CENTRE FOR LAND WARFARE STUDIES

ISSUE BRIEF

No. 323 January 2022

China's Developing Cyber Warfare Capabilities

Major General PK Mallick, VSM (Retd) held the Chief of Army Staff Chair of Excellence at CLAWS. The General is an Electronics and Telecommunication Engineering graduate from BE College, Shibpore, MSc (Defence Studies) from Madras University, M.Tech from IIT, Kharagpur, MMS from Osmania University and M. Phil from Madras University. He was commissioned in the Corps of Signals of Indian Army. The Officer has interest in Cyber Warfare, Electronic Warfare, SIGINT, Technology and Strategic Affairs. His last posting before retirement was Senior Directing Staff (Army) at National Defence College, New Delhi.

Introduction

Chinese President Xi Jinping has made it clear that China's objective is to emerge as a 'cyber superpower'. China wants to be the world's largest nation in cyberspace and also one of the most powerful. The information technology revolution has produced both momentous opportunities and likely vulnerabilities for China. China is home to the largest number of netizens in the world. It hosts some of the world's most vibrant and successful technology companies. It is also a major victim of cybercrime.

Key Points

- PLA believes that future wars will be decided by the side that is more capable to generate, gather, transmit, analyse and exploit information.
- China has been conducting cyber operations against India for a long time.
- PLA differs considerably from its Western counterparts in its approach to cyber and network operations. It recognises the importance of a digital battlefield.
- The PLA is actively looking at and experimenting with new concepts and capabilities to leverage artificial intelligence to improve its combat power and deterrence.
- The Strategic Support Force is responsible for collecting and managing technical intelligence from cyber and space assets as well, supporting joint operations and carrying out attacks against the adversary's command network. SSF seeks to integrate Electronic Warfare with cyber, space and psychological warfare.

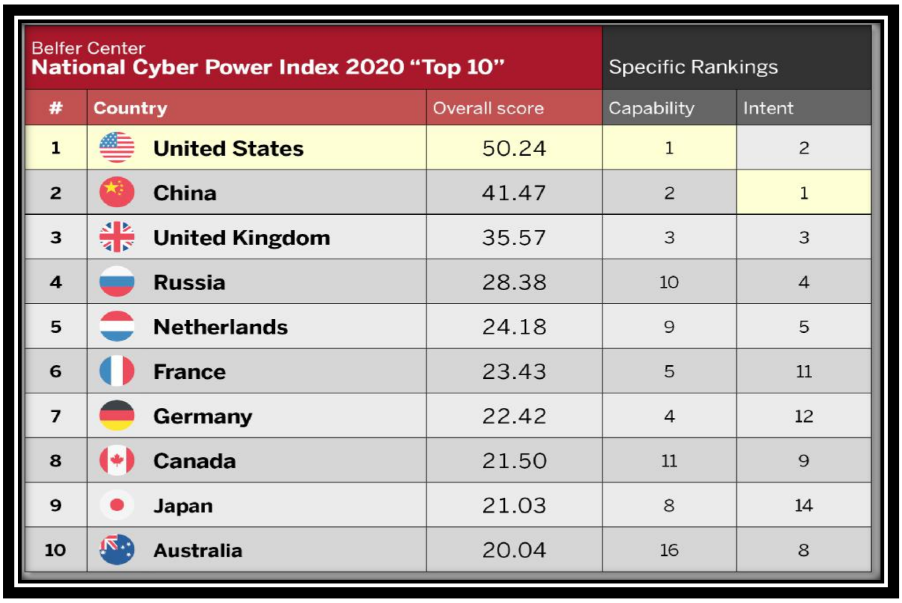
The "comprehensive national power"—the measurement of a state and society's power, which includes military, political, economic, diplomatic, science & technology and cultural components—is now measured in terms of information. China has emerged as a cyber superpower. China possesses enormous economic and military capabilities that augment

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with national security and conceptual aspects of land warfare, including conventional & sub-conventional conflict and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.
Website: www.claws.in Contact us: landwarfare@gmail.com

its overall national power. It is actively pursuing today's emerging technologies such as big data, robotics, quantum computing, 5G technology and Artificial Intelligence (AI). This would enable China to flourish in the new industrial revolution that is presently unfolding. China’s cyber power constitutes a critical component of its ‘comprehensive national power’.

