Countering the Contagion Effect of COVID-19: An Appraisal of China's Influence Operations

Vivek Verma

Abstract

For China to realise its millennium goal, it needs to radiate its influence globally and simultaneously engage internally with the local population to ensure social stability. COVID-19 has disrupted China's dream of showcasing to the world a model state with Chinese characteristics. Influence operations thus form the basis of curating and presenting a credible image of the Communist Party of China (CPC) besides altering the behaviour of its adversaries. China has tried to firewall the western influence besides making inroads into other countries' economic, political and societal institutions. At the time of COVID-19 crisis, it is employing leverages to correct the narrative while gaining situational awareness through revamped structures and employment of technologies. It is thus imperative to appraise China's influence operations capabilities.

Introduction

On 8 September 2020, China celebrated the success against the COVID-19. Chinese President Xi Jinping in his lengthy speech at the

Brigadier **Vivek Verma** is a Senior Research Fellow at The United Services Institution of India, New Delhi. He was the former Deputy Director at the Centre for Land Warfare Studies, New Delhi.

Great Hall of the People used the occasion to recount the merits of the one-party rule and emphasised the need for strong leadership as "the most reliable backbone" for the Chinese people in times of crisis.[1] According to World Health Organization (WHO), there have been 45,942,902 cases with 1,192,644 deaths worldwide; while in China, there have been 91,921 cases with 4746 deaths, as on 1 November 2020.[2]

Though China may be rejoicing and showcasing to the world and their local populace that it has been able to tame the pandemic, but it is aware of the headwind facing it. The origin and delay in sharing COVID-19 specimen details with the world and naming it as 'Wuhan Virus' or the 'China Virus' has tarnished China's image. China does not want history to be unkind to it, and it is set to face the world squarely through its influence mechanism.

With the United States (US) being affected the most under COVID-19, with more people lost to a pandemic than it did during the raid on Pearl Harbour during World War II or the attack on the World Trade Centre on 11 September 2000; the US is leading the charge against China over handling of COVID-19 by manipulating the WHO. The US Secretary of State Mike Pompeo even justified the US unilateral action of quitting the WHO.[3] The sequence of events leading to the pronouncement by the WHO of declaring COVID-19 as a Public Health Emergency of International Concern (PHEIC) on 30 January 2020, has been at the centre of the debate. Incidentally, the initial WHO timeline was replaced on 29 June 2020, with the curated version by the WHO to set the record straight.[4] According to WHO's initial statement the cluster of cases of pneumonia of unknown cause was noticed by Chinese authorities in its Wuhan City, Hubei Province, on 31 December 2019, and genetic sequence of identified COVID-19 was shared on January 12, 2020; and it was only on 11 March 2020, WHO declared COVID-19 as a 'pandemic.'

Contextualising COVID-19: The Pre-COVID Actions by China

Quelling the Truth

China's core national defence aim is to safeguard national political security, people's security and social stability.[5] China seemed to be well aware of the pandemic fallout on the society and had probably assessed the capability degradation to administer and control the movement of populations.[6] The foremost priority for the CPC, therefore, was to deal with societal turbulence and to quell any noise within the medical and media fraternity. This was evident from the quick reaction by the China Public Security Bureau to suppress Dr. Li Wenliang's warning of a SARSs-like virus in Wuhan on 30 December 2019—an issue that had the potential to disturb the social order.

The timing of disclosure and messaging are of importance to the CPC. By mid-December 2019, the guidelines for the local journalists were issued by the CPC to ensure content sanctity includes cinema, TV, journalism, music, radio, social media and all the new ways to consume content. The Cyberspace Administration of China (CAC), the Chinese government's watchdog, has set up supervision on platforms that include those run by microblogging service provider *Sina Weibo*, short video and news apps operator ByteDance, and Tencent Holdings, WeChat app known as *Weixin* in mainland China where it has more than 1 billion users. "WeChat account shutdowns" became a trending topic on *Weibo* before the discussion page was removed on 6 February 2020.[7]

Ramping up the Effort

Despite growing cases in Wuhan, China carefully weighed the pros and cons with the nurtured support at the WHO. While the flurry of activities was taking place at WHO emergency committee to submit the report, China used the period to ramp up the state machinery in a quasi-

warlike mode to deal with the virus which it knew to be pandemic. The leadership was probably aware of the unknown virus. Hence, it used the time to secure the supplies of epidemic related medical equipment from the worldwide market, including the US, which exported 2.4 million pieces to China between 24 January and 29 February 2020.[8]

Almost a week before the WHO declared COVID-19 as a pandemic, Xi Jinping on 25 January, on the eve of the Chinese New Year of Rat, declared the tough measures to tackle the COVID-19 threat which had Wuhan at its epicentre. Within a day Premier Li Keqiang was made the head of the leading small group of epidemic control with 32 departments established under its wing, mobilisation of the People's Armed Police (PAP), activation of PLA Logistics Command at Wuhan and pairing of 19 provincial regions with 16 cities to prepare for Hubei-like outbreak of the COVID-19.

