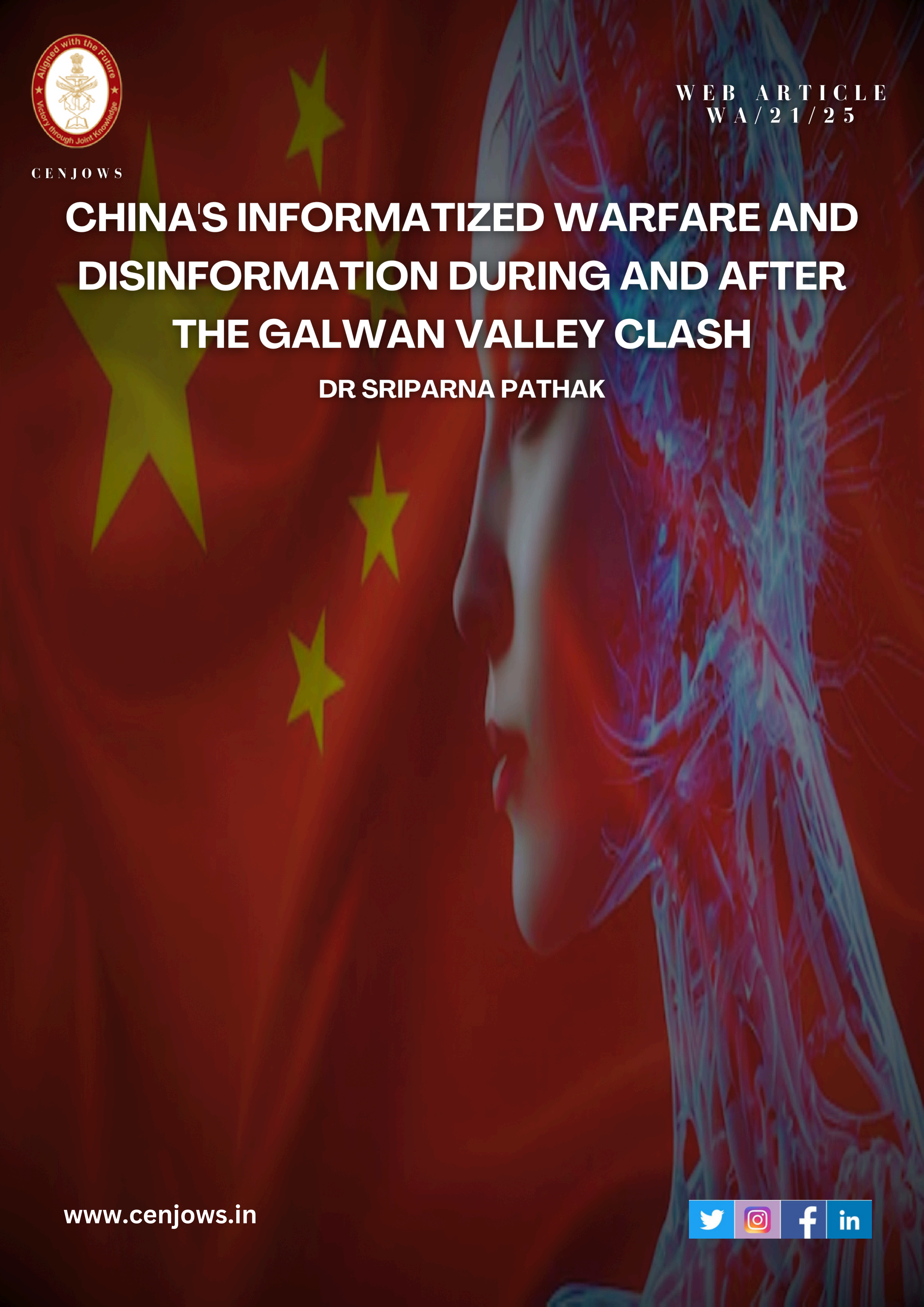


CENJOWS

WEB ARTICLE
WA/21/25

CHINA'S INFORMATIZED WARFARE AND DISINFORMATION DURING AND AFTER THE GALWAN VALLEY CLASH

DR SRIPARNA PATHAK

www.cenjows.in

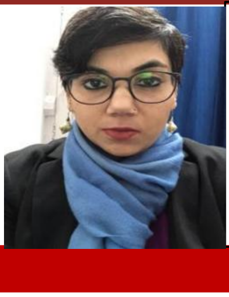
CENTRE FOR JOINT WARFARE STUDIES

Aligned with the Future

Victory through Joint Knowledge

CENJOWS

China's informatized warfare and disinformation during and after the Galwan Valley Clash



Dr. Sriparna Pathak is a Professor and Associate Dean of Admissions to Associate Dean of Careers at the Jindal School of International Affairs of O.P. Jindal Global University, Haryana, India.

