. Algorithmic amplification escalated the situation to such an extent that authorities were forced to block social media for several days to prevent the spread of false claims[79].

Additionally, in May 2019, following the terrorist attacks and social media blackout, Sri Lanka experienced a series of cyberattacks on at least dozen state and international websites. The defacements of these websites were aimed to further destabilize society: they amplified information chaos, undermined trust in the state, and perpetuated the growing cognitive crisis among the public opinion[80].
It is worth noting that a similar mechanism, fueling a spiral of ethnic violence, was observed in Myanmar in 2017, resulting in the Rohingya genocide. Researchers point to disinformation spread via Facebook and fueled by its algorithms as one of the causes of this wave of hate and violence[81].

Image Credits : **REUTERS**

Case Study 5: Disinformation against ethnic minorities in Bangladesh

Similar phenomena of violence against ethnic or religious groups could be observed in Bangladesh in the last 15 years. Roy et al. call this a social-media-rumor-instigated violent attack and set examples of false accusations against Hindus allegedly insulting prophet Muhammad, which led to riots and direct attacks[82].

Another example from the region of the same disinformation/misinformation pattern: during the COVID-19 pandemic in India, false information was spread to accuse Muslims of deliberately spreading the disease[83].

Case Study 6: China-Bhutan border dispute (2020-2024)

The China-Bhutan border issue has long been overshadowed by India's strategic role in Bhutan's external affairs, as it has also been evolving into a distinct front of cognitive warfare. To go with the large-scale military moves, the contest increasingly unfolded through that of the media narratives, disinformation, and influence-based campaigns that shaped perceptions in Bhutan, India, and beyond.

One of the tweaking episodes occurred when some Indian media, led by NDTV, alleged that China had constructed a village, named "Pangda", two kilometers inside Bhutanese territory. Satellite imagery and official Bhutanese statements later confirmed the village lay well within Chinese borders, and Bhutan's envoy to India publicly denied any Chinese intrusion. Nonetheless, the story circulated widely, reinforcing the perception of Chinese "encroachment" and mixing anxiety in the regional and international arena[84]. Cognitive warfare here worked on two different levels, as India projected narratives of Chinese aggression to sustain its strategic role in Bhutan, while Chinese media highlighted the falsehood of Indian reporting, framing it as deliberate disinformation aimed at driving a wedge between China and Bhutan.

This imbalance in information flow made Bhutan highly vulnerable to narrative manipulation. Chinese outlets exploited this vulnerability by publishing interviews with Bhutanese figures, accusing India of compromising Bhutanese sovereignty by inserting itself into boundary talks with China.

Image Credits : **Al Jazeera**

With the widespread protests against the Citizenship Amendment Act, which was introduced in India in 2019 and was seen as discriminatory against the Muslim communities, social media became a tool for fueling specific narratives. TikTok emerged as a powerful amplifier, as this platform's short video format, algorithmic reach, and popularity among the young and active users allowed the content to circulate far beyond.

TikTok was used to spread the hashtag #IndiaAgainstCAA, which was intended to fuel protests and stoke anti-government sentiments. The hashtag also gained popularity in influential circles, which strengthened its impact[85].

One of the videos presenting two women, one in a burqa and the other in jeans, chanting outside Jamia University's main gate to cheering crowds, became a tool for digital mobilisation[86]. From the cognitive warfare perspective, TikTok performed both as a platform of solidarity and persuasion, colliding with micro-narratives of emotional resonance, but also hosted pro-government voices, making it a contested space.

Strategic Posture of India in the Cognitive Arena

IV. Strategic Posture of India in the Cognitive Arena

The example of India will serve as a case study, the aim of which is to comprehensively assess regulatory and institutional solutions in the area of counteracting cognitive threats.

Cognitive warfare in the official doctrine

The official doctrine of India does not explicitly denote the term “cognitive warfare”. It might be seen as a missing element of the “Cold Start Doctrine”, resulting in a lack of ready-made action plans in the area of psychological and narrative attacks.

In regard to official documents, the emphasis remains on information warfare and psychological operations, which illustrates how these concepts are embedded in strategic thinking. The offensive use of cognitive tools is not acknowledged formally, however, in practice, India envisages shaping the adversary’s perception through psychological operations, particularly in its military posture towards hostile states[87]. Psychological warfare, that has a long history of applications, continues as a significant element in both wartime and peacetime context. India, realising these dependencies, has maintained units that conduct PsyOps as part of its military architecture[88].

At the same time, Computer Emergency Response Team (CERT-In), National Cyber Coordination Centre (NCCC), and National Critical Information Infrastructure Protection Centre (NCIIPC) play defensive roles, strengthening national resilience against disinformation and cyber-enabled cognitive threats. Although the absence of the exact terminology in strategic documents might show that India may not formally label cognitive warfare, its practices reflect both offensive and defensive elements of such activities, and they are consistent with India’s military tradition.

For these reasons, India’s military is increasingly integrating the modern warfare Defence strategy in its doctrine. Indian forces are preparing to fully handle what is called the “fifth generation warfare”, which is understood as the non-contact combat, strategic and psychological dominance. This nexus demands putting into action the conventional power with emerging technologies[89].

Responses to information security threats

India currently lacks a dedicated national strategy or overarching legal framework exclusively addressing disinformation or information disorder. However, there are several overlapping policies and legal documents, as well as institutional countermeasures to address these issues. Section 353 of the Bharatiya Nyaya Sanhita, 2023[90], targets disinformation by penalizing false or misleading content causing public harm, while Section 111 covers organised cybercrime like deepfakes. These laws apply equally to AI-generated content, and are supported by active government enforcement and platform collaboration. However, there is no formal definition or classification of foreign manipulation or cognitive influence operations, which constrains the country's ability to identify and respond to coordinated cognitive or hybrid threats systematically.