Harvard Kennedy School of Government in a study of cyber power of various countries has ranked China as the second most powerful nation after US. (see **Table 1**)

Table 1: 2020 NCPI Rankings



Belfer Center
National Cyber Power Index 2020 “Top 10”

			Specific Rankings	
#	Country	Overall score	Capability	Intent
1	United States	50.24	1	2
2	China	41.47	2	1
3	United Kingdom	35.57	3	3
4	Russia	28.38	10	4
5	Netherlands	24.18	9	5
6	France	23.43	5	11
7	Germany	22.42	4	12
8	Canada	21.50	11	9
9	Japan	21.03	8	14
10	Australia	20.04	16	8

Source: Julia Vooet al, National Cyber Power Index 202, Harvard Kennedy School of Government, September 2020 available at: https://www.belfercenter.org/publication/national-cyber-power-index-2020

The International Institute for Strategic Studies (IISS) published a report titled ‘Cyber Capabilities and National Power: A Net Assessment’. IISS has done a qualitative assessment of the cyber capabilities of 15 major countries. The report analyses the cyber capabilities of the US, the UK, China, Canada, Russia, North Korea, Japan, Israel and India among others. It puts US. in first tier and China as second-tier cyber power along with Russia and five US allies Australia, Canada, UK, France and Israel.

The report estimates China’s cyber power as: [1]

- Conducts large scale cyber operations abroad, aiming to acquire intellectual property, achieve political influence, carry out state-on-state espionage and position capabilities for disruptive effect in case of future conflict.
- Established the world’s most extensive cyber enabled domestic surveillance and censorship system.
- Core cyber defences remain weak compared with those of the US; cyber resilience policies for its critical national infrastructure are only in the early stages of development.
- Given its growing industrial base in digital technology, China is best placed to overtake US in National Cyber Power Index.

Cyber Exploitation Activities

The People’s Liberation Army (PLA) believes that, with the rise of Information Age, future wars will occur in the information domain. Wars will be decided by the side who is more capable to generate, gather, transmit, analyse and exploit information.

Informationalised warfare blurs the line between peacetime and wartime. A nation in the information age cannot wait for the hostilities to break out to collect intelligence, carryout influence operations, develop anti-satellite systems or design computer software weapons. Such warfare will include activities in peacetime, aimed at civilian and commercial entities, as well as operations against adversary’s military systems in war.[2]

Chinese hackers have carried out cyber industrial espionage at high-technology and advanced manufacturing companies of emerging industries, such as aerospace, biotechnology and semiconductors in the US, Europe, Japan and Southeast Asia. Hackers were interested in firms' negotiation strategies and financial information in the energy, banking, law, and pharmaceutical sectors. Former NSA Director Keith Alexander said that, the Chinese operations enabled the "greatest transfer of wealth in history”.[3]

The Washington Post reported that Chinese hackers stole critical files related to missile defence, including "the advanced Patriot missile system,…an Army system for shooting down ballistic missiles,....and the Navy's Aegis ballistic missile defense system". The hackers also gathered information on planes, helicopters, and ships, including "the F/A-18 fighter jet, the V-22 Osprey, the Black Hawk helicopter and the Navy's new Littoral Combat Ship, which is designed to patrol waters close to shore".[4] These were the weapons on which the US would rely in a fight with China. These vulnerabilities were now exposed for China to study.

China's Ministry of State Security (MSS) has come out as a highly skilled player in cyberspace, demonstrating increasing sophistication and operational security while undertaking a global cyber espionage campaign for economic, political and strategic purposes. China can use its MSS to support political and geopolitical objectives in peacetime, including continued targeting of countries involved in territorial disputes in the East and South China seas. China's emergence as a cyber power will have critical implications for the future of security and stability of the Asia-Pacific and beyond.

GhostNet. China has been conducting cyber operations against India for a long time. One of the examples is the GhostNet episode. Between June 2008 and March 2009, the Information Warfare Monitor conducted an investigation focused on allegations of Chinese cyber espionage against the Tibetan community. GhostNet penetrated computer systems containing sensitive and secret information at private offices of the Dalai Lama and other Tibetan targets.

GhostNet infected 1,295 computers in 103 countries. Almost a third of the targets infected by GhostNet included the Ministries of Foreign Affairs of Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados and Bhutan; Embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany and Pakistan; the ASEAN (Association of Southeast Asian Nations) Secretariat, SAARC (South Asian Association for Regional Cooperation) and the Asian Development Bank; news organizations; and an unclassified computer located at NATO headquarters.