Pushing the Narrative in the Post-COVID-19 World by the CPC

The CPC intended to showcase the existence of strong command governance system under Xi. The agile governance narrative was woven to tell the citizen in China and the world community at large that the CPC cared for its people and the willing participation by the people helped in stemming the pandemic outbreak. The WeChat and *Weibo* were put under vigilance. Amidst global destabilisation, the strategic objective for Xi Jinping is clear—to protect the supremacy of the CPC and prevent the snowballing of crisis. It endeavours to localise the impact due to COVID-19 while ensuring social stability within its borders so that its millennium goal of prosperity remains intact. For the CPC, its image is very important to it. It needs to be seen as the champion of the Chinese cause. China recognises that the stigmatisation due to COVID-19 will add another humiliation narrative attributing to the CPC rule—a narrative it can ill afford. Hence, employing the 'three warfare' strategy is the only choice available to it to control the opinion,

legal and psychological space to correct the battle of perceptions both locally and internationally.

The CPC's bigger concern rested on handling of the narrative coming out from Wuhan. As a result of which, Ms Sun Chunlan, the Vice Premier and former United Force Work Department (UFWD) minister,[9] was appointed instead of an epidemic expert to deal with the Wuhan crisis. A Big-Data surveillance plan through mobile applications like AliPay and WeChat were used to enforce restrictions and allowed the government to keep track of people's movement. The news of the mysterious disappearance of 21 million mobile users[10] at the start of the pandemic had to be refuted. To communicate the curated images and assuage the local population apprehensions, daily briefings by the State Council were undertaken. Chinese prowess in dealing with the epidemic was showcased by building of a 1000-bed hospital over ten days with the two-pronged aim—firstly to calm the population about the lack of medical facility and secondly to market Chinese healthcare systems to the countries tied to China's Belt and Road Initiative (BRI).[11]

To further control the narrative, Research Paper Sanitisation Directive was promulgated for the research scholars.[12] Sponsored research such as "China's Fight against COVID-19" was jointly compiled by China Daily, Tsinghua University and Peking Union Medical College was published to showcase agile governance, strong leadership of President Xi and applause people's contribution in containing the virus.[13] Besides, China's National Library has been tasked to record the history of COVID-19.[14]

The world, distanced, divided and destabilised, is being shaped by geoeconomics and geopolitical tumult. The origin of COVID-19 or so called 'China Virus' seriously impacts the credibility and image of China and the CPC. The Party is therefore fully engaged in a concerted influence war to show the world that the handling of the pandemic by the liberal democracies of the world has been casual and causal for its spread. At the same time, it intends to firewall any UN-led initiative to trace its origin

of the COVID-19 as alluded by the UN Secretary-General, Antonio Guterres.[15] While the world is struggling to deal with the pandemic spread, the CPC has its game plan cut out that entails: first, concerted influence operations to correct the narrative globally. Second, employ situational awareness programme to gain strategic intelligence. And third, localise conflict through a well-orchestrated war-control strategy

China's Influence Operations

Influence operation relies on persistent communication capability driven by the content, carrier and the audience compartmentalised into echo chambers to alter their behaviour. The content weaves the narrative that is controlled, curated and filtered and disseminated to the masses, and the global audience in accordance with the CPC guidelines. The modern world has made communication ubiquitous with exponential pace of proliferation. The problem that China encountered with the collapse of the Soviet Union was the rapid growth driven by the internet explosion and the ability of the western world to penetrate Chinese society through new innovative products from social media platforms, to search engines tools to smartphones. The cyber dependency tied to economic and societal progress created vulnerabilities for the CPC to control the narrative. Behavioural dynamics attributed to social platforms have also triggered protests in Hong Kong and Arab Spring. Hence, to firewall, the vulnerabilities shaped by influence mechanism, the CPC has instituted multi-pronged measures, as discussed below.

Securing Data, Cyber and Space

The Internet of Thing (IoT) led by Big Data is supported through Artificial Intelligence (AI), and quantum computing tools to handle the veracity, velocity and volume of data flow. It created echo chambers based on the individual choices. The data tool is used to trigger tailored responses against the targeted audience. The intent is to infuse and sustain

a narrative and eclipse it if it turns negative. Thus, overdependence on data technologies across governance structure, business and financial environment is guiding the new age competition and conflict. Data breaches and cyber-attacks have emerged as the top global risks. Since the data economy is reliant on cyber and space for storage and flow of data, hence, it has tasked the PLA to protect and secure the critical domains of cyber and space. Thus, structures within the CPC and PLA have been reformed and revamped to deal with the influence operations.

Securing Strategic Technologies

According to 2017 PricewaterhouseCoopers report, China has pre-empted the US in rolling the 5G connectivity and AI. It has used predatory methods to secure strategic technologies to bridge the capability gap. The large efforts of its agencies are also devoted to influence and obtain key technologies. Some of them may fall within the economic realm, but most of the targeted source is through cyber business espionage and intelligence-based operations. The Chinese modus operandi is outlined in Table 1.