Abstract

The original concept of war as hostilities between armies of actors, that largely remained restricted to sovereign borders has undergone several changes. With the emergence of non-traditional actors, warfare no longer remained limited to sovereign borders or to armies specifically created and designated to launch and control the effects of wars. With the emergence of non-traditional actors, what also emerged was unconventional warfare, which is broadly understood as military and quasi-military operations that entail the usage of covert forces or actions aimed at sabotage, diversion, subversion, biowarfare, propaganda, or guerilla warfare. This article explores the evolution of warfare into its modern forms that are unconventional, urban, and participative and are mostly shaped by rapid technological advancements

The original concept of war as hostilities between armies of actors, that largely remained restricted to sovereign borders has undergone several changes. With the emergence of non-traditional actors, warfare no longer remained limited to sovereign borders or to armies specifically created and designated to launch and control the effects of wars. With the emergence of non-traditional actors, what also emerged was unconventional warfare, which is broadly understood as military and quasi-military operations that entail the usage of covert forces or actions aimed at sabotage, diversion, subversion, biowarfare, propaganda, or guerilla warfare.

With the emergence of easily available technology, warfare underwent further changes. The advent of smartphones and global connectivity added further layers of complexity to the issue. Due to the usage of personal digital devices, even conventional war, while occurring in an entirely connected information technology changes into what is now known as participative warfare. As seen in the case of the ongoing Russia- Ukraine war, participative warfare takes place through the integration of various non-traditional actors into the conflict space, facilitated by advancements in technology and communication networks. Several national security smartphone apps launched by the Ukrainian government enable civilians to use their smartphones to report troop movements. (Norman,2024)[1]

Facets of technology that can and have been used in urban warfare in the age of technology include unmanned aerial vehicles (UAVs), equipped with cameras and sensors that gather intel on enemy positions and movements, or high-resolution satellite images to identify enemy hideouts or tunnels, and other infrastructure. An example of this is from 2021 when there was a twin drone attack on the Jammu Air Force station, in which two UAVs dropped two improvised explosive devices (IEDs) damaging a part of the building, and this was the first reported use of drones to attack military installations in India. (Krishna and Singh, 2023)[2]. Acoustic sensors that detect and locate gun fires and other sounds to locate enemy locations also are important tools. Encrypted communication systems for real time coordination between troops, integrated systems providing situational awareness, and mapping also become realities of urban warfare in the technology era. Social media, which has become a part of human lives in this epoch of history also become tools during warfare as monitoring platforms provide useful in times of crises to gather intelligence on enemy movements and for facilitating propaganda led psychological warfare.

Cyber warfare which includes network exploitation, cyber-attacks to disable enemy infrastructure are also hard to ignore realities. In a week after China intruded into India's territory in Galwan, Chinese hackers launched more than 40,000 attacks on Indian cyber space (Mishra, 2020)[3].

Additionally, there were several social engineering tactics from China to unleash psychological warfare against India. As such, while the Indian Army and the Chinese People's Liberation Army (PLA) still await de-escalation of tensions at the borders between India and China, it becomes pertinent to analyse China's disinformation during the Galwan Valley clash and to understand how the People's Republic of China (PRC) uses current trends in the urban warfare in the age of technology.

China's weaponisation of information during wars

The Chinese approach to weaponising information during wars is an evolving, yet sophisticated strategy, which is deeply integrated with its military doctrine. Information, as a crucial domain of modern warfare has been recognised long ago by the PLA. It is reflected in the ways in which kinetic operations are amalgamated with informatized warfare. According to Chawla, 2022, informatized warfare is a concept for offensive purposes, and implies three kinds of usage of information, as it pertains to the enemy. (Chawla, 2022)[4]. At a general level, it entails knowledge and awareness of the identified enemy's social, political and economic structures. At the second level it implies precise knowledge of the enemy's assets, coupled with a knowledge of the enemy's control and command structure. Thirdly and at the narrowest level, it belongs to the enemy's cyber space.

