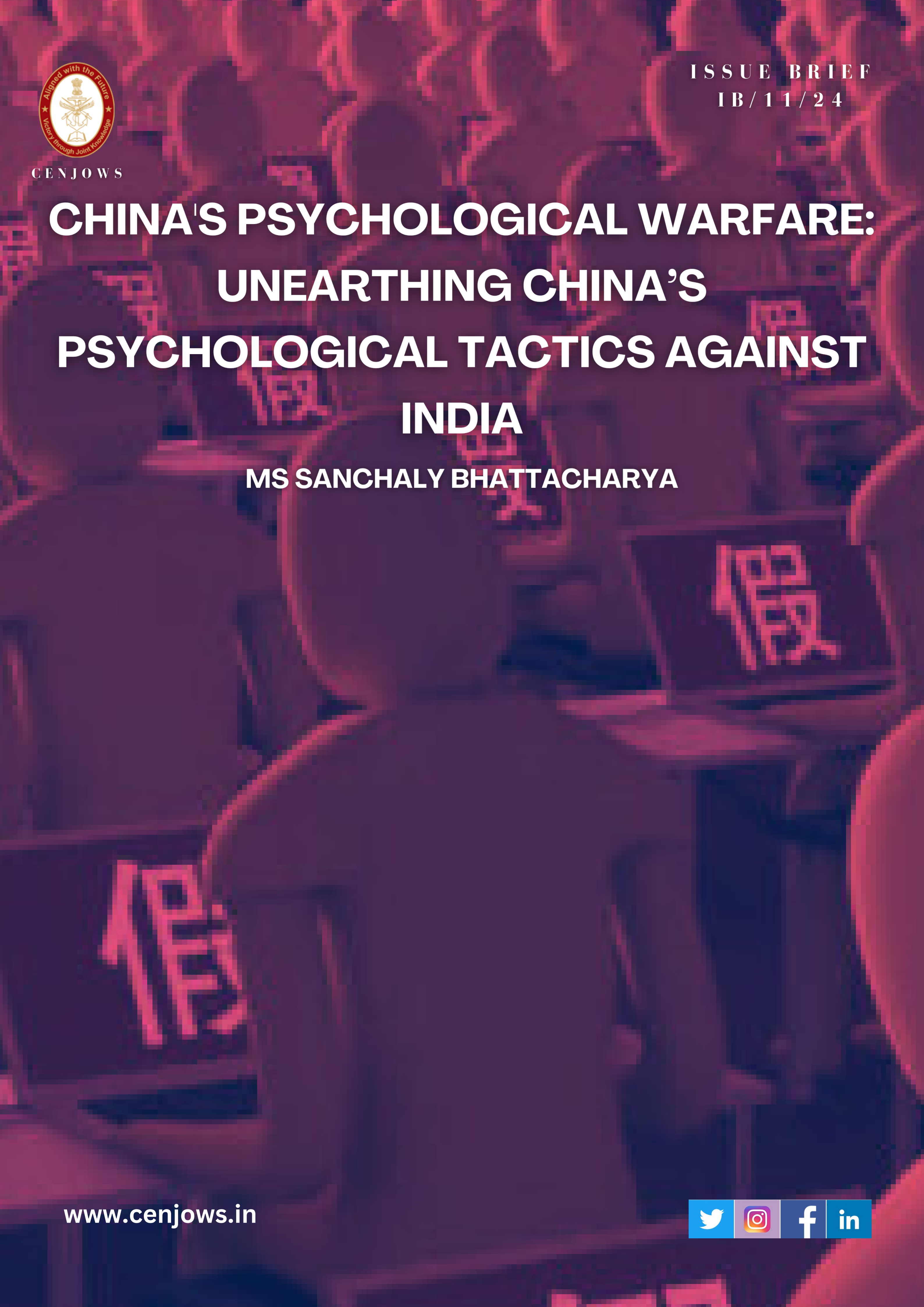

CENJOWS

ISSUE BRIEF
IB/11/24

CHINA'S PSYCHOLOGICAL WARFARE: UNEARTHING CHINA’S PSYCHOLOGICAL TACTICS AGAINST INDIA

MS SANCHALY BHATTACHARYA

www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

Aligned with the Future

Victory through Joint Knowledge

CENJOWS

CHINA'S PSYCHOLOGICAL WARFARE: UNEARTHING CHINA'S PSYCHOLOGICAL TACTICS AGAINST INDIA

Ms Sanchaly Bhattacharya, is a Research Intern at CENJOWS, New Delhi.

Abstract

The article will focus on 'Psychological Warfare', with a special emphasis on China's repeated utilization of 'information' in its 'unrestricted warfare' strategy. As a crucial part of Psy-Ops, the article will assess how much the 'informationalization' has influenced public opinion and leveraged China's interest over its adversary, especially India. With a special focus on India as a case study of China's information warfare, the article will bring a few key instances to understand how China uses its so-called information network to manipulate the facts and attempt to build narratives against India's position in the international community.

Introduction

The character of warfare has changed worldwide. The technological advancement, on one hand, brought ease to millions of lives, while, on the other, it led to the growing fantasy for 'hybrid warfare'. Hybrid warfare is combining conventional warfare through military forces and a tech battlefield, continuously supporting or undermining the ground actions to seek international support. The ongoing Russia-Ukraine is a notable example of employing ‘hybrid warfare’. China is also not far behind in attaining its national interest through employing the strategies of hybrid warfare. Although this is a recently added strategy in China’s military domain, the progress of China’s ‘three warfare strategy (3W)’ or ‘San Zhong Zhanfa’ is considerably significant. The 3W strategy of China is- Psychological Warfare, Public Opinion Warfare, and Legal Warfare.

The 3Ws are interconnected but each domain has its typical operational areas and peculiar target outcomes. Psychological Warfare or Psy-Ops aims either to influence mass opinion by weaponizing information penetration or seek to degrade the adversary’s confidence. Information warfare, in the high-tech battlefield, is a recent focus area of non-conventional warfare, which is one of the key aspects of China’s ‘unrestricted warfare’. Information Warfare is an integral part of China’s military strategy, commonly called as ‘Integrated Network Electronic Warfare’. [1]

Apparently, China is not involved in any direct conflict with its perceived adversary India after the Galwan Valley clashes. Several rounds of negotiations are currently ongoing to de-escalate the situation. However, as American analysts say information warfare is the ‘Offensive Peacetime Operations’ to attack repeatedly on the adversary without having any real operational costs.