Table 1: China's Modus Operandi to acquire Technology and Talent for Capability Development

Joint Ventures (JV)	Uses JVs for acquiring technology and technical know-how.
Research Partnerships	Seek partnerships with government laboratories to acquire specific technology and soft skills to run such facilities.
Academic Collaborations	Uses collaboration with universities to acquire specific research and gain access to high-end research equipment.
S&T Investments	Sustained long-term state investments in S&T infrastructure.

Merger & Acquisitions	Seeks to buy companies tied to technology and talent.
Front Companies	To obscure the CPC links in acquiring export-controlled technologies.
Talent Recruitment	Influence foreign talent to work for Chinese key projects.
Intelligence Services	The Ministry of State Security and intelligence units are deployed to acquire technologies.
Legal and Regulatory	China uses the law to disadvantage foreign companies.

Source: Adapted from National Counterintelligence and Security Center (2018).[16]

Firewalling Cybersecurity through the Legal Framework

In 2017, China legislated Cybersecurity Law to ensure 'Hierarchical Protection of Information Security'—to mandate localisation of data in China while making the network operators responsible for cybersecurity. The sales of critical cybersecurity products are subjected to security certification. Article 38 of the law imposes a steep penalty on compromising the critical information that may cause serious damage to national security, economy and public interest as notified by the State Council. Thus, legislation has been used to allow predatory practices by the CPC.

Predatory Practices

On 1 December 2019, China rolled out Cybersecurity Multi-level Protection Scheme (MLPS 2.0) to deal with emerging technologies like mobile applications, Big Data, cloud computing and IoT. On 1 March 2020, Information Security Technology—Implementation Guide for Classified Protection of Cyber Security[17] was legislated to regulate technical and organisational internet security controls of companies and individuals. Thus, it allows the Ministry of Public Security and the CCAC and the Office of the Central Leading Group for Cyberspace Affairs have complete access to regulate the internet, and control content. The aim is

to firewall Chinese interests through surveillance and controlling the flow of data out of the Ministry of Public Security precinct. However, the data is available to be used by the CPC to bolster state-owned enterprises like the CETC, Huawei, and others.

Strengthening Cyber Defence

According to the 2013 *Science of Military Strategy*, 'low cost, high benefit and low risks' is what makes cyberwar a preferred tool for influencing. The publication is sceptical of the US military and the phenomenal overreach of FANG (Facebook, Amazon, Netflix and Google) to undermine the society. The cyber defence measures initiated by the CPC include: First, alternate applications, to provide alternate flavour to its society, China has mirrored the social platform by creating BAT (Baidu, Alibaba and Tencent) while banning Facebook, Twitter, etc. The list of mirrored platforms is in Table 2. It allows China to monitor content and control its spread which was effectively used by the cyber agencies of China to prevent the societal disturbance during COVID-19 outbreak.[18]

Table 2: List of Mirrored Apps by China

Chinese Platform	Mirrored Equivalent
WeChat	Facebook
Sina Weibo	Twitter
Tencent QQ	Instant Messenger
Zhihu	The Quora of China
DouYin (TikTok)	Short-video App akin to YouTube
Youku Tudou	Former YouTube of China
Baidu Tieba	A Search Engine Forum
Momo	Tinder of China
Maimai	LinkedIn of China

Source: Prepared by the Author with reference to DeGennaro (2020).[19]

Second, indigenous technology Development based on 5G and AI, to firewall outside influence and improve its penetration across the globe, China has invested heavily in localising the Information Communication Technology (ICT) industry aided by 5G and AI. According to CCAC, China has 802 million netizens and a digital economy of US$ 3.86 trillion, and it estimates that the cybersecurity market by 2021 may reach US$ 11.2 trillion. Thus, China is keen to bite into this exclusive market share. The leaked files of China Zhenhua Data Information Technology with suspected connections with the Ministry of State Security intelligence service reveal that it has collected data on more than two-million prominent individuals worldwide including 10,000 Indians using AI-enabled algorithm.[20]

Controlling Influencers

Chinese firms have courted Hollywood's film industry to control the influencers. More than half of the ten best movies of 2019 selected by Time magazine were financed by Beijing-friendly firms, such as Tencent Pictures, Sunac Group, Shanghai Road Pictures Film and Television, Media Asia Film, and Bona Film Group. Chinese conglomerate Wang Jianlin, founder of *Dalian Wanda* and member of CPC acquired US AMC Entertainment for US$ 2.6 billion in May 2012, and Hollywood studio Legendary Entertainment and theatre Carmike Cinemas in 2016 raising heckles within the US policymakers. According to a report by PricewaterhouseCoopers, China became the world's largest cinema market in 2020, with box office revenue expected to jump to US$ 15.5 billion by 2023.[21] Thus, Chinese firms are seizing every opportunity to shape China's external image.