NCCC[91], CERT-IN, and the NCIIPC collectively monitor, detect, and mitigate digital threats that target information systems and public perception, too. These agencies also coordinate with ministries and security forces during crises, thereby acting as India's rapid response architecture for information attacks or coordinated disinformation operations.

The Indian Armed forces through their Public Information and Psychological Operations (PsyOps) divisions have explicitly acknowledged the role of perception and narrative management in contemporary warfare. Strategic literature emerging from the Integrated Defence Staff (IDS)[92] and think tanks such as Centre for Land Warfare Studies (CLAWS)[93] and United Service Institution (USI) has repeatedly highlighted the need to strengthen India's cognitive and informational defences against adversarial influence campaigns.

India has begun addressing the malicious use of generative AI under its broader digital and cyber governance ecosystem. However, independent oversight or transparency mechanisms remain limited, which also raises concerns about overreach or inconsistent application of anti-disinformation measures.

On a more proactive note, India has introduced specific programs for safeguarding elections, the Election Commission of India's SVEEP (Systematic Voter, Education and Electoral Participation)[94] initiative and partnerships with digital platforms aim to counter disinformation during electoral cycles. Similarly, media and digital literacy education have been integrated under the National Education Policy (NEP) 2020, or state level programmes such as Kerala's Satyamev Jayate initiative[95].

India’s cybersecurity posture

India has a highly developed digital market, which requires far-reaching cybersecurity measures and constant protection of vulnerable infrastructure. The cybersecurity architecture comprises specialized units in a dispersed structure, which can complicate the coordination of information flow and actions taken in times of crisis. The Computer Emergency Response Team (CERT-IN) within the Ministry of Electronics and Information Technology and National Critical Information Infrastructure Protection Centre (NCIIPC) within the National Technical Research Organisation play a key role in incident management. The Indian Cybercrime Coordination Centre (under the Ministry of Home Affairs) also significantly strengthens Indian capabilities in that sphere, as does the Defence Cyber Agency (under the Ministry of Defence), which serves as the cyber force[96].

India’s cybersecurity framework is guided by a comprehensive National Cyber Security Policy and subsequent institutional and policy developments led by the National Security Council Secretariat (NSCS) and the Ministry of Electronics and Information Technology. The evolving strategy explicitly recognises the growing challenge of information operations and disinformation, as reflected in official statements and strategic coordination under CERT-IN and the NCIIPC.

In addition, India’s cyber doctrine and institutional mechanisms place notable emphasis on human factors and cognitive attack vectors, addressing social engineering or phishing as important social threats[97]. The national cybersecurity framework has undergone updates and reviews within the past years[98], followed by continued alignment with global standards and recent cybersecurity advisories. Together, these developments confirm India’s multidimensional approach that integrates information operations, AI threats and human centric vulnerabilities in its evolving cybersecurity architecture.

One of India’s parliamentary acts, titled the Digital Personal Data Protection Act, 2023[99], establishes a comprehensive framework for handling digital personal data in India. Its core purpose is to safeguard individual privacy by defining strict rules for processing personal data. Within the realm of cyber-doctrines, it understands and reflects a posture of deterrence through denial and legal clarity, as India treats data protection as an integral part of national security[100].

AI-driven threats

Governmental think-tank NITI Aayog's articulated National Strategy for Artificial Intelligence[101] released in June 2018, which has been expanded through India's AI-related policies. They provide a roadmap for the ethical, inclusive, and responsible use of AI. These documents address information security and potential misuse of AI-powered tools for disinformation purposes, stressing responsible use of AI and general rules of transparency and accountability.

While the AI strategy itself does not include explicit laws regulating synthetic media, India relies on an adjacent framework like the IT Act and criminal law provisions, rather than a standalone statute.

Malicious use of deepfakes is already being prosecuted under existing legal provisions[102] that cover impersonation and identity theft. Importantly, the strategy also emphasizes cognitive and social resilience which is reflected in public initiatives for ethics, inclusion, and digital literacy. These programs are embedded within the Digital India Programme, the National Education Policy 2020, and language access projects like **BHASHINI**[103]. **IndiaAI Mission** aims to drive inclusive AI innovation through indigenous models, startup funding, computer infrastructure, and ethical governance. It focuses on talent, tools, and technology to build a robust, responsible AI ecosystem.

India has steadily built a multi-layered institutional framework to address emerging AI-driven threats, integrating efforts across Defence, intelligence, and administrative domains. In parallel, India has begun to adopt LLM-based solutions for translations, governance, automation based on the Indian stack. DigiLocker and UMANG platforms exemplify how India increasingly uses homegrown software for administration purposes.

International posture

India has emerged as an active and responsible stakeholder in global dialogues on AI governance, cyber diplomacy, and information security, reflecting its growing role as a digital power.

The country participates in formats that address ethical and inclusive AI development. It has endorsed the UNESCO Recommendations on Ethics of Artificial Intelligence (2023), and participated, e.g., in the AI Seoul Summit, or Paris Action AI Summit[104]. India is actively engaged, notably as the founding member and co-chair of the Global Partnership on Artificial Intelligence (GPAI)[105], and advocates enhancing cyber-diplomacy.

Image Credits : **Live Mint & Digital India**

V. Recommendations

Policy and Strategy

- It is advisable to develop comprehensive strategies to counter cognitive operations, which should include cross-sectoral cooperation, coordination, and information sharing. Only a coherent state approach will enable an effective response to these complex threats.

- Regulations on the transparency of digital platforms should be strengthened, especially with regard to algorithmic content amplification, targeting non-authentic behaviour, or manipulative synthetic content. The model for such solutions can be found in the EU digital legislation, including the Digital Services Act. This will force technology companies to take greater responsibility for their role in spreading disinformation.