Evolution of Information Warfare as a Tool of Psychological Warfare Strategy of China

There is very little known about the origin of the 3Ws; but in the ancient text of Sun Tzu, “The Art of War”, there is a great emphasis on the strategy of ‘winning without engaging in a real war’. There is a concept of “zhixinxiquan” (制信息权), which means the ‘right to intellectual information is probably the basic ground of China’s ideological focus on ‘information superiority’. From the utilitarian perspective, the 3Ws are helpful as a weapon for offense even in the peaceful phase. As discussed before, though there is an interconnectedness among the three warfare strategies, employing them in the appropriate context is also crucial to be successful. Information warfare as a tool for breaking down the enemy’s psychology is important to crash the self-esteem of the enemy without directly engaging in the battlefield. Information warfare, in the information age, is a part and parcel of ‘*grey zone warfare*’, where there is neither any boundary nor any rule to spread false information.

Peng Guangqian and Yao Youzhi in their seminal texts “Science of Strategy” (2001) and “The Science of Military Strategy” (2005) respectively argue that information superiority has not only become a prerequisite of supremacy in every battlefield but the priority of decoding the modern nature of conflicts. Against the backdrop of the Russian invasion of Ukraine, there is a floating of information on China’s social media platform, Weibo, supporting the Russian claim that developing biological weapons in Ukraine is the reason that the Kremlin attempts to protect Kyiv.

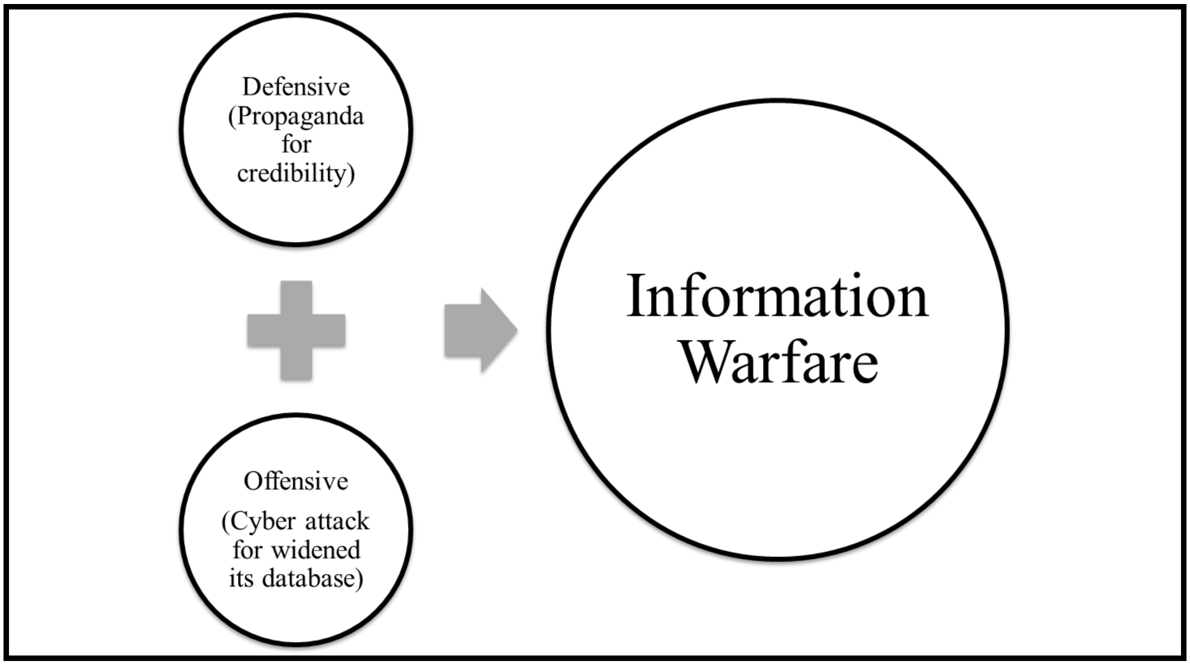
Defensive (Propaganda for credibility)
Offensive (Cyber attack for widened its database)
Information Warfare

Figure 1: Two aspects of China’s information warfare

(Source: Compiled by the author)

There are two type of information warfare (IW), offensive and defensive, as shown in Figure 1. Countries utilised the defensive nature of IW for narrative-building purpose to seek credibility. Apart from the defensive nature of information warfare, China also operates in the offensive front through cyberattacks on its perceived hostile foreign countries’ government agencies to get more information about them. This offensive approach has two purposes: first is to extract all the information, eventually will be beneficial for China’s core national interest and second is to diminish opponents’ capability to protect their crucial information. That is how the ‘information’ is increasingly becoming the decisive factor in fighting modern warfare without really going into a full-scale war. As reported by a US-based cyber intelligence firm, a Chinese hacking group I-Soon, a cyber contractor of China’s Ministry of Public Security (MPS), claimed to have targeted key offices of the Indian government, including Prime Minister’s Office (PMO), Reliance Industries, and Air India enterprises. Insikt group, the threat research division of Massachusetts-based Recorded Future has revealed in one of its reports that the Chinese hackers are increasingly targeting the power sector of India[2].

Information warfare is not a new thing in military strategy. There are several instances during the two world wars, where armies manipulated battlefield information to break down opponents' self-confidence. However, the current focus on information is exploiting the virtual network to get the information required and using it as a tool of modern-day conflict. Eventually, the Chinese Communist Party (CCP) also started to realize that building central control over the information network has been becoming more important[3]. In 2015, a white paper of China mentioned that "the form of war is accelerating its evolution of informatization", and highlighted that China aims to build a national defence mobilization system by having centralized control over the whole information network of China worldwide[4]. There is a clear change in '*Preparation of Military Struggle*' (PMS), which is a basic practice to maintain peace by containing the possibility of wars. The evolved strategy of PMS is from winning local wars under conditions of modern technology since 1993 to winning local wars under conditions of informationisation from 2004 and finally, since 2015 winning informationised local wars[5].