Media Remodelling

China has put its weight behind its foreign-language news outlets to regulate the narratives. In December 2016, CCTV (the state television broadcasting

news service), rebranded itself as China Global Television Network (CGTN). It broadcasts six channels in English, Arabic, French, Russian, and Spanish with reporting teams in more than 70 countries. *Xinhua*—the Party's primary news agency—has almost 200 foreign bureaus;[22] while *China Daily* and *Global Times* publish English language editions. In March 2018, CCTV, CRI, and China National Radio were merged to form the China Media Group, also called Voice of China, led by the Propaganda Department of the Central Committee of the CPC.[23] China Radio International broadcasts 392 hours of programming each day in almost 38 languages from 27 overseas bureaus.[24] The November 2015 *Reuters* investigation reports show that the media firms also covertly run influence operations through more than 30 radio stations in 14 countries through front companies. On 15 December 2019, the code of ethics legislated for the Chinese journalists makes it clear to them to "safeguard the political and the cultural security of the country" besides ensuring social stability.[25] Hence, the domestic media in China is the CPC's key mouthpiece.

Education Exchanges

China has more than 541 Confucius Institutes spread across six continents and affiliated with China's ministry of education mirroring cultural associations like the UK's British Councils, but it partners with universities.[26] Broader concerns about improper influence over teaching and research, industrial and military espionage surveillance prompted the US to enact Foreign Influence Transparency Act in March 2018 to regulate the funding in the US academic colleges. China has tried to improve the ranking of its institutions like Peking University and Tsinghua University as it helps in gaining access and controlling research. Chinese Students and Scholars Associations (CSSA) have been involved in promoting party works and reporting against the dissidents within the domestic and foreign universities. They are guided by the CPC members at the embassies.[27]

Economic Inducement and Ambushes

China has used BRI as a platform to showcase its economic prowess to the beleaguered nations across the world. The whole attempt is to create client state and support for the Chinese model of governance. It also aggressively looked at acquiring economic stakes in successful businesses across the world given the economic meltdown post-COVID outbreak. The large stake acquisition in India's financial bank prompted India to review its Foreign Direct Investment policy in April 2020.[28]

Influence Operations Stake Holders

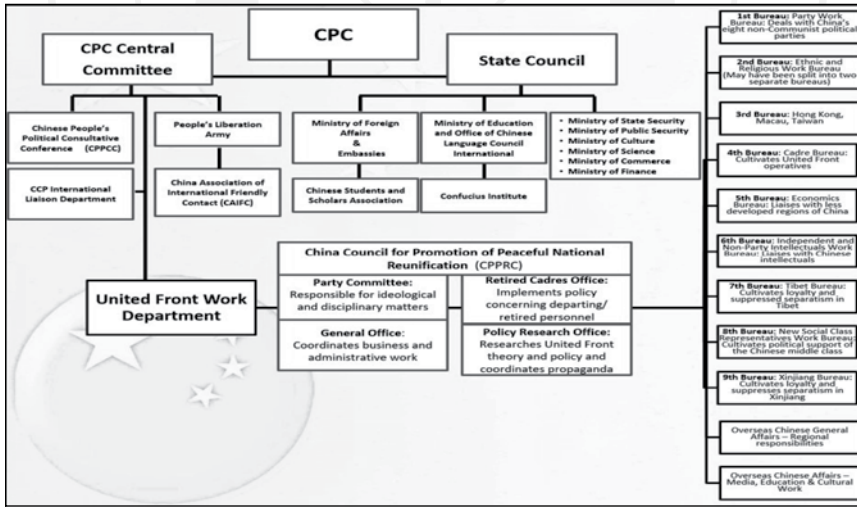
China's international influence activities groups are the External Propaganda Leading Group, which has a dual bureaucratic identity as the State Council Information Office; the Central Committee Propaganda Department; the Central Committee UFWD; the Central Committee Foreign Affairs Commission; and the Central Committee Education Leading Small Group. Although bureaucratically ranked slightly lower, the Ministry of Culture and Tourism, the Ministry of Education, the newly created Voice of China, and the *Xinhua News Agency* all exercise policy formulation and oversight roles in their functional domains. The two major players in China influence operations are the UFWD and the PLA Strategic Support Force (PLASSF).

UFWD-China's Magic Weapon

UFWD coordinates influence operations related to the management of potential opposition groups inside China and is now geared for important foreign influence mission too. Xi Jinping has energised a century-old organisation by adding almost 40,000 new UFWD cadres in first few years of his Presidency[29] and established a leading small group on UFWD with himself at its head, signifying a direct line of command from CPC Politburo to UFWD. The UFWD has been actively involved in implementing the Chinese 'three warfares'

strategy in concert with the Central Military Commission (CMC) and Ministry of State Security. It looks deeply into the fault lines and has invested in social engineering using cyber tools, political subversion, and supporting anti-national elements. The surreptitious ploy also aims to instigate the neighbours of country in dispute with China. It can be seen by browsing the credentials of Chinese ambassadors posted to South Asian countries. Nong Rong, Ambassador to Pakistan; Li Jiming the current representative in Bangladesh; and former Chinese Ambassador to Sri Lanka Cheng Xueyuan all have links with the UFWD. Even the Chinese Ambassador in Nepal Hou Yonqi was Director, Department of External Security Affairs in 2012-2013, and has been at the forefront of keeping the communist movement in Nepal together and engineering conflict with India on border issues.[30]