- It is advisable to establish national and regional centres for monitoring cognitive threats. Such institutions can act preventively and support rapid response. It is important to monitor the information environment in order to gain pre-emptive situational awareness.

- Public policies should integrate and ensure the protection of human rights, including freedom of expression and speech, as well as privacy. This will prevent abuses in the implementation of security mechanisms.

Law & Order

- International law on cyber, information, and cognitive warfare needs to be updated. This will allow for better classification and sanctioning of actions below the threshold of war. This also requires coordination at the international level and active advocacy for clearly declaring the applicability of IHL to cyber and information space.

- National legislation should penalise sponsored disinformation campaigns, in particular the question of using and abusing inauthentic behaviour. This will ensure that perpetrators can be prosecuted more quickly.

- The legal framework must protect freedom of expression while allowing for the removal of harmful content. The balance between security and human rights is crucial.

- Regulations on artificial intelligence should include enhancing control over content generated by LLM and introducing specific provisions on deepfakes that would ban specific harmful applications. This will limit the use of AI as a tool for manipulation

Technology

- It is essential to implement modern solutions that enable the analysis of inauthentic behaviour online and the impact of disinformation, e.g. based on sentiment analysis.

- It is crucial to develop tools that enable the detection of synthetic media, including deepfakes, in order to flag and remove them from the internet. These technologies can also be used in other areas, such as the verification of evidence in court proceedings or the detection of child sexual abuse materials.

- Cooperation between the public and private sectors is essential for the effective implementation of technological solutions and the utilisation of the experience of specialised entities

Strategic Communication & Crisis Management

- Countries of the region should develop consistent crisis communication strategies to respond quickly and credibly to false narratives.

- Public institutions must build trust through transparency and regular communication with the public. Trust is the best barrier against manipulation. In this context, it is also crucial to provide transparent information about policies and their implementation, as well as to refrain from using disinformation for political purposes.

- Authorities should use real-time data analysis to monitor the spread of false narratives and predict moments of public vulnerability to disinformation. This will allow them to take preventive action before false narratives become entrenched.
- Partnerships with independent media and fact-checkers should be systematically developed. This will increase the effectiveness of counter-narratives and enhance their credibility.

- Crisis response systems should include a psychological component, including messages that reduce anxiety and prevent mass panic. This will help stabilize public sentiment in crisis situations. Countries might also develop psychological support and emotional resilience programmes, especially for groups most vulnerable to manipulation.

Infrastructure

- National alternatives to key digital platforms should be developed. This will reduce dependence on foreign suppliers and the risk of algorithmic manipulation from outside the region. In this context, it is also recommended to develop a national LLM infrastructure that takes into account cultural and social specificities and can be trained on specific data sets.

- Regular security audits of public institutions' IT systems are necessary. They can detect vulnerabilities before they are exploited by hostile actors.

- Critical infrastructure should also be protected against the psychological effects of cyberattacks (e.g. blackouts). Crisis response plans must include a communication and information component.

Institutions

- Public institutions should establish specialised units for cognitive and information security. This will facilitate a coordinated response to disinformation and cyber threats. The activities of agencies such as Viginum in France or the Psychological Defence Agency in Sweden can serve as useful role models.

- The administration should invest in training employees in recognising and counteracting information manipulation. This will increase the resilience of the entire state apparatus[106].

- It is necessary to increase cooperation between state institutions, local governments, and the private sector. Better exchange of data and experience will allow for a faster response to new types of attacks.

- Control and audit institutions must regularly assess the effectiveness of strategies to counter cognitive threats. Continuous evaluation will ensure that actions remain up to date and effective.

- All elements of the security system should be developed in parallel and in close coordination. The psychological dimension of some cyber attacks does not mean a complete shift in focus from infrastructure protection to protecting public perception. Therefore, standard cyber-measures should be simultaneously developed.

Research and Innovation

- Countries of the region should support funding for research into cognitive resilience and detection technologies. This will enable the creation of local defence tools tailored to the specific characteristics of the region.

- It is necessary to develop interdisciplinary research centres combining psychology, computer science, and social sciences. Only such synergy will allow for a better understanding and neutralisation of cognitive warfare.

- Pilot programmes for innovative solutions should be supported by the public and the private sector. This will increase the pace of implementation of practical tools.

Alliances and Cooperation

- International cooperation in AI and information security research must be deepened. Joint projects will increase resilience and reduce the risk of technological isolation. Countries of the region could establish joint mechanisms for responding to cognitive operations. Only cross-border cooperation can limit the impact of online activities and reduce the potential for cross-national tensions.

- Cooperation with international organisations (e.g. UN, NATO, EU, ASEAN) in the field of knowledge and technology exchange should be strengthened. Such partnerships reinforce collective resilience.

- Regional exercises and simulations of cognitive threats should be conducted regularly. This will allow defence mechanisms to be tested and improved, as well as introducing cas well as introducing confidence-building measures among partners.

Society & Education

- Educational campaigns and media awareness programmes must become a priority. An informed society is less susceptible to manipulation. Therefore, education systems should introduce modules on critical thinking, cybersecurity and disinformation. This will prepare younger generations for life in a digital world saturated with manipulation[107]. Schools should teach responsible use of social media. This will reduce the risk of succumbing to manipulation.

- Non-governmental organisations and citizen media should be supported in fact-checking. Their independence increases credibility and public trust.

- Cooperation between universities and state institutions can support research into cognitive resilience. This will provide practical solutions for policy and society. Scholarship programmes for AI and cybersecurity researchers in the region will increase local expertise. This will reduce dependence on foreign technology.

- Training for opinion leaders (e.g., teachers, journalists, civil servants) in recognising manipulation and coping with psychological pressure should be strengthened. This will enable them to better protect their communities.

- Social ties should be strengthened and trust built between ethnic and religious groups. This will reduce vulnerability to divisive cognitive operations.