Structure and Composition of China's Information Network

From the Chinese perspective, combat operations in the high-tech battlefield, in which both sides utilize information technology to obtain dominance over their rival party. In this environment, the combat aimed at seizing the actual battlefield initiative with digitalized ground combat force and using the information as its main substance or key weapon i.e., 'smart weapon' to derogate the opponent's self-esteem. This is the main foundation principle of China's 'stratagems' to build and maintain information superiority. Cyberspace operations are mostly used to achieve information dominance through reconnaissance and espionage, conducting network incursions in the virtual battlefield, and possibly stealing or sometimes altering the available information. This is understandable from China's practice of 3Ws by using strategic psychological operations, overt and covert media manipulation, and carrying out legal warfare. Achieving information superiority shall provide CCP gaining mastery by striking first over its rivals.

China's information network has some known dimensions in its domestic as well as in gathering foreign data. CCP maintains a countrywide network of government data surveillance tools, colloquially called "Public Opinion Analysis Software", that was developed over the past few years and are being extensively used to assess the officials' and citizens' loyalty towards CCP's rule[6]. The surveillance system warns the officials to refrain from sharing politically sensitive information online. This helps the CCP to push the narrative that favours its governance style worldwide. In times of Covid-19, China attempted to 'market' its governance style by degrading 'democracy', especially in the context of India's incapability of preventing deaths[7].

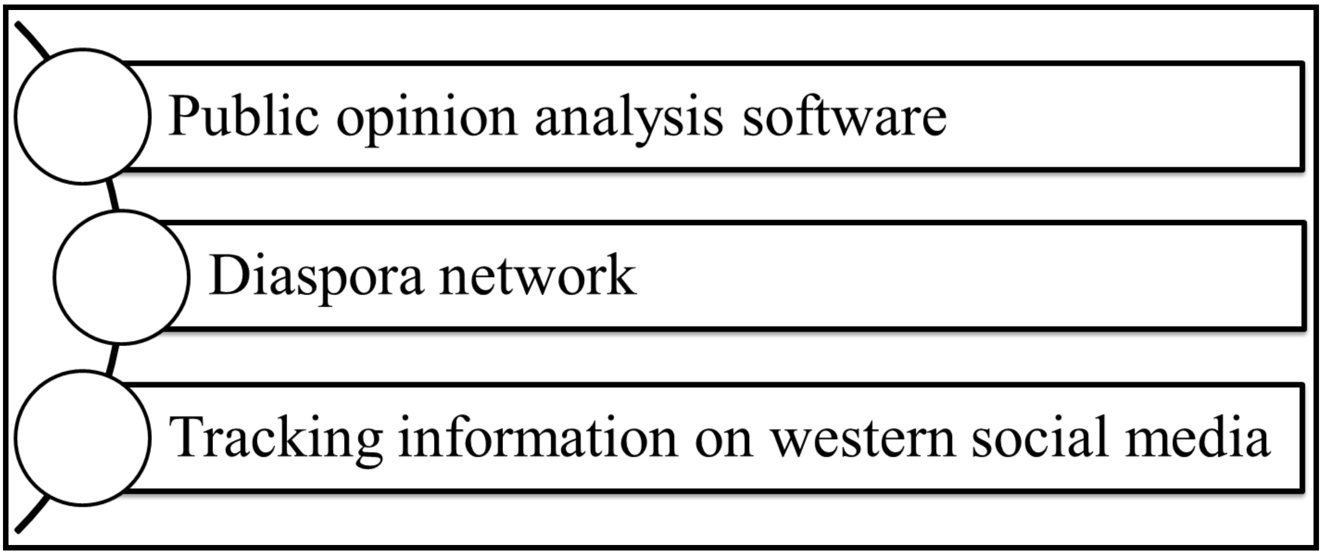
Public opinion analysis software
Diaspora network
Tracking information on western social media

Figure 2: China's information network

(Source: Compiled by the author)

In Figure 2, the three prominent methods of China's informationalisation has been portrayed. Since 2020, this same software has been used to collect data on foreign targets from 'Western' social media like Facebook, Twitter, and so on. As reported by the Washington Post, the post review of the bidding documents and the terms of the contracts for over 300 Chinese government projects show that agencies including state media, propaganda departments, police, military, and cyber agencies of CCP are engaged in purchasing more sophisticated tools to gather more foreign data. The same report highlighted that an amount of $320,000 Chinese state media software program to create a database of foreign journalists and academics; an investment of Beijing's police intelligence system to foreign social media sites on the issue of Hong Kong and Taiwan and a cyber-centre dedicated only to Xinjiang province, home of the most Chinese Uyghur Muslims, the minority group and controversies over the human rights issue from the West in the same province[8].

This system is under China's institutional architecture of information networks. However, there is another wing of CCP's information operations, for which evidence is either limited or not fully proven yet. China gathers intelligence data through its widespread diaspora abroad. The scandal of Gladys Liu is a notable example of China's diaspora intelligence network. In 2019, Gladys Liu from the Victorian seat of Chisholm became the first female Chinese Australian elected to sit in the lower house of the Australian parliament. Eventually, it was revealed that Liu was previously associated with the United Front Work Department of the CCP. Although Liu has denied this claim and even PM Scott Morrison also has strongly backed Liu, this heated a relevant question of covert influence operations and foreign interference activities to gather intelligence data by the Chinese operatives[9]. The United Front Work Department, which is resourced by vast finance and operations was called 'magical weapons' by President Xi Jinping in 2014. Apparently, the objective of this department is to cooperate with overseas Chinese individuals and organizations, but it has an implicit function of operating and coordinating overseas influence operations[10].

Understanding the structure of China's information network domestically is key to assessing its operative capabilities. China's information network operates at three different levels with its peculiar roles and responsibilities. The upper hand is on the Joint Staff Department's Information and Communications Bureau, which takes responsibility for high-level control and command. In the next stage, the Strategic Support Force (SSF), which is an integral part of the People's Liberation Army (PLA), inevitably plays the crucial role of implementing strategic information operations and providing the support system. Then comes the Equipment Development Department, which is responsible for providing the research support. The PLA SSF is the most crucial wing of the entire network[11].

