India Foundation Monograph - 01

September 2023

THE WAR ON CONSCIENCE:
INDIA IN THE AGE OF COGNITIVE WARFARE

Divyanshu Jindal

The War on Conscience:
India in the Age of Cognitive Warfare

By

Divyanshu Jindal

India Foundation

2023

Foreword

I write this foreword for the Monograph titled "The War on Conscience: India in the Age of Cognitive Warfare" written by Divyanshu Jindal with immense pleasure. This is an important piece of research work to understand the nature and scope of the cognitive warfare and further to explain how India is facing this new warfare. At the outset, this work explains the key concepts on the issues related to cognitive warfare in order to provide a conceptual clarity to proceed with.

India has been fighting the cognitive warfare unleashed by her two nuclear rivalries valiantly for the past few decades. It is evident that Pakistan's ISPR has actively engaged in Operation Influence using the latest technologies and social media platforms in order to create public outrage and angst against the government and its agencies. Moreover, recent incidents point out that China has also joined in Operation Influence in driving an opinion against India.

This study is really significant for two simple reasons. First, it provides a conceptual clarity on the issues and themes associated with cognitive warfare. Second, it discusses extensively various cases and incidents pertinent to India. This is a pioneering work in the new emerging area of warfare and will be quite useful for students, scholars of strategic studies/security studies/intelligence studies and the practitioners and policy makers and shapers. I would like to appreciate the India Foundation and its team for encouraging and supporting such scholarly research work that would immensely benefit the defense and security policy of India.

Dr. J.Jeganaathan
Associate Professor
Centre for European Studies
School of International Studies
Jawaharlal Nehru University
New Delhi - 110067

List of Figures & Tables

Abbreviations

Abbreviation	Definition
AI	Artificial Intelligence
CCP	Chinese Communist Party
CIA	Central Intelligence Agency
DDoS	Distributed-Denial-of-Service
DIME	Diplomatic, Informational, Military and Economic
DoD	Department of Defence
GPT	Generative Pre-trained Transformer
ICO	Influence Cyber Operation
ISPR	Inter-Services Public Relations
IO	Influence Operations
IT	Information Technology
MBS	Military Brain Science
OIC	Organization of Islamic Cooperation
PLA	People's Liberation Army
PR	Public Relations
PSYOPS	Psychological Operations
RMA	Revolution in Military Affairs
UFWD	United Front Works Department
WHO	World Health Organization

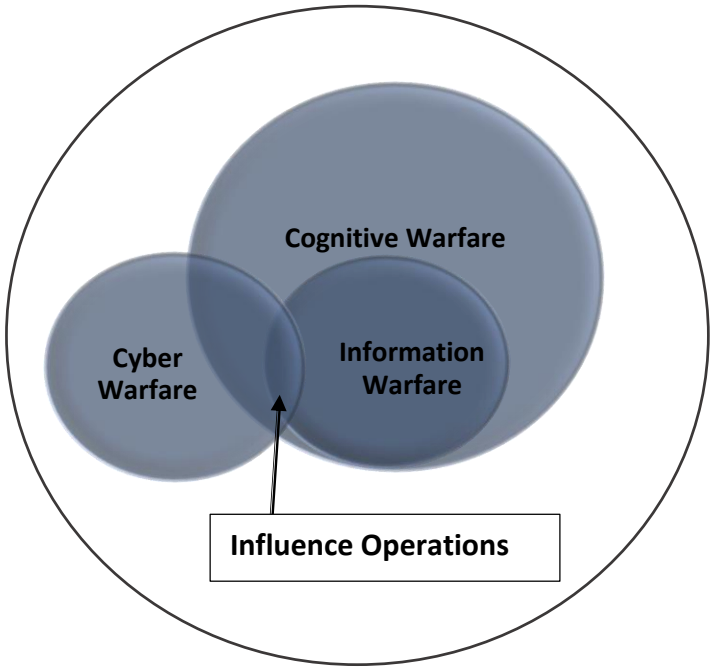
Introduction

Yad bhavam tad bhavati[1] *(You become what you believe)*

One believes what one can read, see, hear or think. And this audio, visual or literary content is crafted by someone – a person, a platform, or an ecosystem. Before the world was taken over by the phenomenon that is social media, influencing someone was restricted to traditional mechanisms like newspapers, radio, cinema, and cultural engagements – often remarked as the tools for propagandism and later rebranded as sources of soft power. However, with the advent of the digital age, the meanings and modes of engagement and exposure have transformed – resulting in long-term effects which, arguably, are not yet completely understood. Going beyond traditional mediums, social media platforms and other digital communication channels gradually became the most effective means to influence people around the world. However, as new technologies like Artificial Intelligence quickly evolve, influence has transformed into a game best played by creating ecosystems from where there can be no easy escape.

The situation underlined is the domain of Influence Operations, a part of the broader information warfare paradigm. A key objective here is to sow confusion, create disorder, and exploit distrust and indecisiveness among adversaries. Influence Operations are the broad spectrum of activities employed to wage information warfare, ranging from operations aiming to shape opinions and perceptions, and those directed toward collecting tactical information about adversaries for competitive advantage over them.

Figure 1: Hybrid Warfare. Own work.



[1] A Sanskrit verse derived from verses in Vedic and Upanishad preachings and the Bhagwad Gita.

While the Influence Operations domain (sometimes also deemed as the 'narrative warfare') (Maan, 2018), continues to evolve in parallel with technological developments, another concept has gained traction in consonance with the above highlighted domains. 'Cognitive warfare' (also called 'brain warfare') (Diggins & Arizmendi, 2012) uses technology to alter human cognition to create a skewed sense of reality. Cognitive warfare aims to overwhelm, destabilise, and exploit cognitive biases and perceptions for strategic benefits against adversaries. When used in conjunction with Influence Operations (at the intersection of information warfare and cyber warfare – Figure 1), cognitive warfare can completely penetrate, alter and weaken societal engagement patterns.

As both information and cyber warfare contribute toward cognitive warfare objectives, it is essential to understand the effects of the parts in isolation to grasp the complete picture. Furthermore, with various terminologies like Influence Operations, information operations, psychological operations and cognitive operations being used today, understanding the minor differences and underlining how each element supports the end goal is important.

This study aims to analyse the developments in the cognitive warfare domain, underlining the cruciality of developing countermeasures for India. Toward this aim, the study utilises reports from social media platforms, studies conducted by think tanks and research labs across the world and inputs from some of the most well-noted experts in the field. While this study is not exhaustive, it provides an overall picture of the emerging strategic threat in the cognitive domain. This would help both scholars and policymakers to understand the evolving paradigm of cognitive warfare, its different aspects, and how these are interconnected. As the study reveals, this threat does not emerge from a single or small group of actors but from multiple, sometimes inter-dependent, mutually benefitting vested interests.

The study is divided into five parts, that delve into the various aspects of cognitive, information, and cyber warfare. These aspects range from conceptual definitions, strategic underpinnings, aims and objectives, impacts, and effectiveness of the activities under the purview of these domains.

The last part of the study aims to underline how the war on India's cognition is unfolding and concludes by analyzing how others are countering the threats explained throughout the study and why India needs to prioritize crafting unique approaches, mechanisms and frameworks based on the Indian strategic thought, to counter the threats in the cognitive realm.

Wherever possible, this study has utilized figures to convey the relationship between various issues in consideration, for the reader's convenience.

Cognitive Warfare

As a relatively new domain, cognitive warfare has been explained through several definitions with minor differences. Some of these definitions include (Claverie & Cluzel, 2021) (Danyk & Briggs, 2023) (Hung & Hung, 2022) -

Figure 2: What is Cognitive Warfare? Own work.

A type of 'psychological-social-technical warfare' combined with a form of 'influence warfare' using cyber means. (Clauverie & Cluzel, 2021)

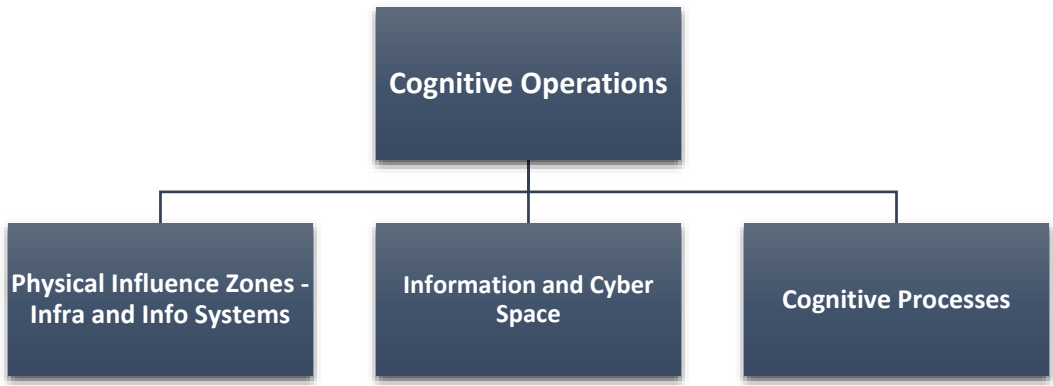
A combination of new cyber techniques for information warfare and the manipulative aspects of psychological operations. (Clauverie & Cluzel, 2021)

A process of directed and controlled influence on system of values, outlook, knowledge, mental space, personal and social consciousness. (Danyk & Briggs, 2023)

A mechanism to control other's mental states and bheaviours by manipulating environmental stimuli. (Hung & Hung, 2022)

While cognitive warfare uses cyber means, it goes beyond the information domain and targets human cognition. Here, an effect (or cognitive effect) is not a by-product of warfare but its very objective (Claverie & Cluzel, 2021). Cognitive warfare is geared toward altering the representation of reality through an alteration of world views for the targeted audience. The figure below shows the various categories where cognitive operations occur (Danyk & Briggs, 2023).

Figure 3: Cognitive Operations Categories. Own work.



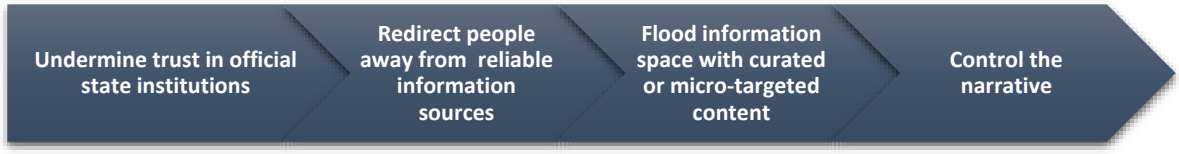
Represented in Figure 3, physical influence zones refer to the infrastructural resources that can be impacted by cyber warfare operations, leading to cognitive effects. This includes cyberattacks on critical infrastructure like medical facilities, energy networks, and nuclear facilities. The second category revolves around the key focus of this study, i.e., the

information and cyber spheres. Finally, the third category refers to thinking patterns, beliefs, interests, values, perceptions, and decision-making.

Comparing cognitive dominance with how state colonization works through the seizure of territory or control over the economy of a state, 'digital colonization' is argued to be possible through cognitive operations using specific socio-cultural and linguistic parameters, attempted with deep knowledge of the mental space of target groups and societies, and their social and mental vulnerabilities (Danyk & Briggs, 2023). Here, digital colonization is seen as the most effective mechanism to influence people and societies using technologies like AI.

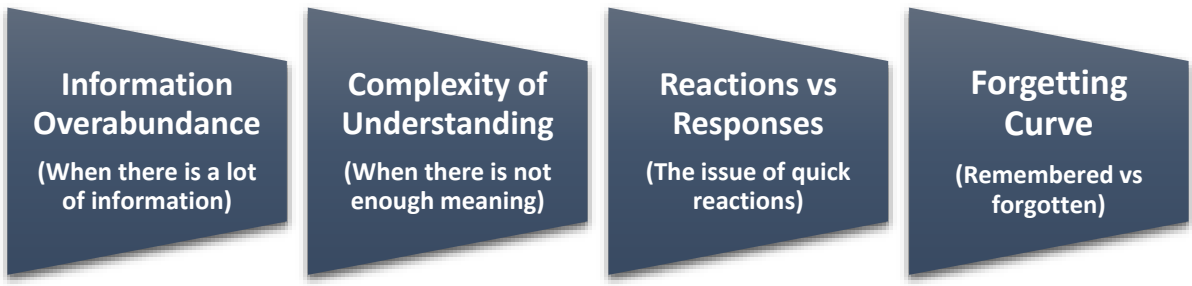
At the strategic level, cognitive warfare is argued to be aimed at dividing and destroying target societies through non-kinetic means in peacetime, whereas, at the operational level, cognitive warfare relies on information warfare (Danyk & Briggs, 2023). However, as shown in Figure 4, moving beyond the manipulation of information space, cognitive warfare coordinates attempts to undermine trust in institutions and critical systems, as well as perceptions regarding reliable sources of information. Furthermore, by flooding the information space to dilute the impact of undesired content, the impact of the micro-targeted content is magnified, resulting in control over the narrative and the responses invoked from the targeted audience.

Figure 4: Aims for Cognitive Operations. Own work.



(Danyk & Briggs, 2023) in their work draw attention to the relationship between the availability of information and cognitive rationalization. Cognitive warfare seeks to cause cognitive distortion to redirect people away from reliable information sources and alter cognitive rationalization. Underlining a study by the US-based RAND Corporation, they argue that information availability affects decision-making in several ways. Some of these are highlighted in Figure 5.

Figure 5: Elements of Cognitive Distortion. Own work.



Information Overabundance

As exemplified in the recent Covid-19 pandemic, information overabundance can lead to chaos. The World Health Organization defines 'infodemic' as too much information (which can be a combination of correct information, misinformation, and disinformation) that occurs during a disease outbreak (WHO, 2023). WHO underlines that it causes confusion and risk-taking that can lead to harmful consequences. The same can be argued for politically and geopolitically sensitive situations or dynamics, where information overabundance can cause risk-taking behaviors among the public or political leadership.