These activities still continue. The latest example being of 28 February 2021, wherein The New York Times (NYT), based on analysis by a US based private intelligence firm, reported that a Chinese entity penetrated India's power grid at multiple load dispatch points. Chinese malware intruded into control systems that manage electric supply across India, along with high voltage transmission substation and a coal-fired power plant.

The Chief Operating Officer of Recorded Future (an American cyber security company) said that, the Chinese state-sponsored group, which the firm named RedEcho, "has been seen to systematically utilize advanced cyber intrusion techniques to quietly gain a foothold in nearly a dozen critical nodes across the Indian power generation and transmission infrastructure".[5] In this report, details of a campaign conducted by RedEcho, targeting the Indian power sector has been analysed. It is believed that the group was responsible for Mumbai power outage on 13 October 2020 that lasted for two hours.

Concepts of Warfare

The PLA differs considerably from its Western counterparts in its approach to cyber and network operations. PLA does not use the word *cyber* as extensively as the West. They perceive everything related to cyber developments as the process as informationisation or informatisation. Rather than seeing cyber power as a distinct capability like air, land, sea and space, PLA's planners view cyber and network operations as occurring in an "information domain". This domain encompasses network, psychological and media operations, as well as electronic warfare.[6]

PLA strategists believe that 'network-electronic operations' will be critical to combat effectiveness as new means of warfare. Cyber and network operations can be an 'indispensable method for deterring powerful enemies' with the potential to enable 'winning without fighting' under certain conditions.

China's 2015 Defense White Paper highlighted that the PLA should be able to fight and win 'informationized local wars'. The report stated: "integrated combat forces will be employed to prevail in system v/s system [i.e. C4ISR] operations featuring information dominance, precision strikes and joint operations" to meet the offensive and defensive operational requirements of modern warfare.

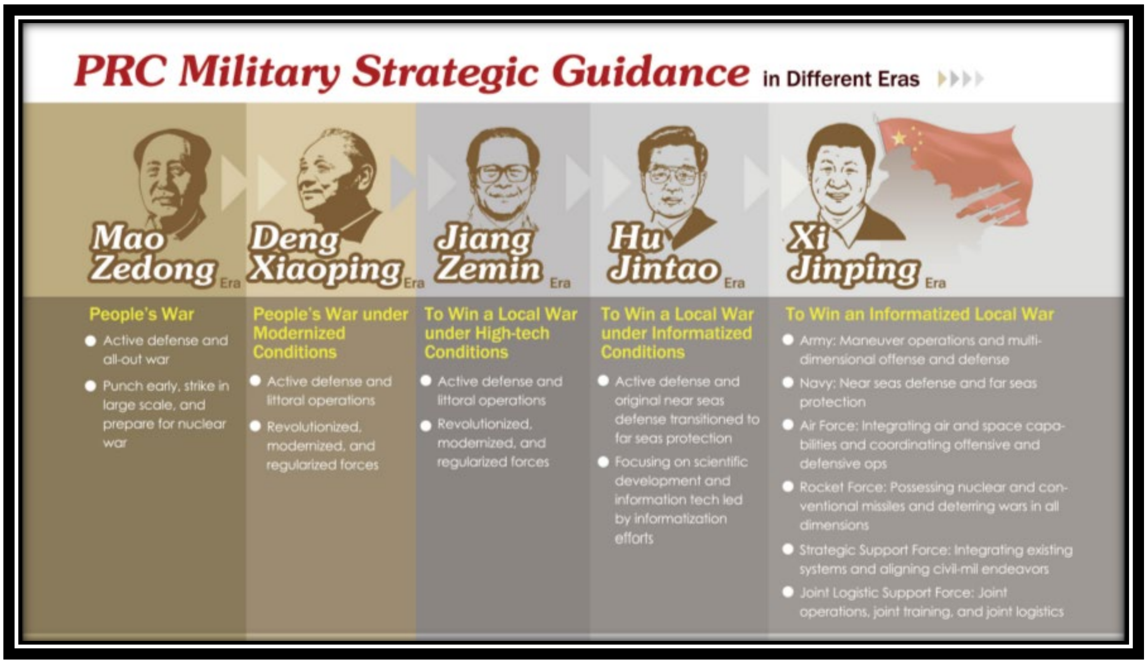
The PLA's Current View on Warfare. The 'Science of Strategy' published by the NDU in 2017 states that, wars will represent a "system of systems confrontation". The PLA envisions warfare conducted on tangible and intangible battlefields. The tangible battlefield includes land, sea, air and space domains, while the intangible battlefield includes the electromagnetic spectrum, cyber, space and psychological cognition. Operations are characterised as highly dynamic, decentralised, blurring lines between the front & rear areas and rapid transitions between offence and defence. Characteristics include non-contact, non-linear and asymmetric operations.[7]