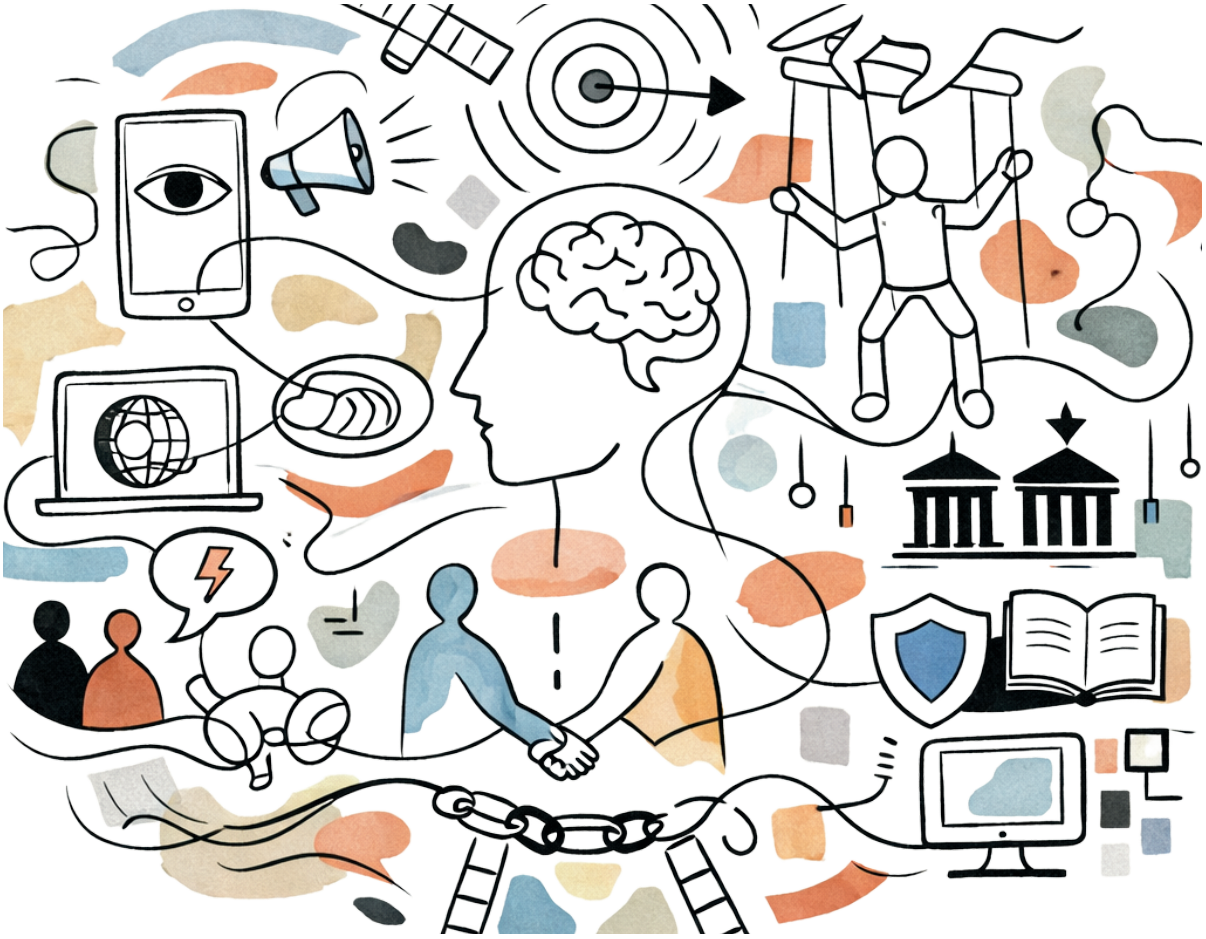


Image Credits : **Abir Mahanta, FSL**

VI. Conclusion

One of the most important conclusions of the report is the need to build social and institutional resilience to such threats. Examples from the region show that the lack of adequate regulation, the still low digital literacy of citizens, and the limited transparency of digital platforms increase the risk of manipulation and thus highlight specific vulnerabilities. For this reason, comprehensive strategies combining law, politics, education, technology, and international cooperation are necessary. Only a multidimensional approach - taking into account psychological, technological, and social aspects - will effectively limit the effects of information and cognitive warfare.

Contemporary conflicts are increasingly shifting to the cognitive sphere, with digital tools, weaponisation of algorithmic amplification, targeting of digital infrastructure, and dissemination of disinformation becoming key means of influencing public opinion. Manipulating people's perceptions, emotions, and beliefs allows state and non-state actors to achieve strategic goals without resorting to traditional military actions. This is also clearly evident in South Asia, where rapid digitalisation is accompanied by deep social, cultural, and political divisions, creating fertile ground for cognitive operations.

The “battle for minds” is becoming a key dimension of security in the 21st century, although we also emphasise that the importance of traditional kinetic means of offensive activities should still not be underestimated. The response to these challenges cannot be solely technical or military defence, but must also include strengthening public trust, supporting independent media, developing critical thinking skills, and ensuring a balance between security and the protection of human rights.

For South Asian countries, this means an urgent need to invest in education, digital infrastructure, and regional cooperation mechanisms. However, these recommendations are universal in nature - in the digital age, the cognitive resilience of societies is becoming one of the most important pillars of global security.

Acknowledgement

Future Shift Labs extends its sincere gratitude to all individuals and institutions who contributed, directly and indirectly, to the development of this report. We are deeply thankful to the researchers, policy practitioners, subject-matter experts, and reviewers whose insights, critiques, and engagement strengthened the analytical depth and rigor of this study.