An understanding of China's grey zone warfare is pertinent in this context. Grey zone tactics are forceful actions, short of direct, armed conflict, but go beyond normal, diplomatic, economic and other activities. According to Lin, Garafola, McClintock, Blank, Hornung, Schwindt Moroney, Orner, Borrman, Denton, 2022, these activities are widely recognised as being an important part of China's efforts to advance its own domestic, economic, foreign policy and security objectives. (Lin, Garafola, McClintock, Blank, Hornung, Schwindt, Orner, Borrman, Denton, 2022)[5]. The problem is acute because there is no global consensus on the precise tactics.

As a result of increasing digitisation, informatised warfare as a key component of China's grey zone warfare, aims at creating confusions around, or even destroying the national systems.

Public opinion, institutions and legal systems become key targets[6] (Sina News, 2004). As such, the Chinese PLA has been preparing the strategies since 2003, in its three warfare doctrines, which is based on psychological, media and legal warfare tactics, which complement existing diplomatic, economic and military measures, with the aim to cultivate a favourable strategic environment in the neighbourhood and to promote and defend its fundamental interests on sovereignty and territorial integrity in times of peace, while preparing for the myriad possibilities of war[7] (Escriche, 2022).

Historically, China's interest in this area spiked after observing the United States' dominance in the 1991 Gulf War, where information technologies enabled precision strikes and overwhelming battlefield awareness[8] (Dahm, 2021). Since then, the PLA has developed frameworks that blend electronic warfare, cyber-attacks, propaganda and military deception to disrupt enemy decision making and morale[9] (India Foundation, 2017). China's 2008 Defence White Paper formalised the shift, while highlighting the role of information-based weapons, like precision guided munitions and advanced command systems, while also laying the ground work for broader influence operations[10] (People's Republic of China State Council Information Office, Beijing, 2009).

During a potential conflict, the PLA can deploy cyberattacks, as was seen in the case of the Galwan Valley clash with India in 2020; and this is done to paralyse enemy communication networks or to seize control of critical infrastructure, such as satellites, to render them useless for surveillance or for relaying data. Electronic warfare, including jamming radar and communications, complements this by creating chaos in the adversary's operational awareness. Simultaneously, psychological warfare, through the usage of state media, social platforms, or even leaflets, aims to undermine enemy resolve, sow confusion, or sway public opinion both domestically and abroad[11].

A key element is that of 'information superiority', where controlling the narrative along with the flow of data becomes as decisive as firepower (Dahm, 2021). China's amplification of disinformation during tensions has been seen not only in India, but also in its conflicts with Taiwan, Philippines, Vietnam, and so on. In 2024, it was reported by AFP that violent confrontations between Philippine and Chinese vessels in the South China Sea are being manipulated online by disinformation networks with origins in China[12]. Similarly, in 2024, Scott W. Harold, writing for the RAND Corporation, had stated how China targets Taiwan through its myriad disinformation campaigns[13] (Harold, 2024). This suggests a playbook that gets scaled up in war time to manipulate perceptions.

China also leverages its technological edge, investing heavily in artificial intelligence (AI), big data and quantum computing to enhance capabilities for informatised warfare. In 2024, a Chinese government report stated that China is formulating plans to develop emerging industries including quantum computing and will continue to strive for self-sufficiency in technology. It also plans to step up efforts in big data and AI to launch a number of major science and technology programmes to meet major strategic and industrial development goals[14] (Reuters, 2024). The fact that the report mentions strategic goals as one of the reasons for the investments in these realms implies that informatised warfare is a key focus for the country.

As such, the idea is not just to destroy but to dominate the cognitive battlefield- disrupting an enemy's ability to think and react effectively. This aligns with ancient strategist Sun Tzu's principle of subduing the enemy without fighting, updated for the digital age. In a hypothetical war scenario, say over Taiwan, China might combine these tactics: hacking into military networks, jamming U.S. or allied satellite feeds, and flooding global media with narratives of inevitability or moral justification to deter intervention. The goal is to create a fait accompli before a full kinetic response. However, if China's adversaries maintain robust information defences, then its disinformation efforts can backfire. Nevertheless, the PLA's focus on using information as a weapon underscores a broader trend: in modern war, the battle for bytes and minds may decide as much as bullets and bombs. In this context, it becomes pertinent to understand the strands of disinformation China has used against India and the Indian Army in particular in Galwan, to predict whether the trend is to continue with regards to Chinese claims on Indian sovereignty or not.