According to Elsa Kania and John Costello, "Informatization is the core of everything the PLA wants to accomplish— from high-tech missions in space and cyberspace, to long-range precision strike, ballistic missile defence and naval deployments abroad, the ability to transmit, process and receive information is a vital enabler".[8] This theory incorporates thinking and strategy informed by numerous geopolitical and technological developments over the past 25 years. The PLA recognises the importance of the digital battlefield. China's efforts to 'informatise' the PLA extends to cultivating and integrating emerging technologies like quantum computing and artificial intelligence.

Winning Informationalised Local Wars. As PLA leaders recognise the importance of technology, professionalisation and military hierarchy, Chinese military theory has been moving away from traditional Marxist-Leninist and Maoist theory. The PLA, however, remains staunchly Communist and views its modern theories as an evolution of People's War. People's War in Conditions of Informationization, as per PLA, is a modern adaptation of The Art of War and People's War. The 'concept of active defence' is its centrepiece, and deception and political willpower are the most important elements of a successful military campaign.

The diagram below displays the timeline of the evolution of People's War concept under different Chinese leadership.

Figure 1: Evolution of PRC Military Strategic Thought



PRC Military Strategic Guidance in Different Eras

Mao Zedong Era

People's War

- Active defense and all-out war
- Punch early, strike in large scale, and prepare for nuclear war

Deng Xiaoping Era

People's War under Modernized Conditions

- Active defense and littoral operations
- Revolutionized, modernized, and regularized forces

Jiang Zemin Era

To Win a Local War under High-tech Conditions

- Active defense and littoral operations
- Revolutionized, modernized, and regularized forces

Hu Jintao Era

To Win a Local War under Informatized Conditions

- Active defense and original near seas defense transitioned to far seas protection
- Focusing on scientific development and information tech led by informatization efforts

Xi Jinping Era

To Win an Informatized Local War

- Army: Maneuver operations and multi-dimensional offense and defense
- Navy: Near seas defense and far seas protection
- Air Force: Integrating air and space capabilities and coordinating offensive and defensive ops
- Rocket Force: Possessing nuclear and conventional missiles and deterring wars in all dimensions
- Strategic Support Force: Integrating existing systems and aligning civil-mil endeavors
- Joint Logistic Support Force: Joint operations, joint training, and joint logistics

Source: ROC National Defense Report 2021 [9]

Network Warfare. Network warfare is the aspect of information warfare involving the range of activities that occur within networked information space, as the two sides seek to reduce the effectiveness of the adversary's networks while preserving one's own. The purpose of network warfare is to establish "network dominance”. When one has "network dominance”, the full range of one's networks (not just computer networks) can operate smoothly and the information on those networks is safeguarded while being rapidly moved and applied. In contrast, an adversary's networks are prevented from doing the same. Some of the networks that are integral to network warfare include the command & control network, intelligence information network and air defence network.

The Chinese campaign design includes detailed planning for protecting networks in physical (personnel, equipment, and facilities) and non-physical (cyber, electromagnetic, informational) domains. Primary targets will be leadership, C2 nodes, sensors and information hubs.

Network warfare is also a focus area in PLA's big data program, with research agendas across the force prioritising network security and cyber defence technologies. Moreover, PLA restructuring and modernisation efforts go beyond network defence to encompass broader cyber warfare applications designed to accomplish information superiority missions and to enhance operations in other warfighting domains.

Integrated Network and Electronic Warfare (INEW). [10] The future local wars under informationalised conditions will see the merging of network and electronic warfare. The PLA defines the INEW concept which at times is translated as “network-electronic integration warfare”, as a form of information warfare where one implements information attacks against the enemy’s networked information systems through highly melded electronic warfare and network warfare.