Future Shift Labs extends its sincere appreciation to Mateusz Łabuz and Bhairabi Kashyap Deka for their rigorous research, analytical depth, and thoughtful authorship of *Weaponising Minds: AI-, Cyber-, and Information Warfare in Cognitive Activities* Their expertise, commitment, and interdisciplinary approach were central to shaping this report and advancing informed discourse on cognitive, cyber, and information warfare

We also acknowledge the broader community of scholars, journalists, technologists, and civil society actors whose work on information integrity, cognitive security, and emerging technologies informed and enriched this research. Their continued efforts to advance ethical discourse and democratic resilience in the digital age remain invaluable.

Finally, we thank our readers and stakeholders for their interest and engagement. It is our hope that this report contributes meaningfully to informed dialogue, responsible policymaking, and collective action in addressing the evolving challenges of AI-driven cognitive and information warfare.

— Future Shift Labs

Reference

[1] Marjanović, A., Smiljanić, D. (2025). *Cognitive warfare - the human mind as the new battlefield*. "Proceedings of the Defence and Security Conference". Vol. 1(1). pp. 84-114.

[2] *Ibidem*; Nikoula, D., McMahon, D. (2024). *Cognitive Warfare: Securing Hearts and Minds*. Information Integrity Lab: Ottawa; Le Guyader, H. (2022). *Cognitive Domain: A Sixth Domain of Operations*. [In:] "Cognitive Warfare: The Future of Cognitive Dominance" (Eds. Claverie, B., Prébot, B., Buchler, N., du Cluzel, F.). pp. 1-5. NATO Collaboration Support Office: Brussels.

[3] Cognitive should be understood as the one referring to thinking or reasoning, or "involving conscious intellectual activity" (Marriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/cognitive).

[4] Cheatham, M. J., Geyer, A. M., Nohle, P. A., Vazquez, J. A. (2024). *Cognitive Warfare: The Fight for grey Matter in the Digital grey Zone*. "Joint Force Quarterly". Vol. 114. pp. 83-91.

[5] Pauwels, E. (2024). *Preparing for Next-Generation Information Warfare with Generative AI*. "CIGI Paper". Vol. 310.

[6] Cheatham, M. J. et al., *op. cit.*; Nikoula, D., McMahon, D. *op. cit.*; Burda, R. (2023). *Cognitive Warfare as Part of Society Never-Ending Battle for Minds*. The Hague Center for Strategic Studies: Hague.

[7] Hunter, L. Y., Albert, C. D., Rutland, J., Topping, K., Hennigan, C. (2024). *Artificial intelligence and information warfare in major power states: how the US, China, and Russia are using artificial intelligence in their information warfare and influence operations*, "Defence & Security Analysis". Vol. 40. pp. 235-269.

[8] *Ibidem.*

[9] Cheatham, M. J. et al., *op. cit.*; Nikoula, D., McMahon, D. *op. cit.*; Burda, R., *op. cit.*

[10] Miller, S. (2023). *Cognitive warfare: an ethical analysis*. "Ethics and Information Technology". Vol. 25(46).

[11] Batool, F. M. (2025). Cyber Warfare: A Grey Zone in International Law. Accessed, https://www.wgi.world/cyber-warfare-a-grey-zone-in-international-law.

Reference

[12] Miller, S., op. cit.;

[13] Defence Committee (2025). Defence in the Grey Zone. Defence Committee of the House of Commons: London.

[14] Sevis, K. N., Seker, E. (2016). Cyber warfare: terms, issues, laws and controversies. “2016 International Conference On Cyber Security And Protection Of Digital Services”. pp. 1-9.

[15] The Federal Government (2021). On the Application of International Law in Cyberspace. Accessed, https://www.auswaertiges-amt.de/resource/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf.

[16] North Atlantic Treaty Organisation (2024). Cyber defence. Accessed, https://www.nato.int/cps/en/natohq/topics_78170.htm.

[17] Theohary, C. A. (2018). Information Warfare: Issues for Congress. Congressional Research Service: Washington; Orzechowski, M. (2024). Disinformation and propaganda in Russia’s information warfare. Concepts, resources, areas of impact. “Atheneum. Polish Political Science Studies”. Vol. 83(3). pp. 7-23.

[18] Ibidem.

[19] Qureshi, W. A. (2020). Information Warfare, International Law, and the Changing Battlefield. “Fordham International Law Journal”. Vol. 43(4). pp. 901-938.

[20] Hoffman, F. G. (2007). Conflict in the 21st Century. The Rise of Hybrid Wars. Potomac Institute for Policy Studies: Arlington.

[21] Miller, S., op. cit.; Marjanović, A., Smiljanić, D., op. cit.; Nikoula, D., McMahon, D., op. cit.; Backes, O., Swab, A. (2019). Cognitive Warfare The Russian Threat to Election Integrity in the Baltic States. Belfer Center for Science and International Affairs: Cambridge.

[22] Allied Command Transformation (2024). Allied Command Transformation develops the Cognitive Warfare Concept to Combat Disinformation and Defend Against “Cognitive Warfare”. Accessed, https://www.act.nato.int/article/cogwar-concept.

Reference

[23] Ibidem; Deppe, C., Schaal, G. S. (2024). Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. “Frontiers in Big Data”. Vol. 7.

[24] Kania, E. B. (2016). The PLA’s Latest Strategic Thinking on the Three Warfares. “China Brief”. Vol. 16(12). pp. 10-14.

[25] Ibidem; Kania, E. B. (2019). Minds at War China’s Pursuit of Military Advantage through Cognitive Science and Biotechnology. “PRISM”. Vol. 8(3). Pp. 82-101; Pappalardo, D. (2022). “Win the War Before the War?”: A French Perspective on Cognitive Warfare. “War on The Rocks”.

[26] Bugayova, N., Stepanenko, K. (2025). A Primer on Russian Cognitive Warfare. Institute for the Study of War: Washington.

[27] Ibidem.