Figure 1: United Front Works Department (UFWD) Bureaus and Affiliations



Source: Adapted from Cole (2017).[31]

PLASSF-New Information Warfare Force

Military strategists in China have laid out a "unified field theory" of war in which the kinetic dimension is no longer dominant.[32] The articulation on "Unrestricted Warfare" or "wars beyond rules" by Senior Colonels from the PLA, Qiao Liang and Wang Xiangsui simply illustrate that warfare has extended beyond the preserve of the military and civil-military fusion is the trend. Dual-use technologies like AI, 5G, robotics, unmanned systems and sensors, have been associated with economic development as well as security management. Mega-corporations' participation in the development of dual-use technologies has aggravated security concerns. China is enamoured by the big tech-giants in the US who are not only commercially engaged across the world but are intricately linked to the Pentagon. It feels that the information domain is a strategic space created by the western world to undertake influence operations by shaping the opinion and occupying the cognitive space of leadership and society.

The colour revolution and the Hong Kong 2019 protests have reconfirmed their hypothesis. Strategy to influence has emerged through synchronous effort provided by space, cyber and electromagnetic technologies. China realises that besides strengthening its economy and securing its territorial sovereignty, it has to secure these new emerging sovereign domains through unlimited ways and calibrated asymmetrical response for effective control followed by a recalibrated response to retain the influence. The reforms ushered in 2016 by Xi was with an intent to restructure and rebalance the PLASSF to meet the demands of safeguarding China's national security in the new era. The cyber tools provide an excellent means for manipulation and narrative insertion. The CPC has entrusted psychological and public opinion operations with the task of influencing political, economic and intellectuals in other countries and the objective of systematic penetration into systems of targeted country to the Network Systems Department (NSD) of the PLASSF while the strategic information support has been given to the Space Support Department (SSD).

NSD-The Cyber Force

The NSD dovetailed computer network attack handled by the GSD Fourth Department (4PLA), the GSD Informatisation Department handling the PLA counter-network defence operations and the cyber-espionage elements of the former 3PLA except for the PLA's counter-network defence mission, which remains with the JSD Information Support Base under its Network Security Defence Centre.[33] NSD retains the headquarters of the former 3PLA along with its twelve bureau-centric structure.[34] These bureaus are tasked to collect intelligence by targeting the government, defence, research and technology sectors, including the specific targeting of space, aerospace, and communications. Cyber espionage remains the low-cost high yield approach by China to acquire economic and technological know-how to bridge the capability gap in niche technologies and enable wealth creation besides image build-up.

SSD-The Space Force

The SSD has consolidated almost all aspects of PLA space operations including space launch, telemetry, tracking, control and space intelligence, surveillance and reconnaissance measures. The Aerospace Reconnaissance Bureau of PLA Second Department (2 PLA) has been transferred to SSD for strategic intelligence collection while the balance 2 PLA has been merged with the Joint Staff Division (JSD) for carrying out human intelligence, signals intelligence and management of clandestine agents and military attaches. According to 2019 US DIA report, China views space superiority as part of its ability to control the information sphere. It aims to replace the GPS in BRI countries with its own *BeiDou* Satellite system. It has even tested anti-satellite weapons and directed energy weapons as part of non-nuclear deterrence capability. According to *2013 Science of Military Strategy*, the three critical components to achieve the goals of deterrence are 'magnitude of deterrence, determination, and information conveyance.' The methods to be employed intend to

'increase the number of strategic options and enhance strategic flexibility to prevent or win war, secure stability and defend interests.'

Building Situational Awareness

Influence operations ride on the wealth of intelligence inputs. Situational awareness is something that China relies on to build response options. It has used surveillance technology infusion in governance to secure internal stability. Yet, the gap exists at the global level, which it needs to bridge or create an asymmetric capability to block the access to information to technologically superior powers. PLA is aware of the US Strategic Command outreach based on the transparency provided by the US Global Information Grid and ability of the US to target critical infrastructure within and outside China. Computing, storage and communication survivability is therefore an essential imperative for China. Strengthening space situational awareness and freedom to operate and communicate is part of situational awareness developmental overdrive by the PLA. These initiatives include unhackable ISR systems. Few initiatives undertaken by China are as follows:

Early Warning System

China Electronics Technology Corporation (CETC) has been at the helm of putting China on the map of high-end radar besides laying the foundation of missile defence and development of laser and nuclear EMP systems as part of the nuclear missile defence system.[35] Long-range phased array radars (LPAR) in P Band with 4000 km range helps in ballistic missile tracking.[36] To counter the stealth bombers, it has developed anti-stealth radar-like SLC-7 and YLC-8B. To ensure the survivability of radar systems to electronic warfare measures, it has developed jamming resistant JY 27 A VHF active electronically scanned array (AESA) radars that form the backbone of China's PLAAF and PLAN airborne early warning and control (AEW&C) systems. The quantum radar technology by CETC makes stealth technology

redundant as it allows better discrimination properties.[37] The ground-penetrating radar, Eagle Eye-A, built under China Aerospace Science and Industry Corporation is capable of detecting soil, pipelines and even tunnels as deep as six meters underground. Its integration of AI system and *BeiDou* satellite navigation and GPS systems allows the efficiency of auto-detection and high precision positioning of underground targets.[38]