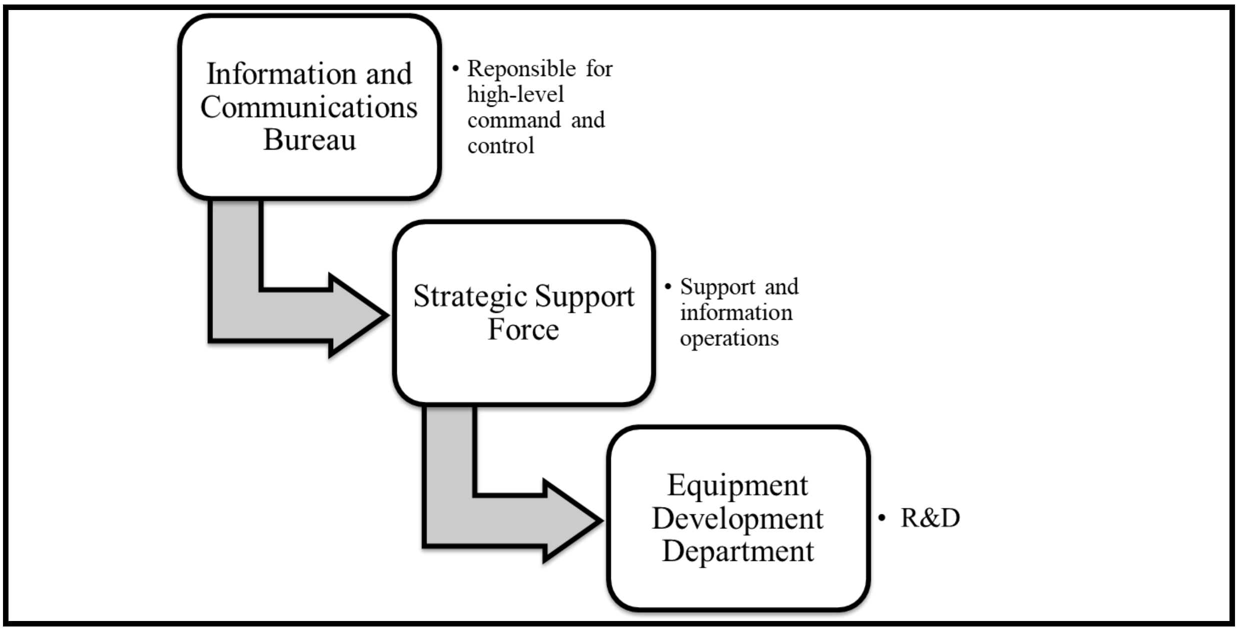
Information and Communications Bureau
• Reponsible for high-level command and control
Strategic Support Force
• Support and information operations
Equipment Development Department
• R&D

Figure 3: Structure of China's centralization information network

(Source: compiled by the author)

Figure 3 demonstrates hierarchical department structure of Chinese agencies involved in managing the information. In 2015, the PLA created SSF to centralize space, cyber, electronic warfare, and psychological warfare under a single agency. The role of SSF, on the one hand, centralising collected information, and its management, provides useful information to theatre commands, and on the other hand, helps to enable PLA's power projections, and supports strategic decision-making by holistic considerations of the operations.

The Network Systems Department, one of the two deputy theatre command-level departments within the SSF is responsible for strategic information operations. As the report mentioned this is the specific department that has the niche to supervise all sorts of information warfare. In achieving success in information warfare, the PLA SSF, as mentioned by President Xi Jinping, is a 'new type of combat force' for increasing the PLA's operational capability to match the need for modern-day warfare[12].

Examining Incidents of Disinformation Campaigns against India

Misinformation in Doklam Standoff and Galwan Valley clash

On July 17, 2017, there was a report by the Chinese state-run media China Central Television or CGTV, that the PLA conducted a live drill exercise in the Tibet region. The same news was reported by the CCP's mouthpiece Global Times on the same day[13]. This was against the backdrop of Sino-Bhutan's Doklam Plateau conflict, where India intervened to protect Sikkim from further possible Chinese incursion. On July 19, 2017, New Delhi denied the claim of troop mobilization in Tibet or towards the boundary of the Line of Actual Control (LAC). Analysts opined that the Chinese put pressure by spreading false information about the PLA's mobilization so that the Indian military would withdraw from the Doklam standoff[14]. Suddenly, Indian media outlets have started to forecast the same rhetoric. Indian media started to telecast the snapshots of the 1962 Sino-India war, which erupted in anti-government sentiment.

On August 4, 2017, Global Times, a Chinese state-media agency tweeted a image, where they portray that the Indian troops have crossed the border with its military vehicle[15]. This can be considered as the visualization of China's disinformation campaign against India. Apart from this, one of the maps of the triangular junction of India-Bhutan-China shows the same thing that Indian troops entered the Chinese territory along with showing Doka La or Doklam plateau as their own territory[16].

Regarding the Doklam valley clashes, Chinese media Xinhua agency floated that India '*illegally*' trespassed into Chinese territory and Chinese broader troops, who attempt to convince Indian troops to maintain the status-quo of the region[1718]. The same news agency has posted a propaganda video on its official YouTube channel, titled "*Seven Sins of India*", in which they claim that Bhutan recognized the Doklam plateau as Chinese territory.

While this video by Chinese state media Xinhua stated that Doklam is recognized as an undisputed Chinese territory by India, Bhutan, and the international community, the Bhutan government in its press release highlighted the following key points:

a) Doklam is Bhutanese territory
b) Constructing the road in Bhutan's territory by Chinese is a direct violation of international laws[19]

Therefore, China's repeated attempt to portray India as an illegal intruder and put pressure on New Delhi to withdraw is a classic example of China's information warfare using its media outlets and different social media platforms.

India's G20 Presidency

While the whole world praised India for showcasing its leadership during the G20 presidency, CCP's mouthpiece Global Times have published an article titled India's G20 Presidency and its dream of becoming a great power just a 'Delusion'. The same article quotes the G20 Delhi Declaration as just an eye-wash to avoid the embarrassment of a fruitless summit[20]. The article also brings the context of India's abstention from voting in the United Nations against the backdrop of the Russia-Ukraine war as a strategy to please the 'West'[21].