China's disinformation tactics around the Galwan Valley clash of 2020

During the Galwan Valley standoff, and post the clash, around 400-500 fake X (formerly Twitter) accounts were activated[15] (Goyal and Priyadarshini, 2020). Most of these fake accounts were of Chinese or Pakistani origin and were created to spread fake narratives in China's favour.

Twitter groups carried out this activity, and once a group made a tweet, it asked others to retweet it. There is a deep alignment between Pakistan and China based handles.

While many times it may seem that a handle is from Pakistan, deeper searchers clarify that China based handles started the disinformation campaign first and then Pakistan based handles picked them up. The five narratives that China based handles spread, both in Chinese as well as in English across a series of platforms in China and beyond are briefly as follows:

1. A video claiming Indian Army and the Chinese PLA in combat at Galwan:

The video is to be found on YouTube claiming to show the 'real fight' between Indian and Chinese soldiers in Galwan, where the clash took place[16] (BBC News, 2020). It had more than 21,000 views and was also viewed on X. Subtitles stated that the Indian government has confirmed the video. However, the Indian government has not claimed any video, and even if it had to, it would not be through an individual person's account on YouTube. Additionally, video is shot in daylight whereas the 2020 clash in the Ladakh region took place at night. The same video had been posted both in August 2017 and September 2019, and on both occasions, it claimed to show skirmishes between the Indian Army and Chinese troops[17] (Alt News, 2020).

2. A video portraying an emotional scene with Indian soldiers crying and hugging (BBC News, 2020)**:**

The Chinese have manipulated old and out of context videos wherein a video from an incident in Kashmir in 2019 involving Indian Army persons has been manipulated to show the Indian Army soldier as weak and emotional whereas this video had no linkages with Galwan Valley clash in any manner.

3. A post on X with a video of Indian Army soldiers and PLA soldiers arguing[18] (TRT World, 2021)**:**

Chinese have uploaded multiple wrong videos including the one highlighting the superiority of the PLA troops. It is a well-known fact that Indian soldiers are far more superior as compared to the Chinese soldiers. In fact, the Chinese soldiers are also at times referred to as Chocolate soldiers.

4. Indian Army was captured by the PLA:

Guancha News posted on June 21 that the Chinese PLA captured the Indian Army. Indian news media was quick to fall to the disinformation and reported that Indian Army has been captured by the PLA[19] (Haider and Peri, 2020)**.** However, responding to the reports, the Indian Army and the Chinese foreign ministry both denied that any Indian Army personnel was taken into Chinese custody[20] (Al Jazeera, 2020). The important point to note here is that the Guancha Syndicate is one of China's most popular and influential online media portals. It was launched in 2012, to provide an alternative, seemingly decentralised source of news for Chinese internet users. Guancha is also a locus of China's "new nationalist" movement (Doublethink Lab, 2021)[21] predicated on anti-Western, and anti-Indian sentiment and conviction in the superiority of China's model of government.

5. Images of dead bodies of the Indian Army[22] (Wen, 2020):

On June 18, 2020, a so-called article was published on China's Weixin on why the Indian Army suffered so many casualties against the PLA in Galwan. Weixin is the Chinese name for the messaging app, WeChat, which is widely used in the country and functions as a comprehensive, super app for communication, payments, social media and various other services. The articles used an image trying to depict how many Indian Army personnel the PLA had killed in the Galwan Valley clash. By the end of 2020, the article had been read more than 100,000 times, and the same image depicting the apparent death of Indian Army personnel in Galwan, also cropped up on social media in India. A simple reverse image search showed that the image is actually from Nigeria and depicts the aftermath of an incident in 2015 when Boko Haram militants had killed Nigerian soldiers[23] (Yandex reverse image search). The image was also used on a so-called Pakistani news website called Baaghitiv[24] (Waseem, 2020).

What do these tactics mean?