Unmanned Surveillance System

The JY-300 (*Tian Shao*) which has a range of more than 1,000 km and a practical ceiling of more than 5,000 metres, is the world's first unmanned Airborne Warning and Control System (AWACS) aircraft. It integrates radars with the airframe, which means radar antennae are part of the craft's skin.[39] It is likely to have fielded stealthy Shendiao for early warning. Morning Star and Rainbow are being developed for persistent surveillance for months as launch on-demand systems thus providing an alternative to satellites with greater flexibility.[40]

Space System

China has developed a robust architecture of space systems to support its strategic situational awareness. Though there is a large difference in holding of satellites between China and the US, the Chinese ranks second after the US in terms of the number of satellites that are currently operational. These satellites provide a wide range of sensors that include ELINT, electro-optical (EO) sensors, synthetic aperture radar (SAR), staring camera, stereoscopic imagers, and hyperspectral, among others.

Maritime Surveillance

The PLAN, with its global commitment and competition along its island chains, recognises the importance of a maritime strategic

early warning system. The PLAN maritime surveillance capabilities are through the sea- and space-based systems, ranging from the launch of satellites dedicated to that mission to the construction of an 'underwater great wall' of sensors, augmented by a range of underwater sensors and unmanned and autonomous underwater vehicles. China's militarisation of the South China Sea has involved the placement of a network of radars on its various installations on features, such as Fiery Cross, Subi Reef, and Mischief Reef. These radars may contribute to early warning, signals intelligence, and even stealth detection, including via high-frequency arrays.

Laser Surveillance System

China has heavily invested in the use of Lidar (a portmanteau of light and radar), AI and 5G technologies to synergise detection and dissemination of the images and intelligence. Lidar uses ultraviolet, visible, or near-infrared light to image objects. It can be used with a wide range of targets, including non-metallic objects, rocks, rain, chemical compounds, aerosols, clouds and even single molecules. However, it has an atrophying effect in fog and murky water. China's new satellite 'Project Guanlan' which means 'watching the big waves' launched in May 2019 at the Pilot National Laboratory in Qingdao uses high-powered lasers to spot objects deep underwater up to 500 metres. It is capable of scanning an area of around 100 km on land. When used alongside microwave radar, it can scan and identify surface movement and also penetrate through the foliage. A narrow laser beam can be used to map physical features with very high resolution. It brings transparency both on land and sea and exposes weapon systems like submarines.[41]

Modernising Command and Control Network

The PLA intends achieving networked C4ISR and counter-C4ISR capabilities that enable systems and subsystems to kinetically or non-

kinetically defeat or paralyse the enemy's decision support systems. China's advances in space-based capabilities, drone technology, and information processing could provide sufficient means to provide situational awareness and targeting quality data to overseas Chinese forces anywhere in the world by 2030 or 2035.[42] 5G has been developed by Chinese defence academics and engineers to improve battlefield communications with faster and more stable information transmission, increasing the timeliness and integration of information. The increased bandwidth could help the PLA to 'intelligentise' its military.

Conclusion

Situational awareness and influence operations go hand in gloves. In future, China could employ more integrated strategic early warning systems. While the PLA has made rapid stride in technology infusion, but it is saddled with legacy equipment, and integration of these systems is a challenge. The efforts of the Chinese defence industry, particularly those of CETC, in providing improved datalinks for real-time sharing and integration of intelligence for enhanced situational awareness have matured. PLASSF, as the new informational umbrella and custodian of the situational awareness engine, is responsible for facilitating information transmission, processing, and distribution, and for supporting early warning. Devising hack-free algorithm is an area China aims to have information parity with the US and information dominance against countries with which it has disputed. It is rapidly exploring the fields of quantum technologies to provide resilience to its communication, sensor technologies and space exploration.

Pandemic has created chaos of an unprecedented kind. The nations struggling to contain the pandemic with limited capabilities are finding themselves overwhelmed by the enormity of the crisis. However, amidst this chaos, China finds itself securely perched having braved the initial brunt of contagion attack, and now it is focussed to advance its agenda

of influence and image preservation. The likely Chinese strategy of handling this crisis may be akin to 'influence-beachhead' by China into other countries' strategic interests. The pandemic has thrown open major fault lines across the world which are being carefully studied by China and will form part of new developing warfare—virtual societal warfare with psychological impacts vectored in leadership choice of response.