According to the Chinese experts, in future conflicts, the electromagnetic spectrum will have a key influence upon the operation of network space, with network and electronic warfare organically linked, operating under a single unified direction. Network warfare will be affected by efforts aimed at dominating the electromagnetic spectrum. Neither electronic warfare nor network warfare alone can comprehensively disrupt that system-of-systems, but given the mutually supporting nature of the two different types of warfare in terms of attack concepts, attack methods and operating environments, they constitute a highly effective integrated attack methodology.

System Destruction Warfare

The PLA classifies all capabilities, ranging from ballistic missiles and fighter aircraft to special operations forces and cyber operators, as military systems. Each system has inherent strengths and weaknesses. System warfare involves:

- Bypassing enemy systems’ areas of strength and gaining a combat advantage by approaching them asymmetrically.

- Developing systems that excel at utilising apparent weaknesses in enemy systems, thus offsetting their strengths by undermining their ability to perform assigned missions.

The most common examples of system warfare are targeting networks instead of shooters, command and communication nodes instead of manoeuvre forces or sensors instead of aircraft. The PLA expands system warfare to include offensive cyber operations disabling air or seaport operations, diplomatic efforts undermining international alliances or special operation forces undermining civilian morale through covert operations.

To operationalise ‘systems destruction warfare’, the PLA has made significant progress towards waging informationalised war, modernising command & control network’s ability to transfer complex information rapidly, new space jamming & anti-jamming weapons and increasingly sophisticated cyber attack capabilities.

System destruction warfare has become a dominant driver behind PLA force structure decisions and modernisation priorities. It explains heavy Chinese investments in counter-battle network capabilities. The means to conduct “informationalised warfare" includes the use of electronic warfare, cyber, computer network attack, information operations, and deception to destroy the integrity of the adversary's battle network.The emphasis on systems destruction warfare also helps to understand the reasoning behind PLA's new Strategic Support Force, a system-of-systems organisation designed to integrate better space, cyber and electronic warfare capabilities into PLA operations.

During war, the PLA plans to build task-organised suites of capabilities designed to strike specific weak points of its opponent’s key systems. These suites of capabilities are called operational systems. Each operational system consists of five main subcomponents: the command system, the strike system, the information warfare system, the intelligence system and the support system.

At the tactical level, system warfare concentrates mostly on targeting high-value battlefield systems such as radars, command & communication nodes, field artillery and air defence systems. It can include selective armoured vehicles and critical logistics support means. Examples of tactical system warfare can be using heavy rocket artillery to defeat or destroy enemy radars and artillery systems, Electronic Warfare (EW) to suppress or neutralise enemy command and communication networks and deception operations to target enemy leadership’s situational understanding and state of mind.

The PLA's use of system warfare supports the development of several traditional military strategies, such as preclusion, isolation and sanctuary, throughout all domains and at all levels of war. Preclusion is attained by keeping enemy commanders and forces off balance through asymmetric means, such as deception and information warfare, while simultaneously denying use of wide geographic areas through long-range reconnaissance-strike capabilities. Isolation is achieved by manipulating communications between units or jamming, employing psychological warfare to confuse and segregate enemy units from one another, then rapidly manoeuvring to physically isolate them. Sanctuary is achieved through a mix of information warfare, protection, defensive planning and deception operations. Sanctuary includes safety from physical attack and enemy information operations.

Informatisation to Intelligentisation

China's military strategists anticipate a transformation in the form and character of conflict. This is evolving from today's "informatised" warfare to future "intelligentised" warfare. The PLA is actively looking at and experimenting with new concepts and capabilities to leverage artificial intelligence to improve its combat power and deterrence. These initial conceptual developments may influence future directions in PLA strategy, doctrine and weapons development. Chinese defence academics and military strategists are creating ideas and theories of 'intelligentised operations,' seeking to determine new mechanisms for victory. Intelligentised Warfare incorporates emerging technologies like decentralised computing, data analytics, quantum computing, artificial intelligence and unmanned or robotic systems into the PLA's conceptual framework. The PLA is studying and adapting lessons learned from US concepts and initiatives closely.[11]

One of Xi Jinping's milestones on the road to Chinese "national rejuvenation" by 2050 is China becoming a global leader in AI technologies and applications by 2030. This includes using AI to build an "intelligentised military". In his report to the 19th Party Congress, in October 2017, Xi Jinping urged that the PLA should, "accelerate the development of military intelligentization and improve joint operations capabilities and all-domain operational capabilities based on network information systems".[12] AI is seen as capabilities to include automated decision aids to enhance the speed and accuracy of operational decisions. PLA strategists also think that AI applications will provide the basis for advanced cruise missiles;

autonomous ground, air, surface and sub-surface drone systems; anti-artillery, air, and missile defence systems and a range of C2 and other systems.