On April 2023, the Chinese Foreign Ministry spokesperson Mao Ning confirmed that neither President Xi Jinping nor Foreign Minister Wang Yi would be coming to the upcoming G20 meeting held in India. In Y20, the Chinese did not send their delegation, saying that the visa issued showed one Chinese territory as India's. China also questioned the theme of the event as Sanskrit is not a UN language. Chinese official sources have stated that India does not use the term 'war' in Ukraine, which implies that India's unconditional support to Russia and Beijing appreciated this step by saying a good move against the continuous rhetoric of the West[22]. However, the document of Chinese foreign ministers did use the term 'war' in Ukraine several times. China pushed narratives such as 'India is too poor to host the G20 and has failed miserably; Modi faces a tough challenge at the G20; and Indian diplomacy failed because it could not persuade Xi Jinping and Vladimir Putin to attend the summit.

Disinformation Campaign During COVID-19

During the COVID-19 pandemic, China was massively accused of involving itself in the disinformation campaign against India from various fronts. While there are a couple of claims that the virus originated in China, Beijing crafted a different narrative to reshape the perceptions of its pandemic response and the efficiency of its governance model. As a natural influence in the region, the CCP advocates its way of dealing with the crisis by portraying India's democracy as a failed model for tackling the crises. CCP's mouthpiece Global Times was actively involved in spreading false information to belittle India's vaccine efforts to fight the pandemic[23][24]. Following the Galwan Valley clash and India's ban on 54 Chinese applications and consequently the changing regulations for India's FDI towards Chinese companies, several cyberattacks have been witnessed by New Delhi. The IT ministry has attributed it to 'Stone Panda', a Chinese threat actor group, linked to the Chinese Ministry of State Security (MSS)[25].

On August 26, 2021, Global Times tweeted India and the other anti-China forces, which is understandably indicative of the 'West', are the source of the 'rumours' that COVID-19 originated from the Wuhan Laboratory of China[26]. This has been come against the backdrop of collective a request by the countries to World Health Organization (WHO) to conduct an independent investigation of the source of the COVID-19 virus. Another classic example of China's information warfare is to spreading a derogatory image of situation comparison between India and China on its social media platform, Weibo.

In Weibo, one image was posted showing China's development in the space industry through a rocket launch, on one side and on the other, the bodies of Covid victims being cremated in India. This image sent a clear signal of China's disinformation to undermine India's capability to tackle the pandemic. One image has been put up with the text in the Mandarin language: "Lighting a fire in China vs lighting a fire in India". It was reportedly published by the leaked account of CCP. This has sparked massive criticism across the world[27].

Misinformation Through Other Means

There is an increasing attempt from Beijing to manipulate the original information by releasing controversial maps and claiming other countries' territory. India-China has a historical territorial dispute. As a reference point, China often claims based on its imperial history and stated that the Indo-China boundary has been largely drawn under the Shimla Agreement was finalized by British India, which is not legitimate in independent India. However, 'Cartographic Aggression' has nowadays become a norm for China to weaken New Delhi's stance on it. Map visualization is an effective tool to undermine India's capability to protect its sovereign border[28].

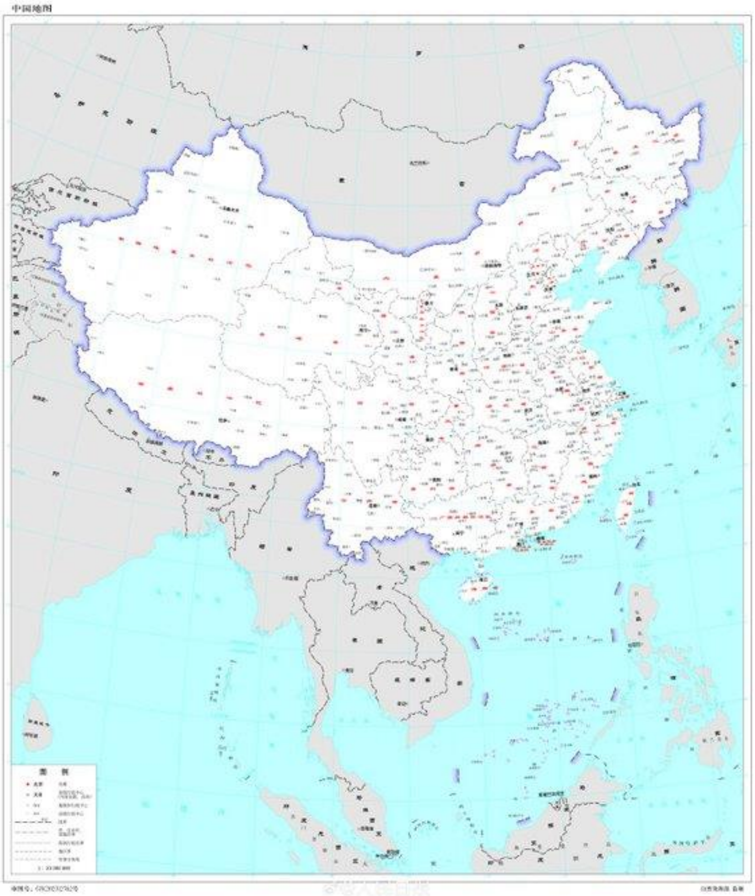

Figure 4: China's official 2023 Map[29]

The controversial 2023 map released by China's Ministry of Natural Resources, shown in Figure 4, incorporates the Indian state of Arunachal Pradesh and disputed territory of Eastern Ladakh region. This official map arguably caused a series of controversies and criticisms from the Indian side. Apart from the cartographic incursion, there is another mechanism of China to manipulate the facts, and information, that is naming of Indian territories. This year, the Chinese Aviation Ministry renamed 30 places in Arunachal Pradesh, the undisputed Indian state, which China claims based on its imperial history.

This is the fourth time that China officially renamed the places of Indian territories[30]. Indian External Affairs Minister (EAM) S. Jaishankar opined that “renaming places does not mean that the territory will be theirs”. However, scholars have stated grave concern about China’s increasing assertiveness about Indian territory[31].