Notes

1. Wang Xiangwei (2020), "*Amid China's coronavirus success, low marks for local 'social credit' apps," South China Morning Post,* September 12, 2020. Available online at https://www.scmp.com/week-asia/opinion/article/3101221/amid-chinas-coronavirus-success-low-marks-local-social-credit, accessed on September 13, 2020.
2. World Health Organization (2020), "WHO Coronavirus Disease (COVID-19) Dashboard," November 1, 2020. Available online at https://covid19.who.int, accessed on November 1, 2020.
3. Dan Sabbagh and Heather Stewart (2020), "*Mike Pompeo attacks WHO in private meeting during UK visit*," The Guardian, July 21, 2020. Available online at https://www.theguardian.com/world/2020/jul/21/mike-pompeo-attacks-who-in-private-meeting-during-uk-visit, accessed on September 11, 2020.
4. World Health Organization (2020), "*WHO Timeline - COVID-19,"* April 27, 2020. Available online at https://www.who.int/news-room/detail/27-04-2020-who-timeline---covid-19, accessed on September 11, 2020.
5. "Full Text: China's National Defense in the New Era," *Xinhuanet*, July 24, 2019. Available online at http://www.xinhuanet.com/english/2019-07/24/c_138253389.htm, accessed on September 14, 2020.
6. National Intelligence Council (2008), "*Global Trends 2025: A Transformed World,"* November 2008. Available online at https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2025_Global_Trends_Final_Report.pdf, accessed on September 15, 2020.
7. Iris Deng (2020), "Coronavirus: China tightens social media censorship amid outbreak," *South China Morning Post*, February 6, 2020. Available online at https://www.scmp.com/tech/policy/article/3049342/coronavirus-china-tightens-social-media-censorship-amid-outbreak, accessed on September 15, 2020.
8. Sam Cooper (2020), "*United Front groups in Canada helped Beijing stockpile coronavirus safety supplies*," Global News, April 30, 2020. Available online at https://globalnews.ca/news/6858818/coronavirus-china-united-front-canada-protective-equipment-shortage/, accessed on September 15, 2020.

9. Alexander Bowe (2018), "China's Overseas United Front Work: Background and Implications for the United States," US-China Economic and Security Review Commission, August 24, 2018, p. 22. Available online at https://www.uscc.gov/sites/default/files/Research/China's%20Overseas%20United%20Front%20Work%20-%20Background%20and%20Implications%20for%20US_final_0.pdf, accessed on September 17, 2020.
10. Shirley Zhao (2020), "China's Mobile Carriers Lose 21 Million Users as Virus Bites," *Bloomberg*, March 23, 2020. Available online at https://www.bloomberg.com/news/articles/2020-03-23/china-s-mobile-carriers-lose-15-million-users-as-virus-bites, accessed on September 17, 2020.
11. Hussein Askary (2020), "The role of BRI in building a global healthcare system," *Global Times*, May 16, 2020. Available online at https://www.globaltimes.cn/content/1188547.shtml, accessed on September 17, 2020.
12. Nectar Gan, Caitlin Hu and Ivan Watson (2020), "Beijing tightens grip over coronavirus research, amid US-China row on virus origin," *CNN*, April 16, 2020. Available online at https://edition.cnn.com/2020/04/12/asia/china-coronavirus-research-restrictions-intl-hnk/index.html, accessed on September 17, 2020.
13. "Report: China's fight against COVID-19 (full text)," *China Daily*, April 21, 2020. Available online at https://covid-19.chinadaily.com.cn/a/202004/21/WS5e9e2c62a3105d50a3d17880.html, accessed on September 17, 2020.
14. "China's national library launches 'collective memory bank' to document coronavirus outbreak stories," *CGTN*, April 25, 2020. Available online at https://news.cgtn.com/news/2020-04-25/China-s-national-library-launches-project-to-record-COVID-19-stories-PYZLBm4vZu/index.html, accessed on September 18, 2020.
15. United Nations Secretary-General (2020), "Statement by the Secretary-General on the World Health Organization," April 14, 2020. Available online at https://www.un.org/sg/en/content/sg/statement/2020-04-14/statement-the-secretary-general-the-world-health-organization, accessed on September 18, 2020.
16. National Counterintelligence and Security Center (2018), "Foreign Economic Espionage in Cyberspace," p. 6. Available online at https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf, accessed on September 18, 2020.
17. Hogan Lovells (2019), "China Marches into Cybersecurity Classified Protection 2.0," May 31, 2019. Available online at https://www.lexology.com/library/detail.aspx?g=87dbca80-c278-4463-9a60-dd12442cd816, accessed on September 20, 2020.
18. Louise Matsakis (2020), "How WeChat Censored the Coronavirus Pandemic," *Wired*, August 27, 2020. Available online at https://www.wired.com/story/wechat-chinese-internet-censorship-coronavirus/, accessed on September 20, 2020.
19. Tony DeGennaro (2020), "10 Most Popular Social Media Sites in China (2020 Updated)," Dragon Social, June 30, 2020. Available online at https://www.dragonsocial.net/blog/social-media-in-china/, accessed on September 20, 2020.
20. Praveen Swami (2020), "Unlike Pegasus, Zhenhua lacks prowess to spy; China's claims on data harvesting a smokescreen, exposes its weaknesses," *Firstpost*, September 14, 2020. Available online at https://www.firstpost.com/world/unlike-pegasus-zhenhua-

lacks-prowess-to-spy-chinas-claims-on-data-harvesting-a-smokescreen-exposes-its-weaknesses-8815081.html, accessed on September 20, 2020.