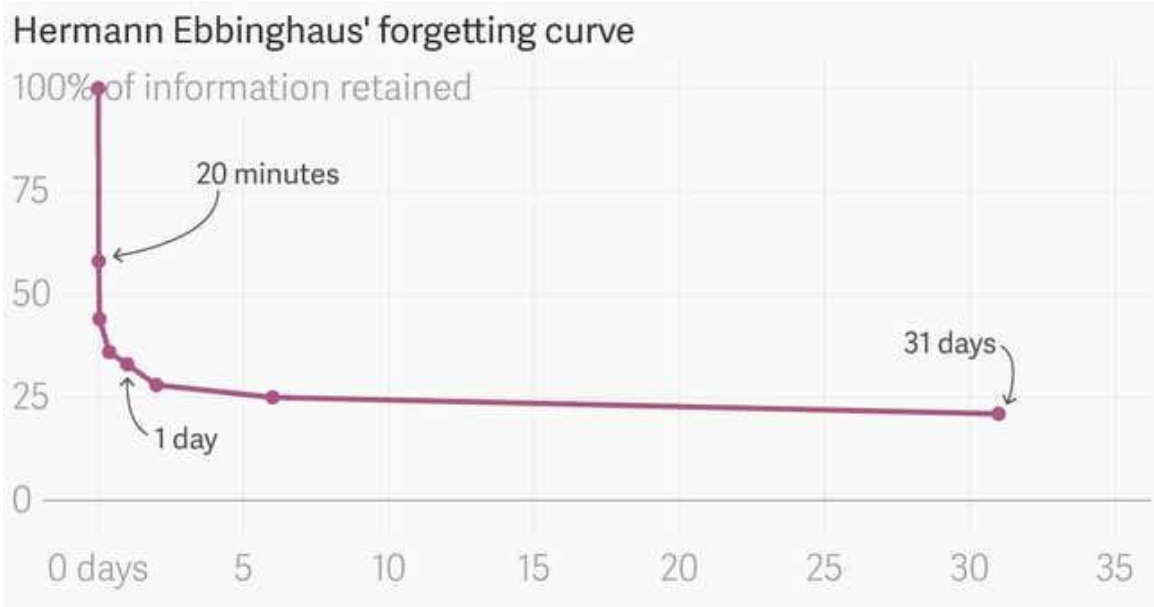
Complexity of Understanding and Reactions vs Responses

In another case, in the absence of adequate meaning in a situation of an overabundance of information, understanding reality becomes an uphill task. Further, knee-jerk reactions to sensationalized media content, clickbait headlines, and luring news titles can invoke subconscious biases (MBC, 2018). Here, 'reactions' are defined as subconscious and emotional decisions made in haste without consideration of consequences. On the other hand, 'responses' involve conscious efforts to review or assess the presented information and situation, and consideration of the options at hand for possible actions, before making a decision to act.

Curve of Forgetting

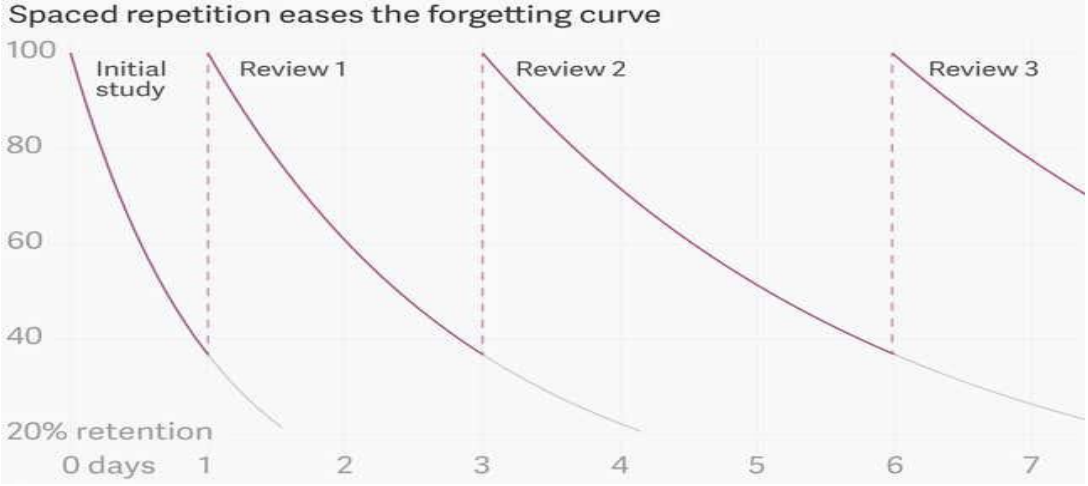
Another element contributing to cognitive distortion is the Ebbinghaus Curve of Forgetting. This memory model highlights how learned information slips out of one's memories over time unless repeated actions are taken to remember it (Sonnad, 2018). The curve involves a mathematical formula describing the rate at which something is forgotten after being learned.

Figure 6: Ebbinghaus's forgetting curve (Sonnad 2018)



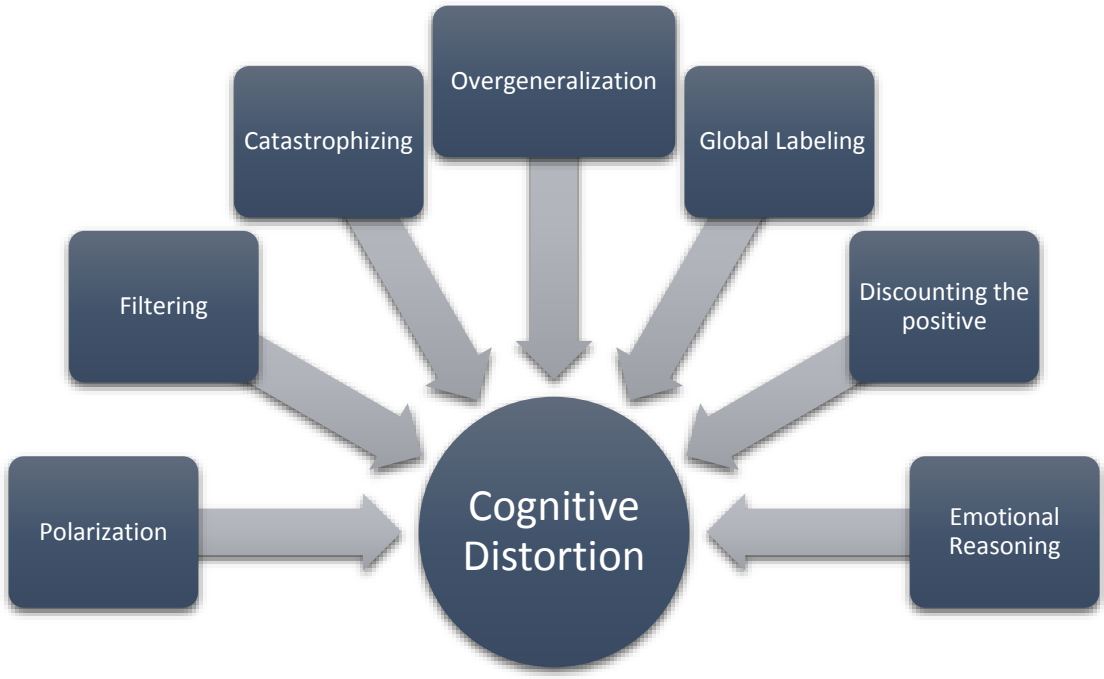
To soften the downward slope shown in Figure 6, a method known as 'spaced repetition' (Figure 7) is recommended, which involves repeating the learned information at particular intervals (Sonnad, 2018). Information warfare utilizes this concept to affect human cognition by infusing cognition and distorting content to affect long-term thinking and decision-making patterns.

Figure 7: Spaced repetition. (Sonnad, 2018)



Almost all the noted effects of cognitive distortion (also referred to as distorted thinking patterns) contribute toward negative thinking (PsychCentral, 2022). While it is argued that anyone can occasionally fall into distorted thinking patterns (Figure 8), frequent engagement with these patterns can have serious adverse health consequences.

Figure 8: Distorted Thinking Patterns. Own work.



In Figure 8, ‘filtering’ refers to the thinking pattern when one exclusively focuses only on the negative aspects of any situation, even if there are more positive than negative aspects. ‘Polarization’ or polarised thinking indicates all-or-nothing thinking, which can lead to unrealistic standards for satisfaction, forcing one to ignore the complexity of the issues in reference. ‘Overgeneralization’ is when one considers an isolated negative event an overall reflection of reality, and ‘catastrophising’ results in reaching the worst-case conclusion in every scenario. Further, taking a single attribute as an absolute reflection of a situation or person is denoted as ‘global labelling’. Finally, holding one’s false beliefs as truth and reacting to a situation under assumptions of those beliefs is called ‘emotional reasoning’. Cognitive warfare aims to create cognitive distortion among the targeted audience (through the elements highlighted in Figure 5) and exploit the distorted thinking patterns (Figure 8) for perpetuity.

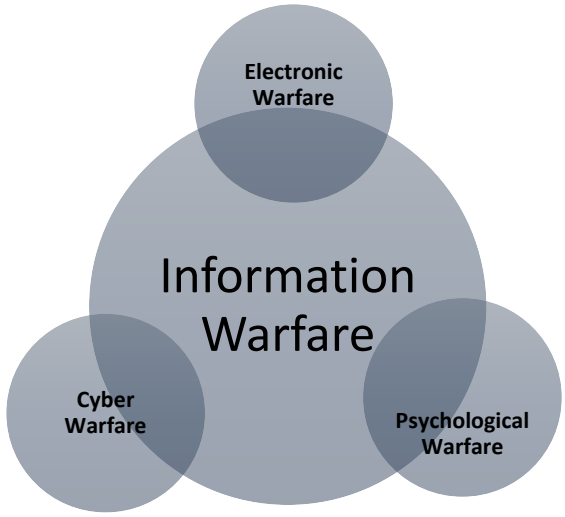
Cognitive operations combine information warfare with cyber warfare. As cyberspace has transformed into a tool for forming individualistic and collective consciousness and social values, information and cyber warfare are the most critical elements to impact society. By disrupting societal understanding and gaining the ability to shape reactions, cognitive warfare can induce significant effects over time, with universal reach. To understand this phenomenon in totality, one needs to analyze both information and cyber warfare, how they are linked to cognitive warfare, and finally, how all these aspects are interlinked.

Information Warfare

The information warfare is a broad concept encompassing several disciplines like information security, information assurance, information superiority, and information dominance.

Though these terms may look similar, the subtle differences produce significantly varied outcomes. For example, while 'information security' relates to preventing sensitive information from getting into the wrong hands (Cisco, n.d.), 'information assurance' refers to the surety of the availability of the correct information to the right person at the right time (NIST CSRC, n.d.). Further, 'information superiority' means a relative advantage concerning possessed information, and 'information dominance' reflects the superiority in using the possessed information (Perry, Signori, & Boon, 2004). When mastered in tandem, these aspects of information warfare provide control over the information domain through generating, terminating and manipulating the reality to shape an information domain aligned toward a desired objective.

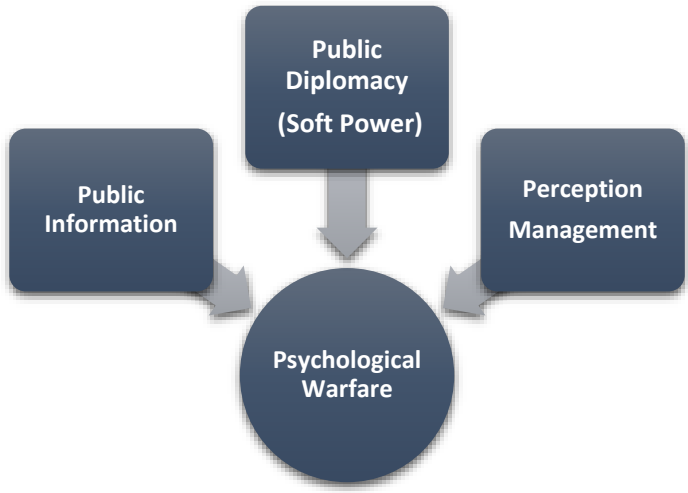
Figure 9: Elements of Information Warfare. Own work.



As shown in Figure 9, information warfare encompasses cyber, electronic, and psychological warfare. While cyber and electronic warfare refers to using cyber and electromagnetic technologies, psychological warfare involves the planned and tactical use of propaganda, diplomacy and perception management (Figure 10). Psychological warfare aims to mislead, intimidate, demoralise, or influence thinking, as well as the adversary's behaviour. Before the advent of the internet, psychological warfare employed tactics like the distribution of pamphlets or flyers to encourage the enemy to surrender or invoke threats of attack by chemical or biological weapons. Overall, the objective remains to gain influence over the adversary. The operations conducted toward this objective are often called PSYOPS or psychological operations. However, as modern psychological operations leverage the cyber and information domains, the operations conducted are also deemed as information operations or Influence Operations. As some approaches to this paradigm consider 'information operations' as a subset of Influence Operations limited to military operations (Brangetto & Veenendaal, 2016), this has resulted in the increasing prevalence of the use of

the term ‘Influence Operations’ to denote the activities undertaken towards psychological warfare through the manipulation of the information sphere.

Figure 10: Elements of Psychological Warfare. Own work



Influence Operations in Strategic Thought

Even before the start of the 21st century, it was widely accepted within the US strategic circles and government departments that the US military capabilities would be decisive only till the US enjoys information dominance over adversaries (Libicki, 1997). Information dominance is meant for both technical and strategic levels. While at the technical level, it means the ability to collect greater, better, and more useful information for battlefield effectiveness, at the strategic level, it means knowing more about one’s adversary – psychologically – to alter their perception and make them see what one wants them to see. The US believes that the competition for information dominance has brought the Revolution in Military Affairs (RMA) and that the side more successful in this realm can overcome the adversary, even without fighting (Libicki, 1997). The goal of information dominance is thus to make the adversary believe that it is in their interests to submit and that the adversary’s demands, arguments, and mission are just.

The US has engaged in Influence Operations for decades. For example, during the Cold War rivalry with the Soviet Union, the US established its state media as a pillar of its foreign policy, placing the state department in control of a peacetime media program abroad (Malzac, 2022). This led to the establishment of broadcasters such as the Voice of America and Radio Free Europe. In the US, Influence Operations fall under the mandate of several authorities and departments, mainly the state department, the Central Intelligence Agency (CIA), and the Department of Defence (DoD). Explicitly, in National Defence Authorization Act 2020, the US Congress clarified the DoDs authority to defend the US, its allies, and its interests, through information operations, including response to malicious influence activities carried out by foreign power, adversarial to the US interests (Malzac, 2022).

Borrowing from the military general Sun Tzu's strategic perspective underlined in *The Art of War*, the Chinese perspective is much broader, considering Influence Operations not as a means for information warfare but as a war in itself. In 2015, the 'Chinese Military Strategy' White Paper underlined that the form of war is accelerating its evolution to 'informationization' – calling for China to build a national defence mobilisation system to win such wars (Jash, 2019). According to Chinese strategic thinkers, information superiority has become the priority mission of modern warfare. For the People's Liberation Army (PLA), securing information dominance encompassing information systems and the cognitive and decision-making aspects of military and political command is essential to the overall approach to warfare. It should also be underlined that while China might be in the nascent stages of attaining information warfare capabilities, it is argued that it is ahead of everyone else except the US (Jinghua, 2019).