Recommendations

1. *National Cyber Security Strategy:*

Since 2013, India has had a National Cybersecurity policy as a comprehensive policy document that has key components like the development of legal provisions, implementing training of the cybersecurity workforce, fostering collaboration between public and private enterprises, establishing mechanisms for on-time detection, reporting, and response to the potential cyber threats[32]. As a national-level agency, the Computer Emergency Response Team (CERT-In) has been established[33]. To supervise the implementation, the National Cyber Security Coordinator (NCSC) has been also established. However, India does not have a proper roadmap or strategy to tackle cyber threats. Disinformation is not only spreading false information but through using bots and AI, furthering the narratives to harm the self-component of the opponents. Hence, India needs a National Cyber Security Strategy, which was conceptualized by the Data Security Council of India (DSCI) in 2020 and is yet to be implemented[34].

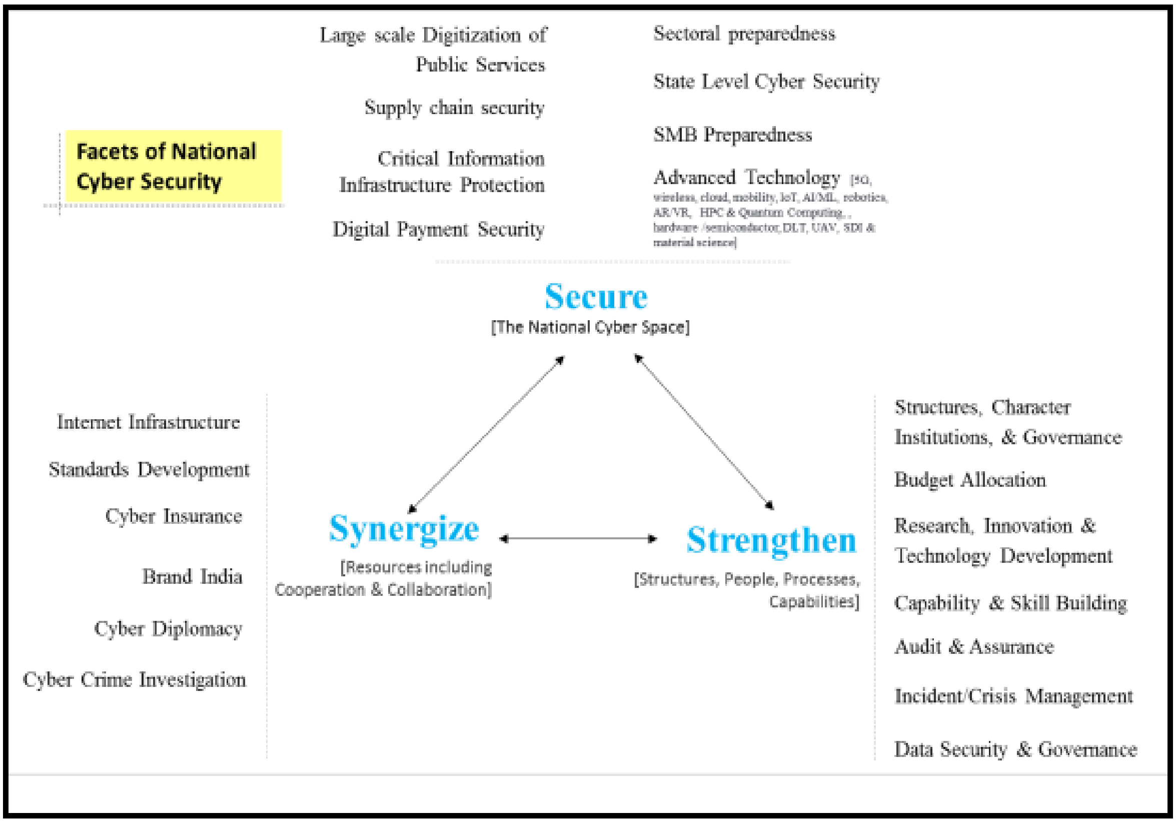
Facets of National Cyber Security
Large scale Digitization of Public Services
Supply chain security
Critical Information Infrastructure Protection
Digital Payment Security
Sectoral preparedness
State Level Cyber Security
SMB Preparedness
Advanced Technology [5G, wireless, cloud, mobility, IoT, AI/ML, robotics, AR/VR, HPC & Quantum Computing, , hardware /semiconductor, DLT, UAV, SDI & material science]
Secure
[The National Cyber Space]
Internet Infrastructure
Standards Development
Cyber Insurance
Brand India
Cyber Diplomacy
Cyber Crime Investigation
Synergize
[Resources including Cooperation & Collaboration]
Strengthen
[Structures, People, Processes, Capabilities]
Structures, Character Institutions, & Governance
Budget Allocation
Research, Innovation & Technology Development
Capability & Skill Building
Audit & Assurance
Incident/Crisis Management
Data Security & Governance

Figure 5: DSCI’s conceptual framework of National Cyber Security Strategy[35]

Figure 5 taken from DSCI’s report, portrays the three key pillars of cyber security strategy needs to incorporate: Securing the cyber space, synergising resources and strengthening the overall cyber space structure including people, processes and capabilities. From the DSCI's report, a few key points that India needs to take steps are the budgetary provision, which is being now allocated only 0.25% of the annual budget and it should be raised up to 1-1.5%. There is a need for incremental investments into deep-tech cyber security innovation. Interestingly, DSCI suggested that the creation of 'Cyber Security Services' under the cadre of Indian Engineering Services will be helpful in creating long-term dedicated cybersecurity personnel. India has already started working on securing its cyberspace by establishing the Indian Cyber Crime Coordination Centre (I4C) and the National Critical Information Infrastructure Protection Centre (NCIIPC) to deal with emerging cyber threats, but it needs to focus on planning a 10-year roadmap to foster the potential collaborations in this end.

2. *Integration of Different Laws and Regulations:*

While there was special emphasis in the National Cyber Security Policy for Public-Private partnerships, there were minimal efforts that have been made to implement these provisions. Collaborations with the private sector can augment resources and for that government needs to incentivize investments for private enterprises for critical infrastructure facilities. As of now, Sections 69 and 72 of the Information Technology Act, 2000 tackles most of the cybercrimes. Section 69 empowers law enforcement agencies to track communication for security purposes and Section 72 deals with protecting sensitive information[36]. Additionally, the National Cybersecurity and Protection of Critical Infrastructure Act, of 2013, and the Data Protection Act, of 2018 also put an extra shield in securing the cyber critical infrastructure. However, considering the evolving nature of cybersecurity threats, there is an urgent requirement of the holistic legal provision under one umbrella legislation, so that the response time can be lessened during the cyber crisis. To deal with the foreign entities fighting their misinformation to further their own propaganda, India needs to have dedicated provisions under the same legislation to deal with foreign threats.