21. See "Global Entertainment & Media Outlook 2016-2020". Available online at https://www.pwc.com/gx/en/entertainment-media/pdf/outlook-cinema-article-2016.pdf, accessed on September 20, 2020.
22. Albert, E. (2018, February 09). *China's Big Bet on Soft Power,* op.cit.
23. Chapter Eighteen, Part II: The Chinese Communist Party's Global Ambitions (UPDATED)," *The Epoch Times*, June 2, 2020. Available online at https://www.theepochtimes.com/chapter-eighteen-the-chinese-communist-partys-global-ambitions-part-ii_2822429.html, accessed on September 20, 2020.
24. Ibid.
25. Zou Shuo (2019), "Revised code of ethics for journalists released," *China Daily*, December 16, 2019. Available online at https://global.chinadaily.com.cn/a/201912/16/WS5df6ed76a310cf3e3557e5c6.html, accessed on September 23, 2020.
26 For details see Pratik Jakhar (2019), "Confucius Institutes: The growth of China's controversial cultural branch," *BBC News*, September 6, 2019. Available online at https://www.bbc.com/news/world-asia-china-49511231, accessed on September 15, 2020.
27. Zou Shuo (2019), "Revised code," n. 25.
28. Ministry of Commerce & Industry, Government of India (2020), "Government amends the extant FDI policy for curbing opportunistic takeovers/acquisitions of Indian companies due to the current COVID-19 pandemic," *Press Interest Bureau*, April 18, 2020. Available online at https://pib.gov.in/newsite/PrintRelease.aspx?relid=202359, accessed on September 20, 2020.
29. Ibid.
30. Shishir Gupta (2020), "China sends hardcore ambassadors to South Asia to push BRI and undermine India," *Hindustan Times*, September 14, 2020. Available online at https://www.hindustantimes.com/world-news/china-sends-hardcore-ambassadors-to-south-asia-to-push-bri-and-undermine-india/story-Oz8Aakf28IQJqHB1uJKOQL.html, accessed on September 20, 2020.
31. J. Michael Cole (2017), "China Seeks Vicious Circle of Violence through United Front Activities in Taiwan," *Taiwan Sentinel*, September 26, 2017. Available online at https://sentinel.tw/china-violence-ufw-tw/, accessed on September 23, 2020.
32. Rajiv Narayanan (2018), *PLA Reforms of Xi Jinping in an Era of Assertive Diplomacy*, New Delhi: Vij Books India Pvt Ltd, p. 16.
33. Ibid.
34. Joe McReynolds and John Costello (2019), "China's Strategic Support Force : A Force for a New Era," in Arthur S. Ding, et al. (eds.) *Chairman Xi Remakes the PLA*, Washington DC: National Defense University Press., pp. 460-461.
35. Elsa B. Kania (2019), "China's Strategic Situational Awareness Capabilities," On the Radar, July 29, 2019, p. 2. Available online at https://ontheradar.csis.org/issue-briefs/china-situational-awareness/, accessed on September 20, 2020.
36. Ibid.

37. "China can use quantum radar technology to monitor high-speed aircraft from space," *Global Times*, June 15, 2018. Available online at http://military.china.com/zxjq/11139042/20180618/32546024.html, accessed on September 18, 2020.
38. "China develops AI radar for underground space detection in cities," *Xinhuanet*, November 28, 2012. Available online at http://www.xinhuanet.com/english/2018-11/28/c_137637800.htm, accessed on Septemebr 18, 2020.
39. Zhao Lei (2018), "Flying radar' is first early-warning drone," *China Daily*, November 10, 2018. Available online at http://www.chinadaily.com.cn/a/201811/10/WS5be6173ba310eff303287c2c.html, accessed on September 18, 2020.
40. Liu Zhen (2018), "Chinese solar-powered drone Morning Star spreads its wings in successful test flight," *South China Morning Post*, October 31, 2018. Available online at https://www.scmp.com/news/china/military/article/2171081/chinese-solar-powered-drone-spreads-its-wings-successful-test, accessed on September 17, 2020.
41. Phoebe Weston (2018), "US subs would be sitting ducks for new Chinese 'Death Star' laser satellite that will be able spot them 1,600ft below the surface," *Mail Online*, October 1, 2018. Available online at https://www.dailymail.co.uk/sciencetech/article-6226683/Chinas-new-spy-satellite-use-LASERS-light-ocean.html, accessed on September 18, 2020.
42. Cortez A. Cooper III (2018), *PLA Military Modernization: Drivers, Force Restructuring, and Implications*, Santa Monica, CA: RAND Corporation. Available online at https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT488/RAND_CT488.pdf, accessed on September 20, 2020.