Countries around the world look at Influence Operations through different lenses. While the US military is argued to consider information warfare as a part of the conflict—thus the term 'information warfare'—the Chinese deem it not limited to the times of conflict, considering it as an ever-ongoing phenomenon. Thus, preferring the term 'information war', where control over people's thinking and perception is the war itself. A similar view exists in Russian strategic thought, equating information warfare as a strategic threat akin to the nuclear threat (Khan, 2012).

When drawing comparisons with the nuclear paradigm, an instant question comes to mind regarding the efficacy or possibility of destroying hundreds of thousands of lives solely through influence operation; however, what one has to keep in mind is that at the end of the decision-making chain, is someone who can be influenced into thinking and believing something that might not be an entirely accurate picture of the existing reality, thus invoking an action which might lead to disastrous results. Therefore, the invocation of actions which would lead to unintentional, unwanted, or irrevocable results is in itself the supreme objective of Influence Operations.

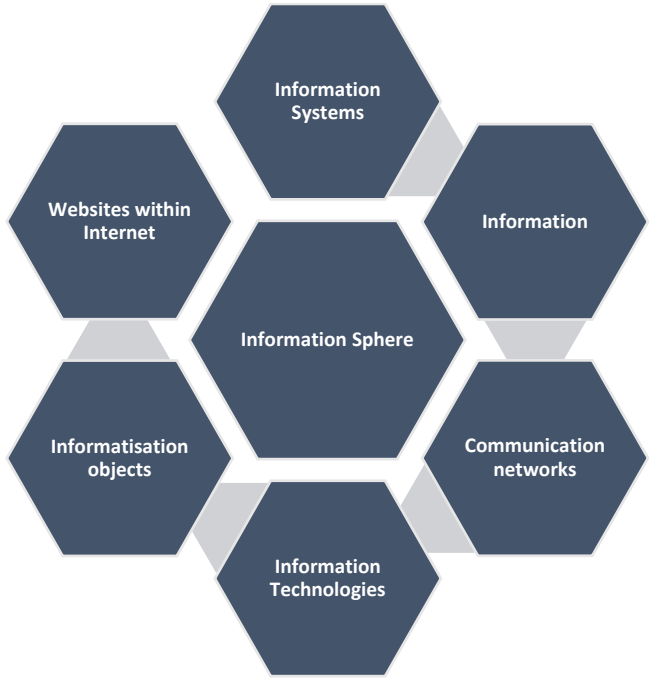
Till recently, Influence Operations remained a 'critically understudied area', with academic research not focused on policy development (Keller, et al., 2020). However, with the world witnessing events like election interferences and regime changes, online terrorist and radical outfit recruitments, and hate speech-induced violence, it has become crucial to understand how internal and external actors can and are already affecting the peace and stability of a nation.

Information Security in the Doctrinal Approach

Despite the absence of critical research, defence against information warfare tactics has been a key concern for several governments around the world. While Western countries have focused more on the universal availability of infrastructural services and the application of principles that keep the free flow of data as the hallmark of cyberspace, others like Russia and China have prioritized focusing on the aspects of the 'content' flowing through cyberspace. In this sense, while the former approach is often termed the cybersecurity approach, the latter is deemed the 'information security' approach.

In December 2016, the Russian Federation approved the 'Doctrine of Information Security of the Russian Federation', laying down a doctrine constituting a system of official views on ensuring security in the information sphere. The doctrine underlines the elements of the information sphere being (Figure 11)

Figure 11: Information Sphere in the Russian Doctrine of Information Security. Own work.



Beyond the above-shown elements, the doctrine defined the information sphere as entities involved in generating and processing information, the development and usage of these technologies, and the mechanisms regulating public relations in the information sphere. It refers to 'information threat' as a combination of actions and factors creating a risk of damaging the national interests and 'information security' as "the state of protection of the individual, society, and the state against internal and external information threats, allowing to ensure the constitutional human and civil rights and freedoms, the decent quality and standard of living for citizens, the sovereignty, the territorial integrity and sustainable socio-economic development, as well as defence and security of the state."

Underlining that information technologies have become global and transboundary and that effective use of these technologies will promote the national economic growth and development of information societies, the doctrine seeks to craft mutually supportive measures in legal, organisational, investigative, intelligence, counter-intelligence, technological, scientific, information and analytical, and economic domains, to respond to the evolving information threats.

Taking the view that information technologies can be weaponized to compromise strategic stability, the doctrine asks for developing the information technology sphere to strengthen equal partnerships in the information domain.

Figure 12: Spheres of Information Security. Own work.

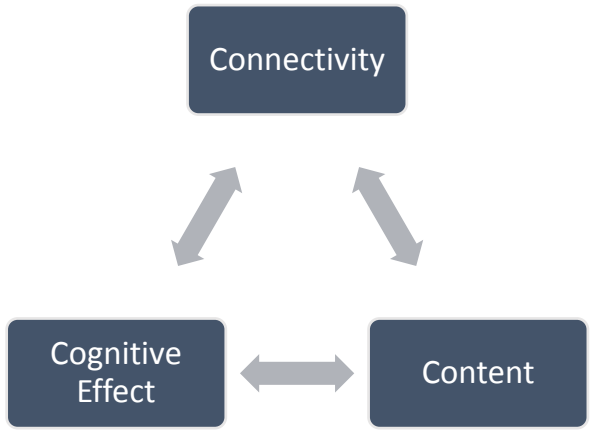
The doctrine highlights that information security encompasses the above mentioned spheres (Figure 12), thus needing a comprehensive framework. The financial sphere includes computer crimes, the national defence sphere indicates the growing use of information technologies for military and political purposes, the social security sphere refers to the risk of information technologies used to infringe on the social stability of the nation, and the science, technology and education sphere involves the need for greater efficiency in scientific research designed to create advanced indigenous technologies and products.

It has now been accepted that information aggression can be used together with political and economic pressure. The information operations to project and protect information include traditional and social media, diplomacy, psychological warfare, cyber warfare, and electronic warfare.

Though Russia adopted the information security doctrine in 2016, calls for a similar approach have been raised in the US as well as in Europe for long. As back as 2006, it was underlined that in the information age, an information strategy becomes a mandatory component in all conflict domains, influencing many of the traditional global strategy areas. In 2015, retired US military personnel made the 'Case for a National Information Strategy', highlighting that while the US has developed multiple national strategies, including one for information sharing, it still lacked a strategy for information content (Murphy & Kuehl, 2015).

Referring to the 'DIME framework', which identifies Diplomatic, Informational, Military and Economic powers as the instruments of national power, the authors underlined the ability to use the information environment as a projection of the information power possessed by a nation (Murphy & Kuehl, 2015).

Figure 13: The 3C Model of Information Power.

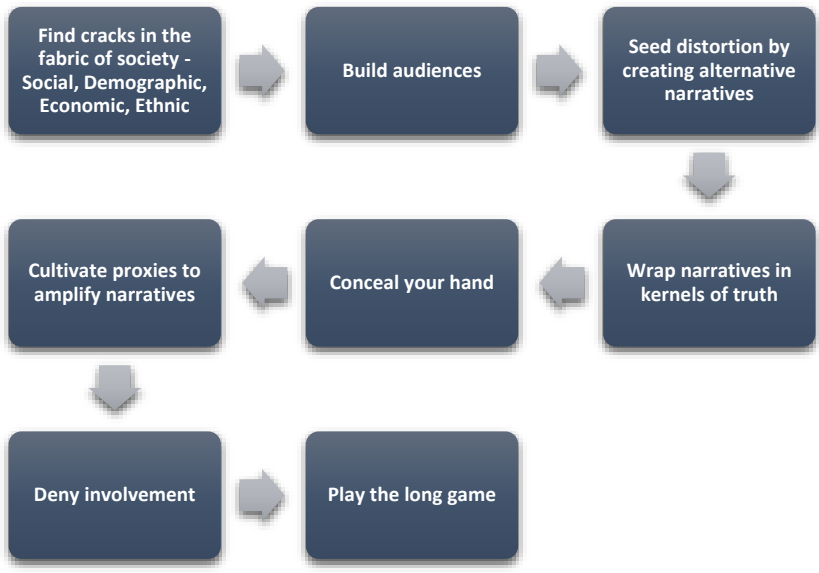


Based on the US military information operations doctrine, the 3C model (Figure 13) refers to the integration of the three dimensions of connectivity (the ability to exchange information), content (the actual information), and cognitive effect (the impact of human beliefs and behaviours) (Murphy & Kuehl, 2015). Thus, the cognitive effect results from using connectivity to deliver content, where the connectivity medium may be technological or non-technological (e.g., human-to-human). However, the result always involves the creation of a belief, after internalisation of the information conveyed, concluding into a specific pattern of behaviour.

Assessing Influence Operations

According to Bruce Schneier, lecturer at the Harvard Kennedy School, Influence Operations can be seen as an 8-step process (Schneier, 2019) –

Figure 14: Influence Operations as an 8-step process (Schneier, 2019)



Schneier highlights that once the attacker determines the cracks in the societal fabric, audience building through platform creation (apps, news channels, newspapers, magazines, etc.) can allow groups of like-minded or vulnerable people to receive the intended messages quicker. The attacker can then seed distortion by creating alternative narratives through mechanisms like fake or manipulated news stories, fabricated videos or other incitory content. This content is wrapped around a core of facts to increase believability, and the real source of information is cloaked. In the last stages, the content is amplified through the receptive audience (and fake users like bots). While it may seem that such content receives little or no attention, such Influence Operations campaigns are generally meant for the long-term impact and run in parallel with several other operations.

Influence Operations in Practice

While Influence Operations are in no way a new concept, these operations have transformed in their importance due to the change in the medium through which they are propagated. Moving beyond the much slower traditional means, influence operations utilise digital platforms and emerging technologies for rapid deployment. Moreover, as social media platforms have become an important part of societal interactions in the past two decades, State and Non-state actors have directed their attention toward carving their own space and building audiences on these grounds.

It has often been highlighted that social media platforms are not inherently neutral (Hallinan, Scharlach, & Shifman, 2021). Further, the privilege of anonymity on these platforms gives way to opaqueness regarding the source of information. Thus, either falsely projecting authenticity or diminishing authenticity due to deliberate attempts to discredit the information source. This has resulted in the disinformation plague.

The widening of internet access for public use since the last decade of the 20th century (2.62 million in 1990 to 414 million users by 2000, and to 4.7 billion by 2020) (Ritchie, Edouard, Roser, & Ortiz-Ospina, 2023) and then the quick proliferation of personal digital devices, especially smartphones, since the first decade of the 21st century has meant that Influence Operations have witnessed back-to-back revolutions in terms of speed and penetration of the content to the targeted audience. However, a similar revolution is now upon us, with emerging technologies like Artificial Intelligence and its applications like ChatGPT, which quickly became popular worldwide (Livingstone, 2023). A report by the US-based Centre for Security and Emerging Technology concluded that the use of AI-powered influence operation campaigns is likely inevitable, highlighting a possibility of normalization of AI-generated disinformation, which would create a downward spiral, leading to more cynical audience providing fertile ground for even greater false information (Sedova, McNeill, Johnson, Joshi, & Wulkan, 2021).

According to estimates, the proliferation of deepfakes witnessed a 900 per cent year-over-year increase between 2019 and 2021 (Letzing, 2021). Defined as hyper-realistic digital copies created through deep learning technology, which uses computer algorithms and data (face, voice, writing style etc.), studies show that deepfakes can significantly and quickly impact the audience even if they have prior knowledge about the deepfake concept.

Moreover, when coupled with the distorted thinking patterns highlighted earlier in this study, the impact of deepfakes can be disastrous.

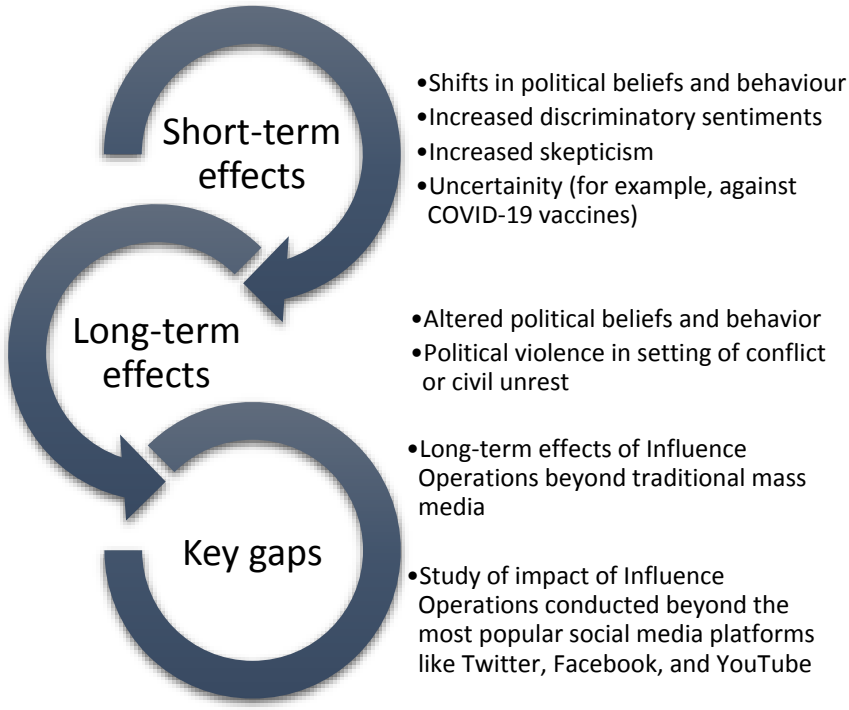
It has been argued that Deepfakes can implant false memories, resulting in people memorising and later recalling audio-visual memories that never actually occurred (Morrow, 2021). Moreover, as the forgetting curve shows, regular deepfake content can induce long-term effects on brain function, memory, and the socio-emotional state of an individual, community, or even a nation.

Studies also show that deepfakes can develop automated response mechanisms or attitudes comparable to those established by genuine content (Hughes, 2021). It has also been underlined that deepfakes can cloud factual information and thus aid the problem of overabundance of information highlighted earlier, thus directly creating cognitive distortion (Ahmed, 2021). Adding the complexity of understanding, and the issue of quick reactions to the mix, deepfakes can lead to an emotionally volatile attitude, invoking hasty actions.

Do Influence Operations Work?

The effectiveness of Influence Operations was underlined in a 2021 study conducted through a systematic review of the available studies that examined Influence Operations to influence a specific population while maintaining statistical credibility (Bateman, Hickok, Courchesne, Thange, & Shapiro, 2021).

Figure 15: Effects of Influence Operations. Own work



The study underlined that social media-based Influence Operations can affect more than just beliefs (Figure 15). Among the short-term effects, multiple studies highlighted statistically detectable increases in racially motivated violence in a given area and increased political

violence in cases of targeted influence operation campaigns. However, beyond a rudimentary understanding of the long-term effects of such social media-based Influence Operations (which borrow heavily from the effects due to traditional mass media-based Influence Operations), the complex and interdependent effects of multiple Influence Operations running in tandem are not clearly understood. Further, considering the booming proliferation of newer platforms, the effects of targeted Influence Operations beyond the most popular platforms is also a critical gap in current understanding of the subject.