3. *Collaborations of Civil Minds in Implementation:*

During COVID-19, after observing the flow of disinformation campaigns against it, the Indian government has created a WhatsApp Chatbot and dedicated fact-checking unit in the Press Information Bureau. In the Indian Army, there is a Director General Information Warfare, created two years ago to counter the propaganda campaign of China and Pakistan. However, India needs a 'grand plan', including civil minds through creating simulation centres, hypothetical war game scenarios, and Cyber Hygiene Programs in the policy and law-making and implementing the strategy countrywide.

4. *Developing Strategic Cyber Defence Doctrine:*

Tracking the source of disinformation is quite difficult because of the presence of state-sponsored non-state actors. China's wide range of disinformation tactics like fake bots, manipulated media, and coordination with the individuals to further the narrative through social media platforms need a comprehensive doctrine from the Indian end. The key components of the doctrine should be as follows:

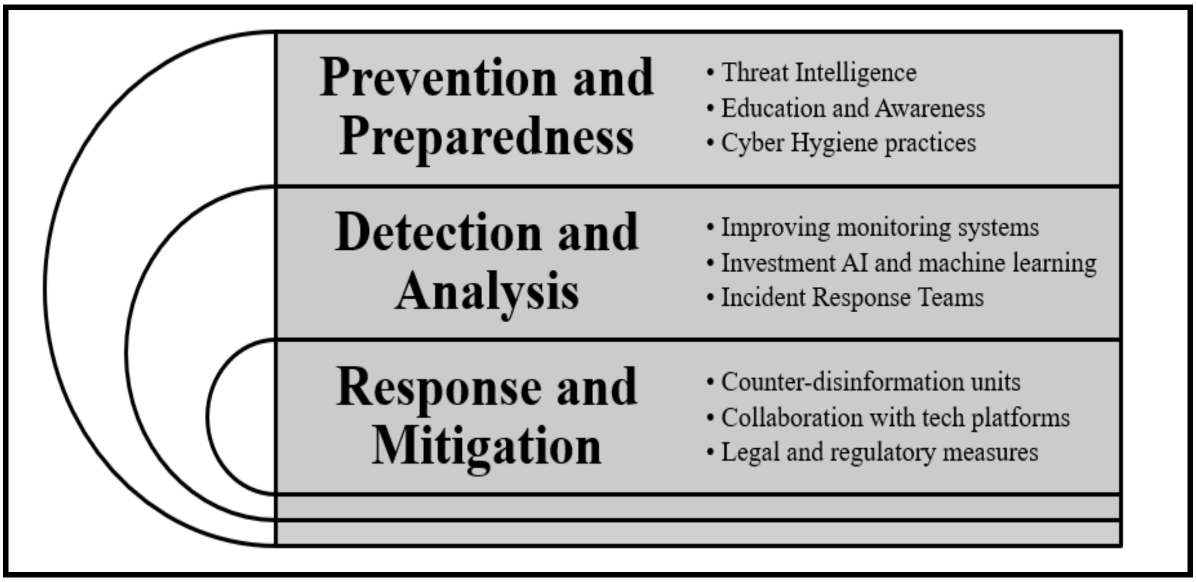
Prevention and Preparedness
• Threat Intelligence
• Education and Awareness
• Cyber Hygiene practices
Detection and Analysis
• Improving monitoring systems
• Investment AI and machine learning
• Incident Response Teams
Response and Mitigation
• Counter-disinformation units
• Collaboration with tech platforms
• Legal and regulatory measures

Figure 6: Recommended Conceptual Framework of Cyber Defence Doctrine

(Source: Compiled by the author)

Conclusion

China’s increasing footprint in global governance with the attempts to manipulate information is a major concern for many countries. While, China’s three warfare strategy is embedded with its vision to impose its own type of world order vis-a-vis the existing one, India along with the other countries with whom China has a boundary dispute, be it in land or maritime, China’s disinformation campaign is constantly influencing the public opinion. Meanwhile, India is also currently on the verge of being a key regional player and rising economic power. Therefore, India needs to take China’s disinformation campaign very seriously. The disinformation campaign of China should not be taken lightly, rather from a critical national security perspective, India needs to disseminate the disinformation and established the proper mechanism to protect its critical database and should adapt combat measures to keep the fact authentic.

DISCLAIMER

The paper is author’s individual scholastic articulation and does not necessarily reflect the views of CENJOWS. The author certifies that the article is original in content, unpublished and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

Endnotes

[1] Sharma, Deepak. 2010. "Integrated Network Electronic Warfare: China's New Concept of Information Warfare." *Journal of Defence Studies* 4 (2): 36–49. https://idsa.in/system/files/jds_4_2_dsharma.pdf

[2] Rising, David. 2022. "Chinese Hackers Reportedly Target India's Power Grid." AP NEWS. April 7, 2022. https://apnews.com/article/technology-business-china-india-b9e32f0d36843b2ac2764d0b4ae2c7e6.

[3] Hunter, Lance Y., Craig D. Albert, Josh Rutland, Kristen Topping, and Christopher Hennigan. "Artificial intelligence and information warfare in major power states: how the US, China, and Russia are using artificial intelligence in their information warfare and influence operations." *Defense & Security Analysis* (2024): 1-35. Artificial intelligence and information warfare in major power states: how the US, China, and Russia (tandfonline.com)

[4] White Papers. 2015. "China's Military Strategy." Eng.mod.gov.cn. 2015. http://eng.mod.gov.cn/xb/Publications/WhitePapers/4887928.html.

[5] White Paper. 2015. "Govt. White Papers - China.org.cn." Www.china.org.cn. 2015. http://www.china.org.cn/government/whitepaper/2015-11/12/content_37046194.htm.