[28] Li, J., Dai, Y., Woldearegay, T., Deb, S. (2025). Cognitive warfare and the logic of power: reinterpreting offensive realism in Russia’s strategic information operations. “Defence Studies”. https://doi.org/10.1080/14702436.2025.2525207

[29] Berzins, J. (2023). The Cognitive Battlefield: Exploring the Western and Russian Views. Center for Security and Strategic Research: Riga.

[30] Press Information Bureau (2025). Mastering existing tech & Staying ready for new innovations & unforeseen challenges is a key to effectively tackle complexities of modern day warfare: Raksha Mantri at RAN SAMWAD. Ministry of Defence. Accessed, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2161131.

[31] Tworek, H. (2021). Disinformation: Its History. Center for International Governance Innovation: Waterloo.

[32] Łabuz, M., Strnad, G. (2025). Political Advertising with the Use of Deep Fakes – Can Deliberative Democracy Really Benefit From This Strategy?. “Politics & Policy”. Vol. 53(3).

[33] Germano, F., Gomez, V., Sobbrio, F. (2025). Ranking for Engagement: How Social Media Algorithms Fuel Misinformation and Polarisation. “BSE Working Papers”. Vol. 1501.

Reference

[34] McLoughlin, K. L., Brady, W. J. (2024). Human-algorithm interactions help explain the spread of misinformation. “Current Opinion in Psychology”. Vol. 56.

[35] McLoughlin, K. L., Brady, W. J., op. cit.

[36] Niedenhoff, S. (2025). Disinformation for beginners: How access to TikTok is threatening European security. European Council on Foreign Relations: Berlin; Weatherbed, J. (2025). Truth Social’s new AI search engine basically just pushes Fox News. Accessed, https://www.theverge.com/news/753863/trump-truth-social-ai-search-perplexity-conservative-bias.

[37] The Times of India (2024). Deepfakes of Bollywood stars spark worries of AI meddling in India election. Accessed, https://timesofindia.indiatimes.com/india/deepfakes-of-bollywood-stars-spark-worries-of-ai-meddling-in-india-election/articleshow/109488973.cms?utm_source.

[38] Ruiz, C. D., Nilsson, T. (2023). Disinformation and Echo Chambers: How Disinformation Circulates on Social Media Through Identity-Driven Controversies. “Journal of Public Policy & Marketing”. Vol. 42(1). pp. 18-35.

[39] Brown, N. (2020). Deepfakes and the weaponisation of Disinformation. “Virginia Journal of Law & Technology”. Vol. 23(1).

[40] Sultana, F. (2024). Bangladesh’s New Democracy Under Threat From Flood of Misinformation. Accessed, https://thediplomat.com/2024/08/bangladeshs-new-democracy-under-threat-from-flood-of-misinformation.

[41] Galindo, J.-P., Nespoli, P., Ruiperez-Valiente, J. A., Camacho, D. (2025). Influence Operation in Social Networks. arXiv. Accessed, https://arxiv.org/html/2502.11827v1.

[42] Raza, T. (2019). Mapping Digital Disinformation around Elections: A Case Study of Pakistan’s 2018 General Elections. Accessed, https://www.cima.ned.org/publication/mapping-online-disinformation-around-pakistans-2018-general-elections.

[43] Ellis Petersen, H. (2025). How Social Media lies Fuelled a rush to war between India and Pakistan. Accessed, https://www.theguardian.com/media/2025/may/28/how-social-media-lies-fuelled-a-rush-to-war-between-india-and-pakistan.

Reference

[44] The Times of India. (2025). Madam N' and influencer spies: How Pakistani Businesswoman built sleeper cell network in India; ISI-backed spy ring under lens. Accessed, https://timesofindia.indiatimes.com/india/madam-n-and-influencer-spies-how-pakistani-businesswoman-built-sleeper-cell-network-in-india-isi-backed-spy-ring-under-lens/articleshow/121651701.cms.

[45] Al-Zaman, M. S. (2024). How Social Media will be weaponised in Bangladesh's Election.The Diplomat. Accessed, https://thediplomat.com/2024/01/how-social-media-will-be-weaponised-in-bangladeshs-election.

[46] Łabuz, M., Nehring, C. (2024). Information apocalypse or overblown fears - what AI mis- and disinformation is all about? Shifting away from technology toward human reactions. "Politics & Policy". Vol. 52(4). pp. 874-891.

[47] Shah, A. A. (2025). AI, Deepfakes, and the Fog of War- Disinformation in the 2025 India-Pakistan Conflict. Accessed, https://www.ifj.org/media-centre/news/detail/category/ai/article/ifjblog-ai-deepfakes-and-the-fog-of-war-disinformation-in-the-2025-india-pakistan-conflict.

[48] Łabuz, M., Nehring, C., op.cit.

[49] Jeangene Vilmer, J.-B. et al. (2018). Information Manipulation. A Challenge for Our Democracies. Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the French Armed Force. Paris.

[50] Marino, E. B., Benitez-Baleato, J. M., Ribeiro, A. S. (2024). The Polarisation Loop: How Emotions Drive Propagation of Disinformation in Online Media - The Case of Conspiracy Theories and Extreme Right Movements in Southern Europe. "Social Sciences". Vol. 13(11).

[51] Muna, A. F. (2024). Misinformation in India about Communal Violence in Bangladesh:Its Implication. Accessed, https://www.researchgate.net/publication/385299833_Misinformation_in_India_about_Communal_Violence_in_Bangladesh_Its_Implications.

[52] Rezwan (2022). Climate change, Digital Authoritarianism and Disinformation Campaigns ruled in South Asia in 2022. Accessed, https://globalvoices.org/2022/12/26/climate-change-digital-authoritarianism-and-disinformation-campaigns-ruled-in-south-asia-in-2022.

Reference

[53] Bengani, P. et al. (2023). “Pink Slime”: Partisan journalism and the future of local news. Tow Center for Digital Journalism: New York.