The above issue is accepted even by major platforms like Facebook, underlining the same in its 2021 'Threat Report on the State of Influence Operations 2017-20' (Facebook, 2021). The report highlights that as it becomes increasingly difficult to run large covert IOs without being detected, IO actors are turning toward 'Perception Hacking'. This means that instead of running actual on-platform IO campaigns, attempts are made to foster the widespread perception that everything is deception.

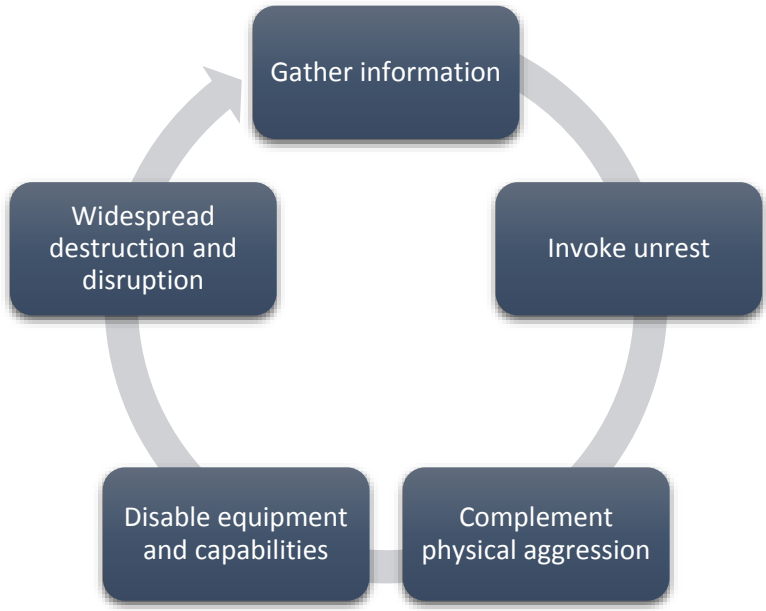
As mentioned in the early part of this study, information dominance and superiority are directly linked with information assurance. So, by creating widespread distrust, perception hacking campaigns seek to flood the information domain with skepticism, thus halting the flow of the right information to reach the person in need in time.

Moreover, the Facebook threat report reveals that sophisticated foreign IO actors are blurring the lines between foreign and domestic IO activity by amplifying narratives through collaboration with unwitting but sympathetic domestic actors. This develops a curtain between the amplifier and the natural source of narrative dissemination, thus making the process of attribution of any IO campaign complex. As a result, Facebook expects to see IO actors continuing to attempt weaponizing moments of uncertainty, exploit fault lines around the world, and elevate conflict-inciting voices.

Cyber Warfare

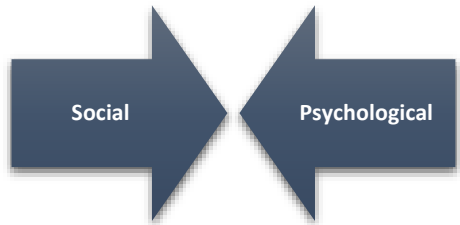
Unlike the effectiveness of traditional warfare, casualties do not indicate the success or failure of warfare conducted in cyberspace (Xu & Lu, 2021). Although the end goal remains the same – to impose costs on the adversary, cyber warfare comes with different aims and objectives. According to Chinese scholars, cyber warfare is waged for five scenarios – cyber espionage (for government-sponsored data gathering), for laying the groundwork for unrest and popular uprising, as a complement to physical aggression, for disabling equipment and capabilities, and widespread disruption and destruction (Li & Liu, 2021).

Figure 16: Objectives for Cyber Warfare Operations. Own work.



Available research indicates that the two key impacts of cyberattacks (conducted to wage cyber warfare) are social and psychological (Bada & Nurse, 2020). This utilises the social disruption caused by the cyberattacks to invoke emotions like anxiety, anger and fear, and loss of confidence in security capabilities.

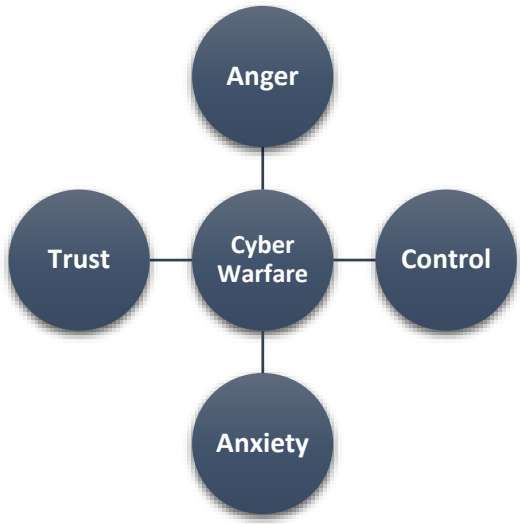
Figure 17: Key impacts of cyber-warfare. Own work.



As (Bada & Nurse, 2020) underline, malicious cyber-events result in a breach of trust, impacting the public perceptions of risk. These events also create a culture of fear, widely

considered a potent tool used as a weapon throughout history for manipulating and controlling people by blurring mental functions and confusing physical reactions.

Figure 18: Cyber Warfare Impact. Own work.



A study on how cyberattacks undermine public confidence and result in a drop in public trust highlights that instead of anxiety being a predominant emotion experienced by people exposed to significant cyberattacks, 'dread' (great fear or apprehension) is a more prevalent emotion (Gomez & Shandler, 2022). The study underlines that combined with hyperbolic media reporting in cyberattack events, the cumulative effect of cyberattacks can create psycho-political effects that can realign public trust and seed doubts over the government's ability to protect the citizens (Schneider, 2022).

Figure 19: Categories of Cyberattacks. Own work.

Cyberattacks are attempts to compromise the confidentiality, integrity, or availability of a system or information and can affect anything and anyone ranging from private data to critical national infrastructure. Cyberattacks like theft are generally categorised (Figure 19) as

cybercrimes, while cyber espionage is the modern version of spying. Among the most prevalent cyberattacks include the Distributed-Denial-of-Service (DDoS) and malware attacks, with ransomware attacks rapidly emerging as the most disruptive cyberattack in recent years.

Figure 20: Categories of Malware. Own work.

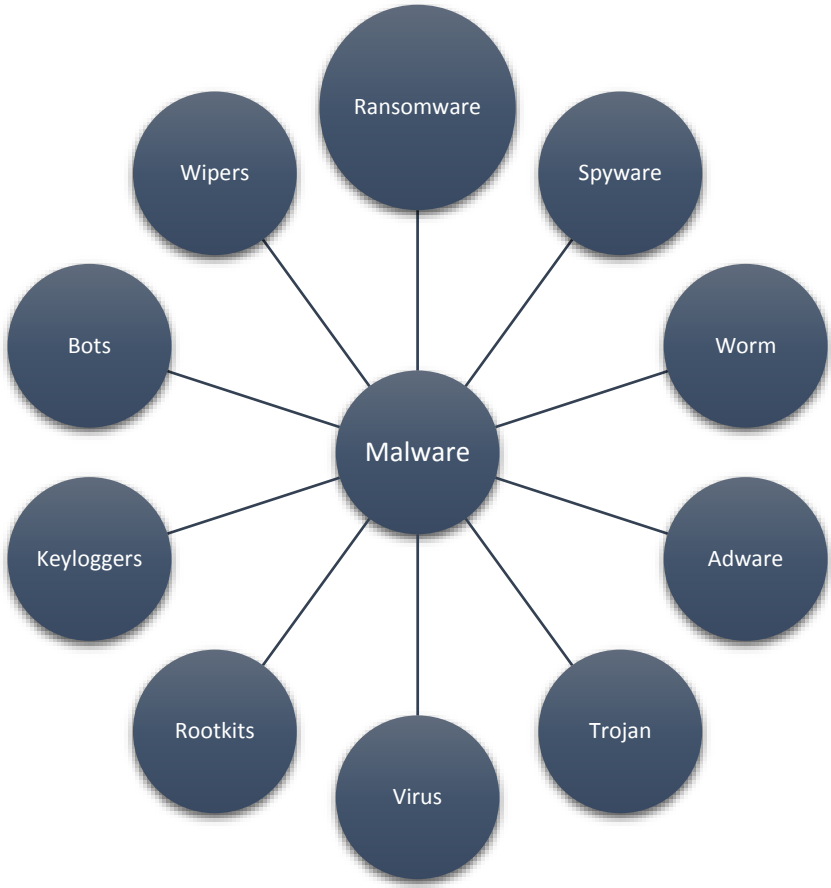


Table 1: Malware categories definitions. Own work

Category	Definition
Ransomware	Software that encrypts the targeted hardware and disables the user's access to data
Spyware	Collects information about user's activities
Adware	Erodes user privacy by overtly or covertly capturing user activity data for analysis/revenue
Trojan	Penetrates the targeted system by disguising itself as desirable code or software. Takes control of the system
Worm	Stand-alone and self-replicating malicious code that infects the target systems after entering through vulnerabilities, software backdoors and other entry points. Infects, steals and launches DDoS attacks on the network.
Virus	Malware triggered by an activating host. Infects, steals and launches DDoS attacks on the network.
Rootkit	Provides remote access to the system to the attacker

Keyloggers	Monitors user activity to steal passwords, and sensitive information
Bot	Software applications to perform automated tasks. Exploited to conduct attacks like DDoS by taking over targeted systems
Wiper	Erases user data without recoverability

In recent years, cyber warfare has undermined the election process in several countries and resulted in skepticism over the election process' integrity in people's cognition. This is an example of how cyber warfare significantly threatens national security. Further, cyberattacks can damage the economy, cause short and long-term disruptions to societal functioning, and even cause casualties in cases where public health and other safety services are impacted (witnessed during the 2017 WannaCry ransomware attack, which significantly impacted the UK National Health Services) (Fruhlinger, 2022).

Some of the most prominent cyberattacks in recent times and their impacts are presented here to provide an overview of how they result in substantial psychological effects-

DDoS Rationale

DDoS attacks are malicious attempts to disrupt regular servers, services, or network traffic by overwhelming it or the related infrastructure with internet traffic (Cloudflare). Though the motivations behind these attacks may vary and encompass financial, ideological and personal reasons. It is argued that DDoS attacks are generally opportunistic in nature, and target public-facing infrastructure like websites, instead of the actual services, leading to limited disruption. However, the major impact of these attacks is psychological, greater than the actual disruption of services (Gatlan, 2022). An example of how DDoS attacks are often deployed is through attacking media and human rights organisations. Once attacked, these organisations may self-censor to avoid future disruption of services and loss of revenue. This has been termed the 'chilling effect', resulting in a 'disempowering' effect (The Engine Room, June).

Bot Connection

Defined as software applications or codes to perform automated tasks, bots are utilised both in conducting DDoS attacks and for various tasks on social media platforms like Twitter to share and reshare targeted content. Studies have shown that bots increase exposure to negative and inflammatory content in online social systems, maneuver opinion dynamics, and effectively result in what is termed as 'social hacking' (Stella, Ferrara, & Domenico, 2018). It underlines that by targeting humans on social media platforms through generating semantic content that can invoke the target audience's already existing polarised stance, temporal behaviour patterns can be shaped to obtain the desired result. The study suggests that bots engage with messages that evoke negative sentiments and are associated with negative connotations.

Spyware Angle

Defined as any software that installs itself on a computer or smartphone and covertly monitors user behaviour without the user's knowledge or permission, spyware can result in harassment and physical attacks (Veracode). In addition, this can cause psychological effects on both those who have been a victim before and those who have come across such instances happening to others (Fong, 2022).

Ransomware Menace

Studies conducted on the psychological effects of a ransomware attack on organisations and individuals have shown that the impact of such events can persist long after the attack. These attacks tend to alter the worldview of the victims, with the majority of them turning more suspicious and feeling that the world is less safe (Help Net Security, 2022). This was highlighted during the 2017 WannaCry ransomware attack which crippled around 230,000 computers worldwide, impacting critical services like the health sector. (Kaspersky, 2023)

Cyber Terrorism

Among several other definitions, cyber terrorism is "a pre-meditated, politically motivated attack against information systems, programs and data, that threaten violence or results in violence" (Sheldon & Hanna Katie, 2022). This includes cyberattacks that intidimate or are meant to generate fear among the targeted audience. In this way, by conducting cyberattacks on critical infrastructure like hospitals, dams and schools, non-state actors intend to cause physical, political, psychological, economic and ecological damages (Maryville University, 2022) to induce fear among the public and coerce the victim to satisfy the cyber-terrorist's demands and objectives.

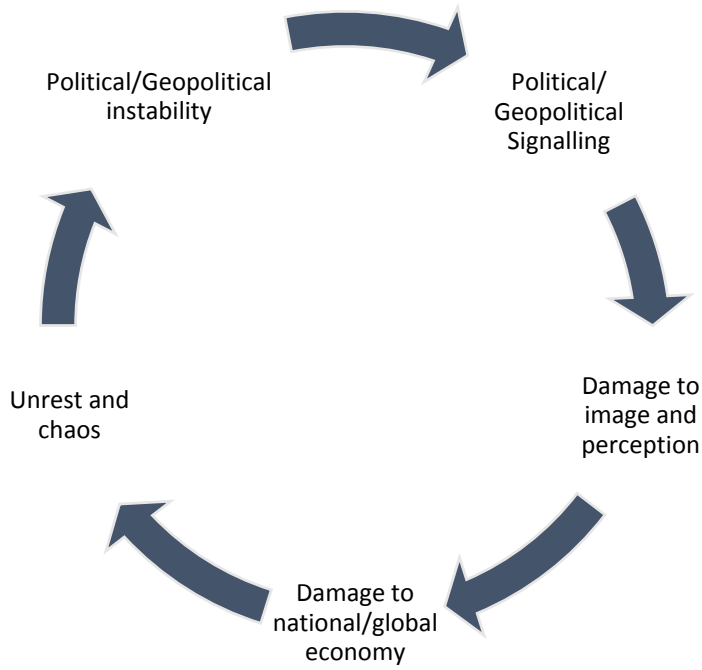
Some even suggest that the psychological effects caused by cyberattacks can rival those caused by traditional terrorism (Guynn, 2020). A study on how cybercrimes and cyberattacks like data breaches affect mental health underlined that such events are leading to depression and anxiety among people and are damaging their thinking patterns.