While these handles were activated in 2020, and a lot of them have been now debunked and taken down by social media platforms, several others have cropped up. The narrative is first circulated on the Chinese cyber space and then it is picked up by Pakistani handles and once it is in English, it enters the Indian cyber space much more easily.

Conclusion

China’s usage of information warfare is only set to increase with the sorts of investments China is making in AI and quantum computing. Given the fact, as previously mentioned, that the Chinese government sees these investments as necessary for strategic and development purposes, only more state led disinformation can be expected against India. The Indian Army and the Chinese PLA are yet to de-escalate at the friction points finally as existing from 2020. In this scenario, the aggressive targeting of the cyber space only means that there is also a preparation for kinetic warfare as well. The Chinese cyber space is deeply controlled by the Communist Party of China (CPC). China’s Cyber security law, enacted in 2016 has led to significant investments in its cybersecurity infrastructure and its country's expenditure on internal security, which includes cybersecurity, has been increasing steadily, with estimates suggesting it surpassed USD 200 billion in 2020[25]. Unless the CPC wants these narratives in the form of opinion pieces or news articles to be in the cyber space, it is not possible for them to exist. The fact that whole sets of videos and so-called news articles on how Galwan is China’s or how the Indian Army lost to the PLA still remain in the Chinese cyber space means that there is preparation for kinetic action as well.

In this context, India can leverage the defence think tanks it has and create data sets of repeat peddlers of disinformation in the Indian cyber space and then get platform providers to take them down. Additionally, India needs to pre-bunk these narratives before they can cause psychological warfare. This could also be done through defence think tanks or through private think tanks. Third, there is an urgent need for the defence services to learn to use tools like WeVerify or Yandex or OpenCTI to understand how to track disinformation and to pre-bunk or debunk them. Collaborations and mutual sharing of experiences with countries like Taiwan that have been at the forefront of fighting Chinese disinformation can also be immensely helpful.

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] Norman, Jethro. “War volunteers in the digital age: How new technologies transform conflict dynamics”. Danish Institute for International Studies. July 1, 2024. https://www.diis.dk/en/research/war-volunteers-in-the-digital-age-how-new-technologies-transform-conflict-dynamics

[2] Krishna, Surya Valliappan and Singh, Ashima. “Drone Intrusions Along the India-Pakistan International Border: Countering an Emerging Threat”. Carnegie Endowment for International Peace. Julu 10, 2023. https://carnegieendowment.org/posts/2023/07/drone-intrusions-along-the-india-pakistan-international-border-countering-an-emerging-threat?lang=en

[3] Mishra, Siddhant. “Chinese hackers attempted attack on Indian cyberspace more than 40,300 times in a week post-Galwan clash”. *Times Now*. June 22, 2020. https://www.timesnownews.com/india/article/chinese-hackers-attempted-attack-on-indian-cyberspace-more-than-40300-times-in-a-week-post-galwan-clash/610315

[4] Chawla, A.K. “China’s Strategy of ‘Informationised and Intelligent’ Warfare”. *SP’s Naval Forces*. Issue 02/2022. https://www.spsnavalforces.com/story/?id=802&h=Chinaandrsquo;s-Strategy-of-andlsquo;Informationised-and-Intelligentandrsquo;-Warfare#:~:text=In%20the%20Chinese%20concept%2C%20informationised,strike%20technologies%20are%20equally%20important.

[5] Lin, Bonny; Garafola, Crisgtina L., McClintock, Bruce; Blank, Jonah; Hornung, Jeffrey W., Schwindt, Karen; Moroney, Jennifer D.P., Orner, Paul; Borrman, Dennis; Denton, Sarah W., “A New Framework for Understanding and Countering China's Gray Zone Tactics”. *RAND.* March 30, 2022. https://www.rand.org/content/dam/rand/pubs/research_briefs/RBA500/RBA594-1/RAND_RBA594-1.pdf

[6] Sina News. “中国人民解放军开始“三战”的研究和训练” (The Chinese People's Liberation Army began research and training on the "Three Warfares"). July 16, 2004. http://mil.news.sina.com.cn/2004-07-16/1738210714.html

[7] Escriche, Inés Arco. "Winning without fighting: China's grey zone strategies in East Asia. *CIDOB Barcelona Centre for International Affairs*. September 2022. https://www.cidob.org/en/publications/winning-without-fighting-chinas-grey-zone-strategies-east-asia