[6] Hwang, Tim. "Maneuver and manipulation: On the military strategy of online information warfare." (2019). Maneuver and Manipulation: On the Military Strategy of Online Information Warfare (armywarcollege.edu)

[7] Chang, Kuo-Cheng. "The impacts of COVID-19 pandemic on the Chinese model of governance and China's propaganda." Taiwan Strategists 6 (2020): 17-32.

[8] Cadell, Cate. 2021. "China Harvests Masses of Data on Western Targets, Documents Show." *Washington Post*, December 31, 2021. https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html.

[9] Lee, John. 2019. "Australia's Gladys Liu Scandal Shows How the Chinese Communist Party Is Weaponizing Race." CNN. September 24, 2019. https://edition.cnn.com/2019/09/23/opinions/gladys-liu-china-australia-opinion-intl-hnk/index.html.

[10] Bowe, Alexander. 2018. "China's Overseas United Front Work Background and Implications for the United States." https://www.uscc.gov/research/chinas-overseas-united-front-work-background-and-implications-united-states.

[11] Kania, Elsa B., and John K. Costello. "The strategic support force and the future of chinese information operations." *The Cyber Defense Review* 3, no. 1 (2018): 105-122. The Strategic Support Force and the Future of Chinese Information Operations (jstor.org)

[12] Costello, John, and Joe McReynolds. "China's strategic support force: A force for a new era." (2018). Costello_Written Testimony.pdf (uscc.gov)

[13] Times of India. 2017. "China Moved Huge Military Hardware into Tibet after Sikkim Standoff: Report." *The Times of India*, July 19, 2017. https://timesofindia.indiatimes.com/india/china-moved-huge-military-hardware-into-tibet-after-sikkim-standoff-report/articleshow/59665316.cms.

[14] Pandit, Rajat, and Saibal Dasgupta. 2017. "China Media Claims Major PLA Build-Up, India Denies It." *The Times of India*, July 20, 2017. https://timesofindia.indiatimes.com/india/india-denies-chinese-media-claim-of-troop-mobilization-in-tibet/articleshow/59674260.cms.

[15] Global Times, Twitter Post, August 4, 2017, 6:00 P.M. https://twitter.com/globaltimesnews/status/893637826759274498

[16] Global Times, Twitter Post, August 28, 2017, 12:57 A.M. https://twitter.com/globaltimesnews/status/902077575731699713

[17] Global Times, Twitter Post, August 19, 2017, 7:46 A.M. https://twitter.com/XHNews/status/898919126567190528

[18] Xinhua. 2017. "Spotlight: What's behind India's Illegal Trespassing into China? - Xinhua | English.news.cn." Www.xinhuanet.com. August 19, 2017. http://www.xinhuanet.com//english/2017-08/19/c_136539497.htm.

[19] MFA, Bhutan. 2017. "Press Release – Ministry of Foreign Affairs and External Trade." Www.mfa.gov.bt. June 29, 2017. https://www.mfa.gov.bt/press-release-272/.

[20] Global Times, Twitter Post, September 9, 2017, 2:15 A.M. https://twitter.com/globaltimesnews/status/1700437751945167141

[21] Jianxue, Lan. 2023. "Reality and Delusion of India's 'Great Power Dream' from G20 New Delhi Summit - Global Times." Www.globaltimes.cn. September 12, 2023. https://www.globaltimes.cn/page/202309/1298054.shtml.

[22] Sagar, Pradip R. 2023. "How China Has Unleashed a Misinformation War on India." Www.indiatoday.in. October 18, 2023. https://www.indiatoday.in/india-today-insight/story/how-china-has-unleashed-a-misinformation-war-on-india-2450656-2023-10-18.

[23] Kakar (retd), Maj Gen Harsha. 2021. "Global Times Attacking India on Covid Mismanagement Should First Investigate Wuhan, CCP." ThePrint. April 26, 2021. https://theprint.in/opinion/global-times-attacking-india-on-covid-mismanagement-should-first-investigate-wuhan-ccp/645547/.

[24] Ahuja, Sarthak, and Samridhi Diwan. 2023. "India's Two-Front Information War." Orfonline.org. May 10, 2023. https://www.orfonline.org/expert-speak/indias-two-front-information-war.

[25] Sharma, Vaasu. 2022. "Information Warfare against India - the China Angle." WION. September 13, 2022. https://www.wionews.com/opinions-blogs/information-warfare-against-india-the-china-angle-515617.

[26] Global Times, Twitter Post, August 26, 2021, 11:20 A.M. https://twitter.com/globaltimesnews/status/1430958232869212166

[27] BBC. 2021. "Backlash after China Weibo Post Mocks India Covid Crisis." *BBC News*, May 2, 2021, sec. China. https://www.bbc.com/news/world-asia-china-56963996.

[28] Banoth, Sai Priya. 2023. "Chinese Cartographic Aggression against India." Cenjows. 2023. https://cenjows.in/wp-content/uploads/2023/08/Sai_Priya_Banoth_IB_Aug_2023_CENJOWS.pdf.

[29] Global Times, Twitter Post, August 28, 2023, 3:7 A.M. https://twitter.com/globaltimesnews/status/1696104724691570945

[30] Wang, Orange. 2024. "China Asserts Claim to Indian-Held Arunachal Pradesh in Latest Place Name List." South China Morning Post. March 31, 2024. https://www.scmp.com/news/china/diplomacy/article/3257387/china-asserts-claim-indian-held-arunachal-pradesh-latest-list-place-names.

[31] Patranobis, Sutirtho . 2024. "China Renames 30 Places in Arunachal Pradesh; Jaishankar Says It Means Nothing." Hindustan Times. April 1, 2024. https://www.hindustantimes.com/india-news/china-renames-places-in-arunachal-pradesh-for-the-4th-time-targets-30-locations-101711976946710.html.

[32] MeitY. 2013. "National Cyber Security Policy." July 2, 2013. https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf.

[33] Ministry of Communication and Information Technology. 2013. "National Cyber Security Policy 2013." 2013. https://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf.

[34] DSCI. 2020. "National Cyber Security Strategy 2020." *Https://Database.cyberpolicyportal.org/Api/Files/1664377398590fe3kyzt8xwd.pdf*. NASSCOM.

[35] Ibid

[36] *The Information Technology Act, 2000*. 2000. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.