Influence Cyber Operations

Some scholars have also focused on the term 'influence cyber operations' or ICOs, when referring to the cyber operations/attacks that result in influence effects or when cyberattacks are directly aimed to support Influence Operations (Brangetto & Veenendaal, 2016). While it is widely accepted that the consequences of cyberattacks cannot be easily measured, unlike in the case of traditional warfare, the impact is gauged through an understanding of consequences in several domains. Also, it is argued that while individual cyberattacks may not be strategically consequential, the cumulative effect of several attacks may cause a

significant impact. Cyberattacks can create hidden and sometimes unintended consequences that are argued to facilitate political crises and re-frame cyber power as a strategic asset.

Figure 21: Consequences of Influence Cyber Operations. Own work.



The Chinese Discourse

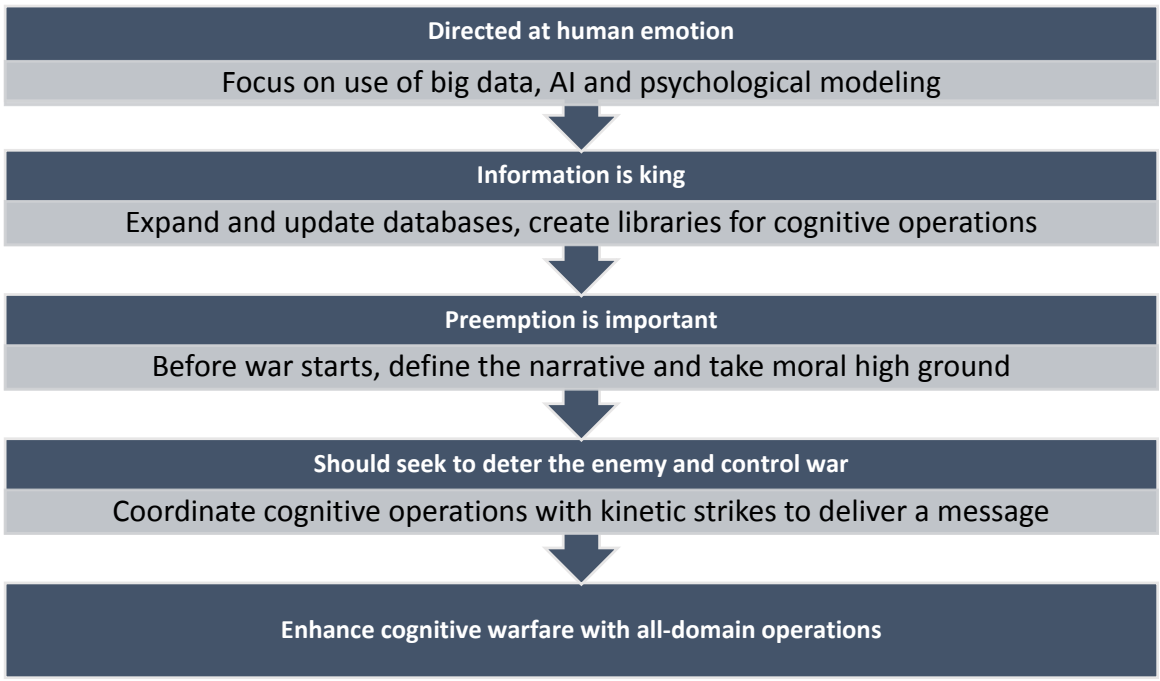
A 2019 White Paper titled 'China's National Defence in the New Era' underlined the Chinese concept of cognitive warfare, integrated with other concepts like 'intelligentised warfare' and 'informationized warfare' (The State Council Information Office of the People's Republic of China, 2019). While intelligentized warfare focuses on using new and emerging technologies like AI and increasing information-processing and rapid decision-making capabilities, China sees control over human cognition as the ultimate advantage for national security.

The Chinese definition of cognitive warfare aims for the systematic utilisation of cognitive science and biotechnology to achieve 'mind superiority' through the ability to influence the adversary's cognition through activities ranging from public opinion (peacetime) to decision-making (wartime) (Cluzel, 2020). For China, 'Military Brain Science' or MBS is essential for innovative military applications in the cognitive domain of operations on the battlefield, while AI is seen as a 'national weapon' (Cluzel, 2020).

At various instances, the Chinese President Xi Jinping has remarked that cyber surveillance, cyberattacks and cyber terrorism have become global scourge (MFA China, 2015). However, the stance taken by the Chinese government under his leadership gives a glimpse of how China now sees military-civil fusion in cybersecurity and informationisation as frontier fields for projecting Chinese power globally (Doshi, Bruyere, Picarsic, & Ferguson, 2021). It is argued that Xi's strategy in the cyber domain refects his insecurities and ambitions to consolidate power, protect his own image, and control the Chinese people inside and outside China (Babb, 2023). For this, all the components of cognitive warfare come into picture.

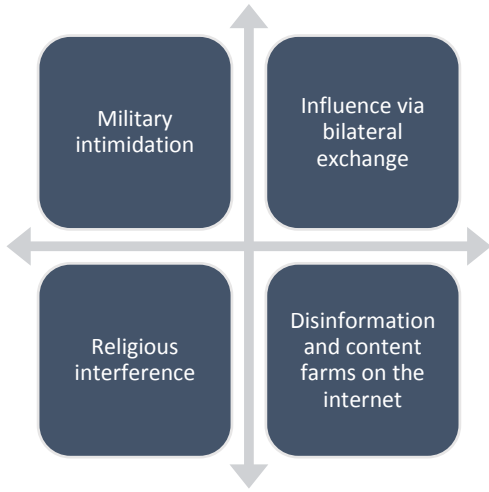
According to an article published in the official paper of the People's Liberation Army, cognitive warfare comprises five elements (Longxi, 2022)

Figure 22: Elements of cognitive warfare for coercing opponents. Own work.



Being amongst the most intense recipients of Chinese cognitive warfare, Taiwanese researchers define Chinese cognitive operations through four main categories (Hung & Hung, 2022)-

Figure 23: Chinese Cognitive Operations. Own work.



The Chinese military has taken a comprehensive approach to theoretical and practical cognitive warfare applications. Studies conducted and published by Chinese military personnel highlight the assigned priorities toward which strategic thinking is now rapidly evolving.

Arguing that the influence of rational factors such as science and logic on individual cognition is likely to be weakened in future cognitive domain operations, the Chinese perspective holds that cognitive confrontation will become a contest between the emotions of the two sides (Zhiwei, 2022). Further, as human brain cognition rises as a field of military confrontation, the logic around information dissemination will transform, thus, promoting greater fundamental changes in cognitive domain operations that are currently underway.

Artificial Intelligence (AI) has been deemed by the Chinese leadership as one of the most significant avenues for bringing China at the helm of the global power structure, through both military and economic power (Allen, 2019). The 'New Generation Artificial Intelligence Development Plan' issued in 2017 by China's State Council and the 'Made in China 2025' document from 2015 highlight the Chinese focus on AI as a strategic technology for enhancing national competitiveness and national security (Allen, 2019). AI is also highlighted as the top technological priority in China's five-year economic plan for 2021-26.

In several speeches, Xi Jinping has emphasised the need for achieving world-leading levels in AI, both in technical domain, as well as the theoretical domain. This focus has been visible in China's accelerated progress in military capability development, centered around 'informationisation' and 'intelligentisation'. It is argued that AI for China is now a matter of 'leapfrog development' in the military domain, to overcome the overwhelming conventional

US military capabilities (Allen, 2019). Furthermore, the progress attained by China in the field of AI has been termed as 'dramatic' and 'stunning', with statistics underlining the increase in Chinese global share of research papers on AI from around 4 per cent in 1997 to more than 27 per cent in 2017, surpassing even the US (Li, Tong, & Xiao, 2021). The benefits of strong AI promoting policies, weak privacy regulations, huge markets and the big data sets it generates, have been argued as some of the several important reasons for China's quick development in this domain.

The Chinese perspective also sees Artificial Intelligence as the primary driver of cognitive domain operations, arguing that "information dissemination is based on data, and the AI technology runs through the entire process of information collection, production, and feedback" (Zhiwei, 2022). Furthermore, recognising AI as a disruptive technology, this perspective sees the extensive and in-depth application of AI as a key aspect of the entire process of future cognitive domain combat planning and implementation.

A prominent aspect of exploitation of information sphere in the cognitive domain is that of 'emotional conflict'. As highlighted earlier (Reaction vs Response), the Chinese argument underlines that through the "centralised release of large batches of information in a short period, the response time of individuals can be greatly compressed, making it difficult for individuals to think deeply" (Zhiwei, 2022). Thus, while new technologies are expected to broaden the scope of human cognition and deepen people's perception, they are also expected to distort 'deep thinking', thus making it greatly susceptible to external impressions. As a result, intensified irrational and emotional responses to information will increasingly diminish the influence of rational perspectives in the information sphere.

Another Chinese scholar underlines that cognitive warfare is similar to a combination of long-term cultural implantation aided by adversarial information suppression (Cunshe, 2022). This takes place through forming an 'information ocean' while diminishing voices and ideas that may reduce the potency of cognitive operations. Three factors are underlined as being crucial to succeed in the cognitive domain effectively –

1. The right to define the nature of events – How the audience looks at an event (just/unjust, legal/illegal).
2. The dominance over defining the event process – What should be done/not done, who is doing the right/wrong thing
3. The right to judge the event's outcome – How to evaluate the winner/loser, immediate winner/loser, and long-term winner/loser.

In this context, the Chinese perspective seeks to adopt pre-emptive strikes and chalking of pre-emptive definitions, crafting groups and alliances, and defining concepts theoretically to attain dominance on the changing discourses in strategic thinking. Then, by dominating the definition of the event process, the dominant party can lead the development direction of the target event, which would satisfy the interests of the dominant party. Finally, by controlling the right and power to judge the outcome of an event, the dominant side can magnify advantages for self and disadvantages for the other side. It is argued that a visible example of

this phenomenon is the ‘intellectual confrontation’ on social media platforms, trying to achieve the ‘first mover’s advantage’[2] on any specific event, theme, or discussion.

Cognitive operations are deemed full-time offensive and defensive, global shaping, and whole-of-government actions, which are multi-level, cross-domain, and long-term, going beyond the boundaries between wartime and peacetime and combing the military goals with political ambitions (Cunshe, 2022).

As the Russian Federation's information security doctrine highlighted earlier, the Chinese perspective also accepts cognitive warfare as a whole-of-government action, which requires coordinated and concerted actions across departments, fields, and the military, for the best effect.

Chinese Influence Operations have attracted global attention in the past decade. Beijing follows the ‘three warfare doctrine’ formulated in 2003, encompassing psychological warfare, public opinion warfare, and legal warfare (Singh A. , 2013). These can be viewed from the prism of the eight steps of warfare highlighted earlier. Taking it all together, some experts deem it ‘cognitive warfare’, the sixth domain of warfighting, beyond air, water, land, space and cyberspace.

Several studies have highlighted Beijing’s objective to influence foreign audiences to satisfy China’s interests by any means possible. It includes disinformation campaigns targeting governance mechanisms in other countries, exploiting societal divides or fault lines, and penetrating societies by creating a positive self-image.

Calling Chinese Influence Operations ‘A Machiavellian Moment’, a report by a France-based Institute highlights how Beijing now employs infiltration and coercion tactics, going beyond the past strategy of ‘seducing and subjugating’ through the attractiveness of Chinese cultural or governance aspect (Charon & Jeangène Vilmer, 2021). The report explains that Beijing has two main objectives – crafting a positive representation of China and penetrating the adversarial societies to reduce the possibilities of any actions contrary to the Chinese ruling regime.

[2] First mover’s advantage is the competitive edge gained by the initial significant occupant of a market segment.

Figure 24: China's Information War Actors. Own work.

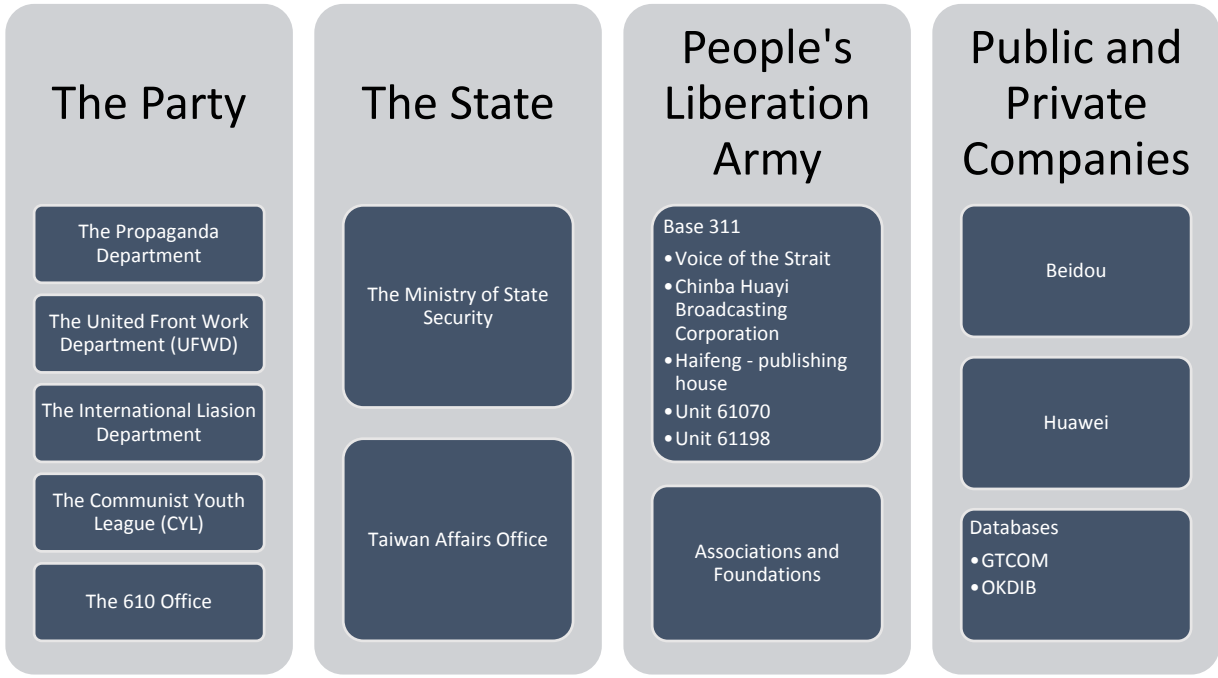


Figure 25: Elements in China's Influence Operation Model. Own work.

Towards these objectives, China has developed various bodies and mechanisms like the Propaganda/Publicity Department that oversees ideological work, the United Front Works Department (UFWD) that runs Influence Operations affecting domestic population inside China, as well as foreign audiences beyond the borders, the International Liaison Department that serves as a parallel diplomatic channel to conduct secret negotiations, the Communist Youth League to serve as a 'relay' between the CCP and the Chinese youth, and the 610 office to detect and record any anti-party religion based activities (Charon & Jeangène Vilmer, 2021).