[8] Dahm, Michael. "China's Desert Storm Education". *U.S. Naval Institute*. Vol. 143/3/1,417. March 2021. https://www.usni.org/magazines/proceedings/2021/march/chinas-desert-storm-education

[9] India Foundation. "PLA in Electromagnetic Domain". September 12, 2017. https://indiafoundation.in/articles-and-commentaries/pla-in-electromagnetic-domain/

[10] People's Republic of China State Council Information Office, Beijing. "2008年中国的国防(China's National Defence in 2008). January 20, 2009. https://www.gov.cn/zhengce/2009-01/20/content_2615769.htm

[11] Bhattacharya, Sanchaly. "China's Psychological Warfare: Unearthing China's Psychological Tactics Against India". *CENJOWS*. https://cenjows.in/wp-content/uploads/2024/06/Ms_Sanchaly_Bhattachary_IB_June_2024_CENJOWS.pdf

[12] https://www.france24.com/en/live-news/20241126-philippines-china-clashes-trigger-money-making-disinformation

[13] Scott, Harold W. "How Would China Weaponize Disinformation Against Taiwan in a Cross-Strait Conflict?". *RAND*. April 15, 2024. https://www.rand.org/pubs/commentary/2024/04/how-would-china-weaponize-disinformation-against-taiwan.html

[14] Reuters. "'China to step up quantum computing, AI in tech self-sufficiency drive". March 5, 2024. https://www.reuters.com/technology/china-step-up-quantum-computing-ai-efforts-its-aims-tech-self-sufficiency-2024-03-05/

[15] Goyal, Prateek and Priyadarshini, Anna. "How a 'disinformation network' on Twitter added to the tension surrounding the Galwan Valley conflict". *Newslaundry*. July 18, 2020. https://www.newslaundry.com/2020/07/18/how-a-disinformation-network-on-twitter-added-to-the-tension-surrounding-the-galwan-valley-conflict

[16] BBC News. “Galwan Valley: The fake news about India and China's border clash”. June 19, 2020. https://www.bbc.com/news/world-asia-53092492

[17] Alt News. “Old video shared as recent confrontation between Indian and Chinese troops”. May 21, 2020. https://www.altnews.in/an-old-video-of-chinese-army-arguing-with-indian-army-at-border-shared-as-recent/

[18] TRT World. February 21, 2021. Twitter. https://x.com/trtworld/status/1363715140021968897

[19] Haider, Suhasini and Peri, Dinkar. “Ladakh face-off | Days after clash, China frees 10 Indian soldiers”. *The Hindu.* June 19, 2020. https://www.thehindu.com/news/national/ladakh-face-off-days-after-clash-china-frees-10-indian-soldiers/article31863845.ece

[20]Aljazeera. “China denies detaining Indian soldiers after reports say 10 freed”. June 19, 2020. https://www.aljazeera.com/news/2020/6/19/china-denies-detaining-indian-soldiers-after-reports-say-10-freed

[21] Doublethink Lab. “Tracing control and influence at Guancha news”. May 1, 2021.

[22]Wen, Zitao. “印军死伤为何如此惨重？” (Why did the Indian army suffer such heavy casualties?). Weixin. June 18, 2020. https://mp.weixin.qq.com/s?__biz=MzA5NjM3MzQzOA==&mid=2651760922&idx=1&sn=3f307a86e47e2c0cb2460e855f3fbbac&chksm=8b4b16cbbc3c9fdd23c4acac4ff3a51d7c1b6e5982f064300affc86c75beacf4f36c73c5f920

[23] Yandex Reverse Image search. https://yandex.com/images/search?cbir_id=371446%2FVnPbvup3fZbC5UzUyIc-Ew3002&rpt=imageview&url=https%3A%2F%2Favatars.mds.yandex.net%2Fget-images-cbir%2F371446%2FVnPbvup3fZbC5UzUyIc-Ew3002%2Forig

[24] Waseem, Aina Maria. “Indian Soldiers Killed by Chinese Army”/ June 17, 2020. https://en.baaghitv.com/indian-soldiers-killed-by-chinese-army/

[25] Zenz, Arian. “China’s Domestic Security Spending: An Analysis of Available Data”. *Jamestown Foundation*. March 12, 2020. https://jamestown.org/program/chinas-domestic-security-spending-analysis-available-data/