[54] Kugelman, M. (2025). Why Disinformation surged during the India-Pakistan crisis. Accessed, https://foreignpolicy.com/2025/05/14/india-pakistan-crisis-disinformation-media.

[55] Munk, T. (2025). Digital Defiance. Memetic Warfare and Civic Resistance. “European Journal on Criminal Policy and Research”.

[56] Malik, S. B.(2021). Pakistanis share tea-rrific memes on anniversary of Abhinandan’s ‘fantastic’ cuppa. Accessed, https://www.arabnews.com/node/1816771/pakistan.

[57] Hasan, M. (2023). Deep fakes and Disinformation in Bangladesh. Accessed, https://thediplomat.com/2023/12/deep-fakes-and-disinformation-in-bangladesh/?utm.

[58] American Sunlight Project (2025). A Pro-Russia Content Network Foreshadows the Automated Future of Info Ops. American Sunlight Project: Washington.

[59] Łabuz, M., Schulze, M. (2025). KI-Hintertür in die Demokratie. Accessed, https://background.tagesspiegel.de/it-und-cybersicherheit/briefing/ki-hintertuer-in-die-demokratie.

[60] Schulze, M. (2025). Cyber-Operationen in den Kriegen in der Ukraine und im Gazastreifen: Noch keine Revolution der Kriegsführung. “Zeitschrift für Außen- und Sicherheitspolitik”. Vol. 18. pp. 229-250.

[61] Basit, A. (2025). Disinformation, Conspiracy Theories and Violent Extremism in South Asia. “Counter Terrorist Trends and Analyses”. Vol. 17(2).

[62] Government of India Press Information Bureau (2025). PIB Fact Check Unit. Accessed, https://www.pib.gov.in/aboutfactchecke.aspx.

[63] Institute for Strategic Dialogue (2025). *Missiles and misinformation: false claims about the India-Pakistan clashes reach millions on X*. Accessed, https://www.isdglobal.org/digital_dispatches/missiles-and-misinformation-false-claims-about-the-india-pakistan-clashes-reach-millions-on-x

Reference

[64] The Economic Times (2025). Pakistan shot down Indian fighter jet? PIB factcheck debunks ISI's misinformation campaign. Accessed, https://economictimes.indiatimes.com/news/new-updates/pakistan-indian-rafale-fighter-jet-pib-factcheck-debunks-isis-misinformation-campaign-jf17-thunder-operation-sindoor-india-air-strike-news/articleshow/120951433.cms?from=mdr.

[65] Shah, A. A. (2025). A Accessel, Deepfakes, and the Fog of War - Disinformation in the 2025 India-Pakistan Conflict. Accessed, https://www.ifj.org/media-centre/news/detail/category/ai/article/ifjblog-ai-deepfakes-and-the-fog-of-war-disinformation-in-the-2025-india-pakistan-conflict.

[66] Institute for Strategic Dialogue, op. cit.

[67] Ibidem.

[68] Gupta, M. (2025). The Invisible War: Inside ISPR's Disinformation Campaign Against India. Accessed, https://www.news18.com/world/the-invisible-war-inside-isprs-disinformation-campaign-against-india-exclusive-ws-kl-9344765.html.

[69] NDTV (2025). Pak-Based Cyber Groups Target India Again, Multiple Defence Websites Hacked. Accessed, *https://www.ndtv.com/india-news/pak-based-cyber-groups-target-india-again-multiple-defence-websites-hacked-8335380*; Cyber Security Incident Database (2025). Cyber Incident Victim: Army Public School Srinagar. Accessed, https://www.csidb.net/csidb/incidents/ea0695a4-170f-4ade-b594-bde73f02c505.

[70] CSO Security Insights (2025). Operation Sandur: Pakistan Allegedly Leads Cyber Offensive on India with Support from Six Nations. Accessed, https://csopakistan.com/operation-sandur-pakistan-allegedly-leads-cyber-offensive-on-india-with-support-from-six-nations; Patil, S. (2025). Operation Sindoor and India-Pakistan's Escalated Rivalry in Cyberspace. Royal United Services Institute: London.

[71] CSO Security Insights, op. cit.

[72] Hindustan Times (2025). Pakistan wants to bleed India by thousand cuts, we drew new redlines to combat terror: CDS Gen Chauhan. Accessed, https://www.hindustantimes.com/india-news/pakistan-wants-to-bleed-india-by-thousand-cuts-we-drew-new-redlines-to-combat-terror-cds-gen-chauhan-101748947579384.html.

Reference

[73] Ganguly, M. (2025). Deadly attack on tourists in Jammu and Kashmir. Accessed, https://www.hrw.org/news/2025/04/30/deadly-attack-tourists-jammu-and-kashmir .

[74] Vosoughi, S., Roy, D. (2016). Tweet Acts: A speech act classifier for Twitter (Technical Report). Accessed, https://lsm.media.mit.edu/papers/vosoughi_roy_speechact_icwsm2016.pdf.

[75] Saleem, N., Rasool, F. (2023). Social Media as an Extended Public Sphere: Study of Twitter (X) in the context of India-Pakistan relationship. Accessed, *https://www.fccollege.edu.pk/wp-content/uploads/5.-Dr.-Faraasat-Rasool.pdf*

[76] Krishna, V. (2019). How the Battle of the Bots is influencing your views on the 2019 Elections and National Security. Accessed, https://yourstory.com/2019/04/battle-of-bots-india-elections-national-security

[77] The New Arab (2019). Fake news rampant after Sri Lanka attacks despite social media ban. Accessed, https://www.newarab.com/news/fake-news-rampant-after-sri-lanka-easter-attacks.

[78] France24 (2019). Sri Lanka proposes new law on fake news after Easter attacks. Accessed, https://www.france24.com/en/20190605-sri-lanka-proposes-new-law-fake-news-after-easter-attacks.