The War on India's Conscience

As this study has highlighted, the war on conscience is waged by cognitive warfare, which spans across information and cyber warfare. To understand how India is amidst this war, we need to look at both the aspects of informational and cyber operations that are inflicted on India. By joining the pieces together, this part attempts to provide a broad, yet non-exhaustive view of the ongoing operations against India. For the sake of brevity, only the summary of various reports, and broad findings have been underlined, rather than specific examples or images. The reports mentioned in this part can be investigated for a deeper view.

In August 2021, the New Delhi based think tank 'Law and Society Alliance' released a report titled 'Mapping Chinese Footprints and Influence Operations in India', highlighting how the Chinese Communist Party (CCP) cultivates, funds, and sponsors institutions in India in fields like cinema, technology, fintech and education, to shape public opinion suiting Beijing's interests (Law and Society Alliance , 2021).

A year later, in August 2022, a US-based think tank claimed that a Beijing-based AI company 'Speech Ocean' had collected voice samples from military-sensitive regions of India (like Jammu & Kashmir and Punjab) most probably to be used and analyzed by the Chinese military (Balding, Sinha, & Wu, 2022). This was done through a New Delhi-based intermediary subcontracted to recruit individuals to record phrases in exchange for small amounts of money. Later, the data was traced to Hong Kong and Germany-based servers; both registered to China's Alibaba group.

Chinese state media outlets have operated social media accounts in multiple Indian languages and garnered a vast following (Freedom House, 2023). They have also sought active engagement with Indian journalists and offered subsidised trips to China. Further, China has sought to employ emerging technologies like AI to accelerate the creation and dissemination of fake news and disinformation. While quickly regulating technologies like deepfakes in China, Beijing is said to be encouraging pro-Chinese influence operation campaigns through Spamouflage—highly deceptive deepfake video content which uses AI to create a video using fictitious people posing as news anchors (Graphika, 2023). Using AI tools for content creation exponentially decreases costs while increasing the content generation speed. This was underlined in a 2022 report by analytics firm 'Graphika', revealing a pro-Chinese operation running since 2019, promoting video content through AI-created news anchors on a platforms name Wolf News (Graphika, 2023).

Chinese penetration in India's neighbouring countries in South Asia have also been highlighted through several studies. A study by the US-based think tank Carnegie underlines that Beijing has adopted a distinct strategy in Bangladesh by prioritising outreach to Bangladeshi media instead of coercion in response to any criticism of Chinese projects appearing in the national media (Pal, 2021). Chinese scholarships and schemes have focused on hiring Bangladeshi journalists for Chinese-state owned media to craft a positive Chinese image in the Bangladeshi imagination. Experts have also drawn attention to the steadily rising Chinese influence and presence in Dhaka and Chittagong, and the attempts to counter India's cultural affinity in the country (Cookson & Joehnk, 2018).

Similarly, the Sino-Nepalese media cooperation on content has been growing with platforms like China Radio International running special programs geared specifically toward the

Nepalese audience. Along with developments in institutional partnerships in culture and academic domains, Beijing has continued efforts to craft its mainstream image of a friend looking for techno-economical development of Nepal (Pal, 2021). The same study argued that Sri Lanka has been trapped in a situation of elite capture and crony capitalism, where the government in power gave-in to the Chinese overtures in return of economic and trade inflows. During the previous decade, Sri Lankan media depicted government's engagement with China as a nonaligned approach, thus shaping the societal perception in Sri Lanka, while the political actors led the country toward an economic crisis of unprecedented scale.

On the other cognitive front, as shown in Table 2, Chinese cyber warfare operations against India intensified since the Galwan Valley clashes along the Indo-China border in May 2020 (Kaushik, 2020). China has repeatedly targeted India's critical infrastructure sectors like power grids, IT systems, banking and the health sector, with daily cyberattacks on Indian facilities reaching a new peak every time an intense situation is observed along the border.

According to a September 2021 report by the global cybersecurity firm CrowdStrike, China was found to be behind 67 per cent of state-sponsored cyberattacks, miles ahead of next-in-line Iran with just 7 per cent (Alspach, 2022).

Table 2: China-linked cyberattacks on India since 2020. Own work.

Timeline	Cyberattacks on
June 2020	Indian banking sector and IT infrastructure
October 2020	Mumbai power grid
February 2021	Times Group
March 2021	Covid-19 vaccine manufacturing units
June 2021	Indian telecom companies and defence contractors
July 2021	UIDIA database
December 2021- April 2022	Power grids in North India
December 2022	Attacks on Indian health sector institutions (AIIMS, Safdarjung, etc.)

According to the China Index 2022, which explores China's influence in 82 countries through questions asked from experts on China's activities in their country, Pakistan topped the index, with Chinese influence being most active in Pakistan in domains of technology, foreign policy, and military (DoubleThink Lab & China in the World, 2023). On other aspects like media, academia and society as well, Pakistan scored higher than most countries for Chinese influence. According to several experts, Pakistan is now deeply reliant on Beijing which has a significant controlling capability on Pakistan's digital infrastructure and digital space (Hillman, 2021). It has also been underlined that Pakistan's data is increasingly in China's hands and that views critical of China are kept away from Pakistani information space. Like China, Pakistan has developed robust institutional frameworks devoted to conducting information warfare.

The media and public relations wing of Pakistan's Armed Forces, the 'Inter Services Public Relations' or ISPR, serves as the central hub for conducting Influence Operations both inside Pakistan and abroad (Malhotra, 2020). Moreover, the ISPR runs an internship scheme to recruit and train young minds to engage in information warfare, especially against India. It is

argued that this provides Pakistan's army with the benefit of leveraging tech-savvy youth and eliminating the need to re-train the existing soldiers (Malhotra, 2020).

A June 2021 report by analytics firm Graphika, titled 'Lights, Camera, Coordinated Action!' highlighted that Facebook had removed a network of Pakistani-origin pages and accounts engaging in coordinated inauthentic behaviour (Ronzaud, et al., 2021). While disseminating praise for Pakistan's armed forces, the network conducted attacks against India (especially focused on alleged human rights abuses in Jammu and Kashmir) through short news bulletins, screenshots of media articles, and photos. Graphika found that the network was coordinated by a Pakistan-based public relations (PR) firm with connections to the ISPR.

In October 2022, a Sweden-based 'Nordic Research Monitoring Network' report highlighted that Pakistan has set up a cyber army with Turkey's help to shape public opinions and attack adversaries (Bozkurt, 2022). It was underlined that the proposal to set up such a unit was discussed between interior ministers of Turkey and Pakistan in 2018 and was given the go-ahead by the then Pakistani Prime Minister, Imran Khan. According to estimates, around 6000 Pakistani police officers were trained by Turkey to counter Pakistan's negative perception using social media (Bozkurt, 2022).

Several studies and reports have revealed the vast network of Turkish Influence Operations across the world. Turkey's ruling regime seeks to establish international digital platforms to disseminate its perspective and use culture to perpetuate its interests. This holds special significance for a country like India, where Turkey has been successful to an extent through film series like Ertugrul Ghazi, which projects ambitions of a Greater Ottoman Empire. (Haque & Meo, 2020) (Subramanian, 2021). Being the only country that actively supports Pakistan's Kashmir agenda on global platforms like the UN and the Organization of Islamic Cooperation (OIC), Turkey's strategic considerations and efforts in the information warfare domain are in sync with Pakistan more than any other country (PTI, 2016 August) (Quamar, 2021).

Turkish media broadcasters TRT World and Anadolu Media work with Pakistani and Qatari counterparts, spreading disinformation about India in the Gulf region. Per claims made in 2021 by Mediterranean-Asian Investigative Journalists, Turkey and Pakistan formed a secret army of mercenary journalists by recruiting Kashmiri journalists in large numbers (including from Pakistan-occupied-Kashmir) (RIEAS, 2021). In India, TRT World has also been criticised for spreading misinformation through its biased coverage of India. As the report underlined, TRT World published over 30 long stories about India's abrogation of Articles 370 and 35A.

According to reports from 2020, Turkey had allocated funds for its intelligence agencies to radicalise Indian Muslims with the help of preachers recruited from surrendered Islamic State (ISIS) cadres (European Parliament, 2021). Ankara offers scholarships and exchange programs for Kashmiri and Muslim students through state-sponsored NGOs, who are on the radar of Pakistani operatives. Another report from 2022 stated that Indian intelligence agencies found evidence of information warfare from the Turkey-Pakistan duo over the Kashmir issue, aimed at influencing the perceptions in Islamic countries (Bhatt, 2022).

For India, the size and diversity of the targeted population exponentially magnifies the scale of the threat. According to various estimates, India has around half a billion (0.467) social

media users and around 0.692 billion internet users, of which 70 per cent are below 35 years of age (The Global Statistics, 2023). As per a study conducted by the Oxford University Press, more than half of the Indian population turns to social media in search of factual information. Further, as high as 87 per cent of those sharing information from social media are confident of its truthfulness (LiveMint, 2022).

By numbers, India has the greatest number of Facebook users in the world. Also, according to the Indian Consumer Sentiment Index, Facebook is the preferred social media platform for Indian users. However, by 2022, Facebook relied on a mere 10 fact-checking partners in India, covering just 11 languages (Shivji, 2021). Most of the content moderation is left to the Artificial Intelligence engines, which may not be well-versed in the diverse indigenous languages in India.

In September 2021, the Supreme Court of India expressed concern over the dissemination of inflammatory fake news by media and web portals, underlining that social media platforms like Twitter, Facebook and YouTube are being misused to tarnish the image of Indian institutions, highlighting that unchecked nature of these activities would bring a bad name to the country (Times of India, 2021). In December 2022, India banned 104 YouTube channels, several websites, and multiple Instagram, Twitter, and Facebook accounts, spreading fake news (Sengupta, 2022). In April 2023, Google underlined that it recorded an all-time high trend of misinformation in India, stating that in a bid to fight the growing issue, it will bring features to let users evaluate the information and understand its source (Indian Express, 2023). But beyond the handful of the most popular platforms highlighted above, dozens of considerably popular platforms and even newer platforms that periodically emerge do not have any capacities to counter Influence Operations, thus leaving those on these platforms extremely vulnerable.

The information war on India is also propagated continuously from the West. It has been frequently highlighted that opinions, headlines, and editorials carried by Western media and publishing houses like The New York Times, Washington Post, Foreign Policy, Guardian etc, have sought to create a negative image of India on themes like minority rights, democracy, and freedom of religion (Gandhi, 2020). A study underlining India's portrayal in the US press over a 48-year period during and after the Cold War, gives an indication of why the Western media has been traditionally hostile toward India in the past many decades (Mazumdar, 2019). Among other key points, it highlights that during the entirety of Cold War, India's closeness to the Soviet Union and the US-Pakistan close ties resulted in the US media regularly working with the aim of tarnishing India's image. While the situation improved gradually since the 2005 US-India civil nuclear deal, showcased in the changed nature of media attitude toward India, it has gone through several ups and downs.

The Indian stance toward the Russia-Ukraine war has come under criticism from the West since February 2022 and the Indian policymakers have frequently been at the target of Western media houses. At one of the events in the US, pointing to the American media houses, the Indian foreign minister had remarked that, "there are some newspapers which everyone knows what they are going to write about" (PTI, 2022). Emphasising that there are biases, he underlined the importance of not sitting back and letting others define India. As the Western media continues to put out inaccurate, biased reporting and narrative to manipulate, distort and harm India's international image (ANI, 2022), it is important to realise the cognitive effects this can have on India in long-term.

Towards India's National Information Strategy

It is imperative for India to see, understand and evolve a counter strategy towards the transforming information war paradigm through an Indian perspective. Many prominent voices, like the former Indian Army chief, General MM Naravane, have underlined the need to incorporate the widely known *Chanakya Neeti* in India's strategic and military thought process. Also known as 'Arthashastra', it defines how one attains the end through non-military methods like intrigue, duplicity, and fraud before waging an armed conflict (Philip, 2020). As Acharya Chanakya noted, if efforts toward *saama* (peaceful negotiation) *and dana* (gifts) fail, the next step before waging the final war (*danda),* should be *bheda*, meaning sowing dissent among the adversaries. As India prospers, its adversaries will seek to undermine India's rise through these mechanisms, especially those unable to wage a symmetric conventional war.

As highlighted in earlier parts of this study, calls for an information strategy in the US, the doctrine of information security in Russia, and the increasing focus on cognitive warfare in China to assimilate emerging technologies like AI, are now turning the attention toward the rising security concern in the information and cognitive domains. Further, facing similar threats in the cognitive domain as India, the newly released Japanese National Security Strategy 2022 (Cabinet Secretariat, 2022) and the National Defence Strategy 2022 (Ministry of Defence Japan, 2022), showcase a focus on addressing the threat of cognitive warfare. Japanese strategy underlines its aim to strengthen capabilities to respond to information warfare in the cognitive domain. To this aim, the new security strategy seeks to create a new entity within the government to collect and analyze disinformation originating abroad, improve external communication, and enhance cooperation with non-governmental organizations. Along with this, the new defence strategy aims to advance the intelligence capabilities for countering 'hybrid and integrated information warfare', focusing on the cognitive domain, by 2027 (Nishikawa, 2023). These capabilities include enhanced fact-checking and counter-messaging and a whole-of-government response during contingencies.

As per reports, India is expected to adopt a new national cybersecurity strategy in 2023, which would update the previous strategy from 2013 (ET Telecom, 2023). India has created a National Counter Ransomware Taskforce under the Ministry of Home Affairs and is taking a whole-of-society approach by basing the new frameworks on the principles of common but differentiated responsibility (CBDR), focusing on responsibilities to be shouldered by individuals, businesses, academia, and the government. The India army has also recently operationalised new specialist units to counter online threats, under its cyber warfare initiaitves. The 'Command Cyber Operations and Support Wings' (CCOSW) are mandated to assist toward strengthening the cybersecurity posture of the Indian army (ANI, 2023). Further, the Indian government is looking to amend (Digital India Bill) the Information Technology (IT) rules 2021, which brings obligations for intermediaries such as social media platforms to monitor and regulate user content that is identified as false or misleading by government's fact-checking unit – The Press Information Bureau, or any other authorised agency (Singh S. , 2023). This step is expected to counter information warfare against India through disinformation and information flooding. A successful implementation of this stratregy will require institutionalisation of both platforms (like fact-checking bodies and monitoring for emerging threats in the cognitive domain) and policies (in consonance with technology and social media companies).

Conclusion

The discourse over cognitive warfare will increasingly gain significance as the information warfare paradigm continues to evolve in synchronisation with technological developments. As this study has underlined, information and cyber warfare now aim to inflict cognitive effects.

Cognitive warfare aims to influence mental states and behaviours by manipulating environmental stimuli and has been defined as a type of psychological-social-technical warfare, combined with influence cyber operations. Cognitive operations span physical zones, information and cyberspace, and cognitive processes. It is argued that digital colonisation is possible through cognitive operations, similar to state colonisation through the seizure of territory and control over the economy. Further, information availability, unavailability, or 'over-availability' is related to cognitive rationalisation. Flooding the information space through crafted content aimed at specific audiences can lead to cognitive distortion, resulting in distorted thinking patterns.

Information war encompasses several spheres, like information assurance, superiority, and dominance. The operations conducted to influence the adversary through elements like manipulating public information, public diplomacy, and perception management are deemed psychological operations or PSYOPS.

Influence Operations have been part of the strategic thought in the US, Russia, China (and others) for decades. Russia and the US have engaged in Influence Operations against each other for the entirety of the Cold War in the twentieth century. In the US strategic thought, its military capabilities are decisive only till it enjoys information dominance over adversaries. Whereas, in Chinese strategic thought, securing information dominance is an essential part of the overall approach to warfare, and information superiority has become the priority mission of modern warfare. Today, Chinese strategists deem the information war as an ever-ongoing phenomenon.

Russia has adopted the concept of information security, underlining its focus on the need to counter the 'information threat' to secure its sovereignty and socioeconomic interests. Its doctrine encompasses financial, economic, defence, strategic, social, technological, and academic domains. It holds that information aggression can be used together with political and economic pressure.

It has to be underlined that while Influence Operations have been practiced for a long, the rapid evolution of the digital domain in the last two decades has transformed the capabilities to conduct cognitive warfare. New technologies like AI chatbots, deepfakes, and data processing capabilities have significantly increased sophistication and speed for exploiting the information domain.

While several studies have underlined the short-term effectiveness of Influence Operations, the long-term effects are still unclear. The process of conducting Influence Operations can be analysed through various frameworks, like Schneir's 8-step process model, highlighted in this study. The studies analysing these operations have indicated that Influence Operations lead to shifts in political beliefs and behaviour, increased skepticism, and altered political beliefs. Beyond this, they have been linked with an increase in racially motivated violence.

Cyber warfare is being used in conjunction with Influence Operations for cognitive effect. As cyber warfare affects socio-psychological states, invoking emotions like anxiety, anger, and fear, cyberattacks and other malicious cyber-related activities undermine public confidence and trust in their government.

In recent years, influence cyber operations, cyber terrorism, ransomware, spyware, etc., have been used for political and geopolitical signaling, damaging the image of adversaries, damaging their national economy, sowing unrest among citizens, and aiming to instill political instability.

The Chinese definition of cognitive warfare has aimed to systematically utilise cognitive science and biotechnology to achieve 'mind superiority'. Its focus on concepts like 'intelligentised warfare' and 'informationised warfare' pivots on using new and emerging technologies, like AI, for information-processing and rapid decision-making capabilities. The Chinese military has taken a comprehensive approach toward the cognitive domain, spanning both theoretical and practical aspects, while underlining that the influence of rational actors like science and logic will likely be weakened in the future.

The Chinese perspective seeks to conduct pre-emptive strikes through definitions, concepts, and alliances to attain dominance in the changing discourses in strategic thinking. It deems cognitive warfare a multi-level, cross-domain, long-term and continuous phenomenon. Following the three warfare doctrine, concentrating on psychological warfare, public opinion, and legal warfare, Chinese efforts in the cognitive domain also incorporate cyberattacks and cyber espionage. Chinese technology is being deployed to generate fake news and disinformation, aiding in its coercive capabilities in political and geopolitical ambitions.

In recent years, various reports have highlighted the Chinese activities on these themes. However, China has also found support towards its ambitions to dominate the cognitive domain. As various revelations indicate, Pakistan has emerged as a Chinese ally for mutual interests in India. Along with partners like Turkey, Pakistan, and China are working to influence public opinion and behaviour in India, which has been reflected in several threat assessment reports by social media platforms like Facebook and Twitter and digital platforms like Google.

Considering this, India needs to evolve a counter strategy, which focuses on the entire gamut of activities that its adversaries are working on. The Chinese strategy for dominating the conceptual and intellectual sphere has to be countered in parallel with boosting cyber defence and offence capabilities. This demands a National Information Strategy, sewed together with a National Cybersecurity Strategy. Toward this, India should borrow from its rich and unique strategic thinking stratagems like *Arthashastra* and counter the threats to its cognition.

Glossary of Terms

Arthashastra

Indian treatise on statecraft, economic policy and military strategy written by Kautilya (also known as Chanakya). Dated to 3rd century BC.

Art of War

Chinese military treatise composed by Sun Tzu, devoted to skills related to warfare. Dated to 5th century BC.

ChatGPT

Artificial Intelligence chatbot. It is a language model created to hold conversations with end user, through natural language processing. This technology is also called as generative AI.

Cognitive Dissonance

State of mind that occurs when two or more opposite ideas are simultaneously entertained.

Cogntive Distortion

Internal mental biases or filters that increase or fuel anxiety and evoke negative emotions. These are thoughts that cause individuals to perceive reality inaccurately.

Cognitive processes

Basic mental processes such as sensation, attention, and perception. Also includes complex mental operations such as memory, learning, language use, problem solving, reasoning, intelligence, and decision making.

Cognitive Rationalisation

Attempt to logically justify a decision or belief.

Cognitive Warfare

An unconventional form of warfare using cyber tools to alter enemy cognitive processes, exploit mental biases, or reflexive thinking, and provoking cognitive distortion.

Colonisation

Process of establishing foreign control over target territories or people, generally for economic and strategic interests.

Cyber Espionage

A type of cyberattack which uses unauthorized user attempts to access sensitive or classified data. Also termed as cyber spying.

Cyber Security

The practice of protecting any assets (like computers, servers, networks, other devices as users) against cyber threats.

Cyber Terrorism

A cyberattack exploiting communication/computer networks to cause sufficient disruption or destruction to geneate fear or to intimidate a society into an ideological goal. Also defined as unlawful attacks and threats of attack against computers, networks, and the information stored therein when

done to coerce or intimidate a government or people in furtherance of social, economic, or political objectives.

Cyber Warfare

A cyberattack or a series of them, targeting a nation-state or international organizations, aimed at causing damage to systems or information.

Deepfake

Synthetic media that has been digitally manipulated through Artificial Intelligence technology to create convincing audio, visual or image content.

Deep Thinking

The process of shedding preconceived ideas in order to discover the truth.

Electronic Warfare

The ability to use electromagnetic spectrum to conduct activities like detecting, interpreting or detecting signals, against adversary.

Hybrid warfare

Fusion of conventional as well as unconventional instruments of power and warfighting methods.

Infodemic

Too much information including false or misleading information during a disease outbreak.

Information Assurance

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. It is the practice of managing information related risks.

Information Dominance

The superiority in the generation, manipulation and use of information sufficient to afford its possessors military dominance.

Information Operations

The collection of tactical information about an adversary. Also, the dissemination of propaganda to achieve competitive advantage.

Information Overabundance

Also known as Information Overload. It is the difficulty in understanding and decision-making due to too much information at disposal.

Information Security

The practice of protecting information by mitigating information risks.

Information Space

The body of information with which a user interacts.

Information Superiority

Operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information, while denying an adversary's ability to do the same.

Military Brain Science

The cutting-edge innovation science that uses potential military application as the guidance.

Overgeneralisation

A cognitive distortion which causes a person to apply something from one event to all other events.

Polarisation

Cognitive distortion in which a person only thinks about extremes in relation to any event or situation.

Propagandism

The action, practice, or art of propagating doctrines or of spreading or employing propaganda.

Revolution in Military Affairs

The inclusion and expansion of new technology within current military tactics.

Soft Power

The use of positive attraction and persuasion to achieve foreign policy objectives.

Spaced Repetition

A method of reviewing material at systematic intervals as part of a learning and remembering process.

References

Maan, A. (2018). *Narrative Warfare.* CreateSpace Independent Publishing Platform.

Diggins, C., & Arizmendi, C. (2012). *Hacking the Human Brain: The Next Domain of Warfare*. Retrieved from Wired: https://www.wired.com/2012/12/the-next-warfare-domain-is-your-brain/

Claverie, B., & Cluzel, F. (2021, June 21). *Cognitive Warfare: The Future of Cognitive Dominance.* Retrieved from NATO CSO CSTO: https://hal.science/hal-03635889/document#:~:text=Cognitive%20warfare%20is%20the%20art,is%20too%20slow%20or%20inadequate

Danyk, Y., & Briggs, C. (2023). Modern Cognitiv Modern Cognitive Operations and Hybrid W ations and Hybrid Warfare. *Journal of Strategic Security , 16*(1), 35-50.

WHO. (2023). *Infodemic*. Retrieved from World Health Organization: https://www.who.int/health-topics/infodemic#tab=tab_1

MBC. (2018, April). *Cognitive Distortions Reinforced Through Social Media*. Retrieved from Mind Boy Co-op: https://mindbodycoop.com/cognitive-distortions-reinforced-through-social-media/

Sonnad, N. (2018, February). *You probably won't remember this, but the "forgetting curve" theory explains why learning is hard*. Retrieved from Quartz: https://qz.com/1213768/the-forgetting-curve-explains-why-humans-struggle-to-memorize

PsychCentral. (2022, January). *15 Cognitive Distortions To Blame for Negative Thinking*. Retrieved from PsychCentral : https://psychcentral.com/lib/cognitive-distortions-negative-thinking

Cisco. (n.d.). *What Is Information Security?* Retrieved from Cisco: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html

NIST CSRC. (n.d.). *Information Assurance*. Retrieved from National Institute of Standards and Technology: https://csrc.nist.gov/glossary/term/information_assurance#

Perry, W., Signori, D., & Boon, J. (2004). *Exploring Information Superiority.* RAND.

Libicki, M. (1997). *Information Dominance.* Instiute for National Strategic Studies.

Malzac, J. (2022). Expanding Lawful Influence Operations. *Harvard Law School National Security Journal*.

Jash, A. (2019). *China seeks to "Informationisation" to Fight Modern Warfare* . Retrieved from https://indianarmy.nic.in/writereaddata/Claws/China%20Seeks%20to%20informationisation%20to%20fight%20modern%20warfare.htm

Khan, K. (2012). Understanding information warfare and its relevance to Pakistan. *Strategic. Studies, 32*(4), 138-159.

Keller, T., Graham, T., Angus, D., Bruns, A., Marchel, N., Neudert, L., . . . Mortensen, M. D. (2020). Coordinated Inauthentic Behaviour' and Other Online Influence Operations in Social Media Spaces. *The 21st Annual Conference of the Association of Internet Researchers.*

Schneier, B. (2019, August). *8 Ways to Stay Ahead of Influence Operations*. Retrieved from Foreign Policy: https://foreignpolicy.com/2019/08/12/8-ways-to-stay-ahead-of-influence-operations/

Hallinan, B., Scharlach, R., & Shifman, L. (2021, August). Beyond Neutrality: Conceptualizing Platform Values. *Communication Theory, 32*(2), 201-222.

Livingstone, C. (2023, April). *ChatGPT, the rise of generative AI BrandPost*. Retrieved from CIO: https://www.cio.com/article/474809/chatgpt-the-rise-of-generative-ai.html

Sedova, K., McNeill, C., Johnson, A., Joshi, A., & Wulkan, I. (2021). *AI and the Future of Disinformation Campaigns.* Georgetown: Centre for Security and Emerging Technology.

Letzing, J. (2021, April). *How to tell reality from a deepfake?* . Retrieved from World Economic Forum: https://www.weforum.org/agenda/2021/04/are-we-at-a-tipping-point-on-the-use-of-deepfakes/

Morrow, E. (2021, September). *Beyond Disinformation: Deep Fakes and False Memory Implantation*. Retrieved from Dana Foundation: https://dana.org/article/neuroethics-essay-general-audience-2021/

Hughes, S. (2021, October). *Deepfakes Can Be Used to Hack the Human Mind*. Retrieved from Psychology Today: https://www.psychologytoday.com/intl/blog/spontaneous-thoughts/202110/deepfakes-can-be-used-hack-the-human-mind

Ahmed, S. (2021). Navigating the maze: Deepfakes, cognitive ability, and social media news skepticism. *New Media & Society*, 1-22.

Bateman, J., Hickok, E., Courchesne, L., Thange, I., & Shapiro, J. (2021). *Measuring the Effects of Influence Operations: Key Findings and Gaps From Empirical Research.* Carnegie Endowment for International Peace.

Facebook. (2021, May). *Threat Report -The State of Influence Operations 2017-2020* . Retrieved from Facebook: https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf

Xu, M., & Lu, C. (2021). China–U.S. cyber-crisis management . *China Int Strategy Rev*, 97-114.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 8176-8186.

Bada, M., & Nurse, J. (2020). The social and psychological impact of cyberattacks. *Emerging Cyber Threats and Cognitive Vulnerabilities*, 73-92.

Gomez, M. A., & Shandler, R. (2022, September). *Cyber Conflict and the Erosion of Trust*. Retrieved from Council for Foreign Relations: https://www.cfr.org/blog/cyber-conflict-and-erosion-trust

Schneider, J. (2022, January). A World Without Trust. *Foreign Affairs*. Retrieved from Foreign Affairs.

Crowdstrike. (2023, February). *Types of Malware*. Retrieved from Crowdstrike: https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/

Fortinet. (n.d.). *Types of Cyber Attacks*. Retrieved from Fortinet: https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks

Fruhlinger, J. (2022, August). *WannaCry explained: A perfect ransomware storm*. Retrieved from CSO Onlinre: https://www.csoonline.com/article/3227906/wannacry-explained-a-perfect-ransomware-storm.html

The State Council Information Office of the People's Republic of China. (2019, July). *2019 White Paper titled 'China's National Defence in the New Era'* . Retrieved from Xinhua: https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html

Cluzel, F. d. (2020). *Cognitive Warfare, a Battle for the Brain.* Retrieved from NATO: https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-HFM-334/$MP-HFM-334-KN3.pdf

Longxi, Y. (2022, August). *Aiming at future wars and fighting the "five battles".* Retrieved from China Military Network - Jiefangjun Daily: http://www.81.cn/ll_208543/10179953.html

Hung, T.-C., & Hung, T.-W. (2022). How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars. *Journal of Global Security Studies,, 7*(4).

Singh, A. (2013). China's 'Three Warfares' and India. *Journal of Defence Studies, 7*(4), 27-46. Retrieved from IDSA: https://idsa.in/system/files/jds_7_4_AbhijitSingh.pdf#:~:text=As%20is%20now%20well%20known%2C%20the%20Chinese%20regime%E2%80%99s,the%20components%20of%20a%20nation%E2%80%99s%20comprehensive%20national%20power.