[79] Ibidem.

[80] Cyware Social (2019). Websites of at least eleven institutions in Sri Lanka hit by cyber attacks. Accessed, https://social.cyware.com/news/websites-of-at-least-eleven-institutions-in-sri-lanka-hit-by-cyber-attacks-3d19a71f.

[81] Zaleznik, D. (2021). Facebook and Genocide. “Systemic Justice Journal”. Critical Corporate Theory Collection.

[82] Roy, S., Singh, A. K., Kamruzzaman (2023). *Sociological perspectives of social media, rumors, and attacks on minorities: Evidence from Bangladesh*. “Frontiers in Sociology”. Vol. 8.

[83] Rifat, M. R. et al. (2024). *The Politics of Fear and the Experience of Bangladeshi Religious Minority Communities Using Social Media Platforms*. arXiv. Accessed, https://arxiv.org/abs/2410.15207.

Reference

[84] Global Times. (2020). GT investigates: China-Nepal, China-Bhutan border disputes rumors 'stoked by India forces'. Accessed, https://www.globaltimes.cn/content/1207952.shtml?utm.

[85] Scroll (2020). CAA: Case filed against Twitter, WhatsApp, TikTok for letting users share ‘anti-national’ content. Accessed, https://scroll.in/latest/954638/caa-case-filed-against-twitter-whatsapp-tiktok-for-letting-users-share-anti-national-content.

[86] Regan, H. (2019). The women at the center of viral video say India will not be divided. Accessed, https://edition.cnn.com/2019/12/18/asia/india-protests-muslim-woman-viral-video-intl-hnk.

[87] Kariya, S. (2020). Psychological warfare- An opportunity for India. Military affairs. Accessed, https://dras.in/psychological-warfare-an-opportunity-for-india/#_ftnref16.

[88] Bisht, S.S.S. (2025). Review of “Modern psychological warfare:A case study of India”. Accessed, https://maritimeindia.org/review-of-modern-psychological-warfare-a-case-study-of-india/.

[89] The Times of India (2025). ’Boots must share space with bots’: Army chief Gen Dwivedi stresses readiness for 5th-gen conflicts;inaugurates ‘Agnishodh’ to boost defence innovation. Accessed, https://timesofindia.indiatimes.com/india/boots-must-share-space-with-bots-army-chief-gen-dwivedi-stresses-readiness-for-5th-gen-conflicts-inaugurates-agnishodh-to-boost-defence-innovation/articleshow/123101303.cms.

[90] Ministry of Electronics & IT (2025). India well-equippied to tackle evolving online harms and cyber crimes; Governement to Parliament. Accessed, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268.

[91] Ibidem (2025). Taking measures to protect critical infrastructure and private data against cyber attacks. Accessed, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2116341.

[92] Singh, R. (2024). IDS to conduct crash course for senior military officers to boost jointness. Accessed, https://www.hindustantimes.com/india-news/ids-to-conduct-crash-course-for-senior-military-officers-to-boost-jointness-101725798847969.html.

Reference

[93] Yadav, D.S.M. (2021). China's Information Warfare Strategy and its implication for India .Accessed, https://claws.co.in/chinas-information-warfare-strategy-and-its-implications-for-india.

[94] Election Commission of India (2025). SVEEP website. Accessed, https://www.eci.gov.in/sveep-website.

[95] Indian Express (2025). Kerala becomes 'first' digitally-literate state in India. Accessed, https://indianexpress.com/article/india/kerala-first-digitally-literate-state-10203121.

[96] Bharadwaj, T. (2025). Mapping India's Cybersecurity Administration in 2025. Carnegie Endowment for International Peace: Washington.

[97] Data Security Council of India. (2020). National Cyber Security Strategy 2020. Accessed, https://www.dsci.in/files/content/knowledge-centre/2023/National-Cyber-Security-Strategy-2020-DSCI-submission.pdf.

[98] Vajiram & Ravi (2022). Draft National Cyber Security Strategy. Accessed, https://vajiramandravi.com/current-affairs/draft-national-cyber-security-strategy.

[99] Ministry of Electronics and Information Technology (2023). The Digital Personal Data Protection Act, 2023 (NO.22 of 2023). Accessed, https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf?utm.

[100] PRS Legislative Research (2023). The Digital Personal Data Protetcion Bill, 2023: An analysis. Accessed, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023.

[101] NITI Aayog (2018). National Strategy for Artificial Intelligence. Accessed, https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf.

[102] Ministry of Electronics & IT (2025). India well-equippied to tackle evolving online harms and cyber crimes; Governement to Parliament. Accessed, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268.

Reference

[103] Bhashini (2025). Bhashini:National Language Translation Mission. Accessed, https://bhashini.gov.in.

[104] Dhrishti IAS (2023). Paris AI Summit 2025. Accessed, https://www.drishtiias.com/daily-updates/daily-news-analysis/paris-ai-summit-2025.

[105] Tripathi,P. (2023). India's chairmanship of the global partnership on AI. Accessed, https://www.orfonline.org/expert-speak/indias-chairmanship-of-the-global-partnership-on-ai.

[106] For instance, the Artificial Intelligence legislators forum by Future Shift Labs is an initiative to empower Indian lawmakers with the knowledge and foresight and networks needed to navigate the evolving landscape. This forum conducts workshops and roundtables to equip MPs and MLAs with the knowledge to undertake AI's impact on public services.

[107] An Initiative by the National Commission for Women in collaboration with Future Shift Labs titled Yashoda AI, provides beginner friendly, role-based learning to build practical, ethical, and legal AI skills. It empowers women and communities with hands-on, multilingual tools to detect deepfakes, use AI safely and report cybercrime. It aims to democratize AI and nurture women digital leaders through grassroots to national level engagement.