Charon, P., & Jeangène Vilmer, J.-B. (2021). *Chinese Influence Operqtions - A Machiavellian Moment.* Institut de Recherche Stratégique de l'Ecole Militaire.

Law and Society Alliance . (2021). *Mapping Chinese Footprints and Influence Operation in India.* New Delhi: Law and Society Alliance .

Balding, C., Sinha, A., & Wu, J. (2022). *Chinese Military Civil Fusion Firms: The Case of Speech Ocean Improving Activity Obfuscation, Pursuing State Interests, Engaging in Third Country Data Gathering.* New Kite Data Labs .

Freedom House. (2023). *Beijing's Global Media Influence 2022*. Retrieved from Freedom House: https://freedomhouse.org/report/beijing-global-media-influence/2022/authoritarian-expansion-power-democratic-resilience

Graphika. (2023). *Deepfake It Till You Make It - Pro-Chinese Actors Promote AI-Generated Video Footage of Fictitious People in Online Influence Operation.* Graphika. Retrieved from https://public-assets.graphika.com/reports/graphika-report-deepfake-it-till-you-make-it.pdf

Kaushik, M. (2020, June). *200% rise in cyberattacks from China in a month; India tops hit list post Galwan face-off*. Retrieved from Business Today: https://www.businesstoday.in/technology/news/story/200-percent-rise-in-cyberattacks-from-china-in-a-month-india-tops-hit-list-post-galwan-face-off-262195-2020-06-24

Alspach, K. (2022, August). *Russian hackers get the headlines. But China is the bigger threat to many US enterprises.* Retrieved from Protocol: https://www.protocol.com/enterprise/china-hacking-ip-russia-cybersecurity

Bhargava, K. (2022, December). *Recent Cyber Attacks With Alleged Chinese Involvement That Targeted India's Critical Infrastructure*. Retrieved from Outlook: https://www.outlookindia.com/national/recent-cyber-attacks-with-alleged-chinese-involvement-that-targeted-india-s-critical-infrastructure-news-241897

DoubleThink Lab & China in the World. (2023). *China Index 2022*. Retrieved from China Index: https://china-index.io/

Ronzaud, L., Hubert, I., Eib, S., Chandra, A., Stubbs, J., Ruan, L., & Carter, J. (2021). *Lights, Camera, Coordinated Action!* Graphika.

Bozkurt, A. (2022, October). *Turkey helped Pakistan set up a secret cyber army for influence operation against US, India*. Retrieved from Nordic Monitor: https://nordicmonitor.com/2022/10/turkey-helped-pakistan-set-up-a-secret-cyber-army-for-influence-operation-against-us-india/

RIEAS. (2021, February). *Turkey-Pakistan: Secret Army of Mercenary Journalists.* Retrieved from Research Institute for European and American Studies: https://www.rieas.gr/images/editorial/medasiajournalist21.pdf

European Parliament. (2021, January). *Turkish funding for anti-India extremism*. Retrieved from European Parliament: https://www.europarl.europa.eu/doceo/document/E-9-2021-000549_EN.html

Bhatt, S. (2022, June). *Pakistani propaganda on Kashmir has a new launchpad — Erdogan's Turkey*. Retrieved from The Print: https://theprint.in/opinion/pakistani-propaganda-on-kashmir-has-a-new-launchpad-erdogans-turkey/1003485/

Philip, S. A. (2020, March). *Gen Naravane's Chanakya neeti for future wars will require India to spend money smartly*. Retrieved from The Print: https://theprint.in/opinion/brahmastra/gen-naravanes-chanakya-neeti-for-future-wars-will-require-india-to-spend-money-judiciously/376449/

The Global Statistics. (2023). *India Social Media Statistics 2023 | Most Used Top Platforms*. Retrieved from The Global Statistics: https://www.theglobalstatistics.com/india-social-media-statistics/

LiveMint. (2022, June). *Despite Misinformation Concern 54% Indians derive factual information from social media, revals OUP study*. Retrieved from LiveMint: https://www.livemint.com/news/india/despite-misinformation-concern-54-indians-derive-factual-information-from-social-media-reveals-oup-study-11656420664780.html

Shivji, S. (2021, December). *Facebook has a massive disinformation problem in India. This student learned firsthand how damaging it can be*. Retrieved from CBC: https://www.cbc.ca/news/world/india-facebook-disinformation-1.6276857

RAND. (n.d.). *Psyhological Warfare*. Retrieved from RAND Corpoeration: https://www.rand.org/topics/psychological-warfare.html

Brangetto, P., & Veenendaal, M. (2016). Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. *2016 8th International Conference on Cyber Conflict Cyber Power.* Tallin: NATO CCD COE Publications.

Cloudflare. (n.d.). *What is a DDoS attack?* Retrieved from Cloudflare: https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/

Gatlan, S. (2022, November). *FBI: Hacktivist DDoS attacks had minor impact on critical orgs*. Retrieved from Bleeping Computer: https://www.bleepingcomputer.com/news/security/fbi-hacktivist-ddos-attacks-had-minor-impact-on-critical-orgs/

The Engine Room. (June, 2020). *Case study: Distributed Denial of Service attacks (DDoS).* Retrieved from The Engine Room: https://www.theengineroom.org/wp-content/uploads/2020/08/OrgSec-Case-study-DDoS-attacks-June-2020.pdf

Stella, M., Ferrara, E., & Domenico, M. (2018, November). *Bots increase exposure to negative and inflammatory content in online social systems*. Retrieved from PNAS: https://www.pnas.org/doi/10.1073/pnas.1803470115

Veracode. (n.d.). *What is Spyware?* Retrieved from Veracode: https://www.veracode.com/security/spyware#:~:text=Spyware%20is%20any%20software%20that,this%20data%20to%20other%20parties.

Fong, M. (2022, August). *Recognizing And Preventing The Psychological Toll Of Spyware*. Retrieved from Forbes: https://www.forbes.com/sites/forbestechcouncil/2022/08/12/recognizing-and-preventing-the-psychological-toll-of-spyware/?sh=29c253127fb0

Help Net Security. (2022, October). *The long-term psychological effects of ransomware attacks*. Retrieved from Help Net Security : https://www.helpnetsecurity.com/2022/10/25/psychological-effects-ransomware/

Sheldon, R., & Hanna Katie. (2022, January). *Cyberterrorism*. Retrieved from Tech Target Security: https://www.techtarget.com/searchsecurity/definition/cyberterrorism

Maryville University. (2022). *Cyber Terrorism: What It Is and How It's Evolved*. Retrieved from Maryville University: https://online.maryville.edu/blog/cyber-terrorism/

Guynn, J. (2020, February). *Anxiety, depression and PTSD: The hidden epidemic of data breaches and cyber crimes*. Retrieved from USA Today: https://www.usatoday.com/story/tech/conferences/2020/02/21/data-breach-tips-mental-health-toll-depression-anxiety/4763823002/

Jinghua, L. (2019, April). *What Are China's Cyber Capabilities and Intentions?* Retrieved from Carnegie Endowment for International Peace: https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734

Murphy, D., & Kuehl, D. (2015, September). The Case for a National Information Strategy. *Military Review*.

Zhiwei, Z. (2022, August). *Cognitive domain operations under intelligent visual threshold: Emotional conflict has become a prominent attribute of cognitive domain operations*. Retrieved from China Military Network - Jiefangjun Daily: http://www.81.cn/yw_208727/10204158.html

Cunshe, Y. (2022, August). *Put the pulse of quasi-cognitive domain combat*. Retrieved from Jiefangjun: http://www.81.cn/jfjbmap/content/2022-08/16/content_322064.htm

Hillman, J. (2021, December). *Pakistan's cautionary tale of digital dependence on China*. Retrieved from Nikkei Asia: https://asia.nikkei.com/Opinion/Pakistan-s-cautionary-tale-of-digital-dependence-on-China

Malhotra, D. (2020). Inter-Services Public Relations (ISPR) Assessment of the Pakistan Military's Discreet Propaganda Factory Post-1990. *Journal of Defence Studies,, 14*(4), 37-57.

Haque, I., & Meo, S. (2020, September). *Why a Turkish historical drama has become wildly popular with India's Muslim youth*. Retrieved from Scroll: https://scroll.in/article/973620/why-a-turkish-historical-drama-has-become-wildly-popular-with-indias-embattled-muslim-youth

Subramanian, N. (2021, July). *'Diriliş: Ertuğrul' is more than just a Turkish delight*. Retrieved from The Hindu: https://www.thehindu.com/opinion/op-ed/dirili-erturul-is-more-than-just-a-turkish-delight/article35549826.ece

PTI. (2016 August). *Turkey backs Pakistan's stance of sending an OIC team to Kashmir*. Retrieved from Business Standard: https://www.business-standard.com/article/current-affairs/turkey-backs-pakistan-s-stance-of-sending-an-oic-team-to-kashmir-116080200837_1.html

Quamar, M. (2021, July). *The geopolitics of OIC activism on Kashmir*. Retrieved from Financial Express: https://www.financialexpress.com/business/defence-the-geopolitics-of-oic-activism-on-kashmir-2288676/

Times of India. (2021, September). *Supreme Court expresses grave concern over fake news on social media and YouTube*. Retrieved from Times of India:

https://timesofindia.indiatimes.com/india/supreme-court-expresses-grave-concern-over-web-portals-spreading-fake-news/articleshow/85858300.cms

Sengupta, A. (2022, December). *Govt blocks 104 YouTube channels, several social media accounts for threatening national security*. Retrieved from India Today: https://www.indiatoday.in/technology/news/story/govt-blocks-104-youtube-channels-social-media-accounts-threatening-national-security-fake-news-2312595-2022-12-23

Indian Express. (2023, April). *Google fights back against misinformation in India, as fake news reaches all-time high*. Retrieved from Indian Express: https://indianexpress.com/article/technology/tech-news-technology/google-ups-the-ante-against-fake-news-8532164/

Cabinet Secretariat. (2022, December). *National Security Strategy of Japan.* Retrieved from Cabinet Secretariat of Japan: https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf

Ministry of Defence Japan. (2022, December). *National Defence Strategy.* Retrieved from Ministry of Defence of Japan: https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy_en.pdf

Nishikawa, T. (2023). *The Mind Is a Battlefield: Lessons from Japan's Security Policy on Cognitive Warfare .* Retrieved from 49 Security: https://fourninesecurity.de/2023/02/22/the-mind-is-a-battlefield-lessons-from-japans-security-policy-on-cognitive-warfare

ET Telecom. (2023, February). *National Cybersecurity Strategy 2023 may come out soon: Pant.* Retrieved from Economic Times: https://telecom.economictimes.indiatimes.com/news/national-cybersecurity-strategy-2023-may-come-out-soon-pant/98093316

Gandhi, P. (2020, August). *Western Media Bias against India.* Retrieved from Vivekananda International Foundation: https://www.vifindia.org/article/2020/august/15/western-media-bias-against-india%20

Mazumdar, A. (2019). U.S. national interests and framing India in the U.S. press during and after Cold War. *The Journal of International Communication, 26*(1), 92-108.

PTI. (2022, September). *Jaishankar takes a dig at American media for 'biased' India coverage*. Retrieved from The Hindu: https://www.thehindu.com/news/national/indias-voice-counts-in-world-because-of-pm-modi-says-eam-jaishankar-in-washington/article65936672.ece

ANI. (2022, September). *Western media distorts India's global image by farcical coverage*. Retrieved from ANI: https://www.aninews.in/news/world/asia/western-media-distorts-indias-global-image-by-farcical-coverage20220929204453/

MFA China. (2015, December). *Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference*. Retrieved from MFA China:https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html

Doshi, R., Bruyere, E., Picarsic, N., & Ferguson, J. (2021, April). *China as a 'cyber great power': Beijing's two voices in telecommunications*. Retrieved from Brookings: https://www.brookings.edu/research/china-as-a-cyber-great-power-beijings-two-voices-in-telecommunications/

Babb, C. (2023, February). *For Xi Jinping, Cyber Is Personal* . Retrieved from National Interest: https://nationalinterest.org/feature/xi-jinping-cyber-personal-206214

Allen, G. (2019, February). *Understanding China's AI Strategy* . Retrieved from CNAS: https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy

Li, D., Tong, T., & Xiao, Y. (2021, February). *Is China Emerging as the Global Leader in AI?* Retrieved from Harvard Business Review: https://hbr.org/2021/02/is-china-emerging-as-the-global-leader-in-ai

Pal, D. (2021, October). *China's Influence in South Asia: Vulnerabilities and Resilience in Four Countries* . Retrieved from Carnegie Endowment for International Peace: https://carnegieendowment.org/2021/10/13/china-s-influence-in-south-asia-vulnerabilities-and-resilience-in-four-countries-pub-85552

Cookson, F., & Joehnk, T. F. (2018, April). *China and India's geopolitical tug of war for Bangladesh*. Retrieved from East Asia Forum: https://www.eastasiaforum.org/2018/04/11/china-and-indias-geopolitical-tug-of-war-for-bangladesh/

ANI. (2023, April). *Indian Army raising new units to counter China, Pak in cyber warfare: Report*. Retrieved from Hindustan Times: https://www.hindustantimes.com/india-news/indian-army-raising-new-units-to-counter-china-pakistan-in-cyber-warfare-reports-101682581848934.html

Singh, S. (2023, July 5). *The Battle Beyond The Frontlines: Social Media Driven Information Warfare In The India-Pakistan Context*. Retrieved from CENJOWS: https://cenjows.in/the-battle-beyond-the-frontlines-social-media-driven-information-warfare-in-the-india-pakistan-context/

Ritchie, H., Edouard, M., Roser, M., & Ortiz-Ospina, E. (2023). *Internet*. Retrieved from Our World in Data: https://ourworldindata.org/internet

Kaspersky. (2023). *What is WannaCry ransomware?* Retrieved from Kaspersky: https://www.kaspersky.co.in/resource-center/threats/ransomware-wannacry

About the author

Divyanshu Jindal is a Research Associate at NatStrat, India and a Non-Resident Scholar at the Middle East Institute, Washington DC. He completed his Master's in Diplomacy, Law and Business from OPJGU, India and B.Tech in Computer science from SRM University, India. Before venturing into research, he was associated with Fidelity Investments as a Systems engineer. His research revolves around the Geopolitics of Cyber, and his writings have appeared for various international and national platforms like the Lowy Institute, the National Interest, Taipei Times, ISDP Sweden, Vivekananda International Foundation, and Hindustan Times among others.

Printed & published by:
India Foundation, New Delhi
mail@indiafoundation.in
(For private circulation only)