China considers big data analytics and AI as strategic resources. Chinese scholars think that big data and AI will improve PLA capabilities and position China to prevail in future conflicts. Hence, the PLA is exploring programs to collect, process, integrate and share data across the force for various applications, including C4ISR, logistics, equipment acquisition, mobilisation, modelling and simulation, training and cyber operations. The PLA believes that intelligentization will primarily change future warfare and provide a rare opportunity to leapfrog its development over China's adversaries.

Chinese aspirations for an innovative military strategy and doctrine to become a reality will mainly depend on applying emerging big data and AI technologies to military purposes and the integration of new capabilities to existing concepts of joint force operations in system-of-systems warfare. CCP leadership has prioritised and resourced the development of the requisite technologies and systems.[13]

At the same time, the PLA faces critical challenges to operationalise artificial intelligence (AI) across a range of applications— from issues of talent to the management of data and adaptation as an organisation.[14]

Challenges in Chinese Military Innovation

PLA's advances and ambitions in autonomy, robotics and a range of applications of artificial intelligence cannot be underestimated. However, the PLA will confront many likely difficulties and shortcomings that will impede its implementation. Some of them are:[15]

- The PLA’s capacity to innovate may be impeded by its bureaucratic politics and culture.
- The PLA’s capability to leverage AI could be delayed by a continued shortage in talent and human capital. Despite progress in training, the PLA may continue to struggle to match the required sophistication for future warfare.

- The PLA appears to have difficulties revising its doctrine, adopting new theories and concepts in practice.
- The PLA has difficulty managing and integrating its data due to bureaucratic challenges and limited adoption of cloud computing.
- The PLA's lack of operational experience under actual combat conditions could lead to failure in appreciating the challenges of operating highly complex autonomous systems.
- The implementation of military-civil fusion might be inefficient and undermined by poor coordination or corruption.
- The massive investments required to promote military-civil fusion and the development of emerging technologies may not be allocated efficiently, creating distortion.
- There are specific weaknesses in key and core technologies within China's technological ecosystem that will be difficult to redress.

Difficulties of Intelligentisation

There are many problems in achieving intelligentisation. Some of them are:

- PLA experts on intelligentisation overwhelmingly call for highly centralised decision-making structures. They think advanced algorithms will help operational commanders to perfectly direct intelligent swarms of autonomous battle systems to achieve campaign objectives. PLA experts think that this approach will fuse command responsibility onto a few Generals who can remain safely away from the battlefield. But this negates the concept of mission command. The PLA theorists do not appear to recognise this risk compared to the perceived gains.
- PLA experts seem to miss the inherent fragility of AI and autonomous systems. The future PLA is based almost entirely on advanced technology, with little consideration for potential risks and mitigation approaches. A well-planned electronic warfare attack from an adversary could severely affect the PLA's command and control setup.

- PLA strategists seem to have too much faith in the capabilities of AI and advanced technologies. They think that autonomous systems will eventually be better at making decisions than humans. They go to the extent of claiming that future warfare will closely resemble the Star Wars movies.
- It is being recognised that AI is neither artificial nor intelligent. But the PLA does not acknowledge or accept this uncertainty. Though advancements in AI continue, many overestimate the ability of AI to make decisions. In future combat operations, autonomous systems will face unexpected challenges which can only be suitably addressed through human ingenuity.
- PLA will need to enhance the technical proficiency of its officers and personnel to continue developing and applying AI to warfare. Ironically, this could result in a greater split among PLA's human resources, with operational commanders remaining under-qualified for technical aspects and underutilised because of automated decision-making.
- The overconfidence of PLA on futuristic technology has potential risks that could affect its war fighting capabilities. These new technologies are only as useful as they are manifested and effectively applied in Chinese war fighting doctrine. Intelligentisation may not deliver all the advantages the PLA hopes for.
- PLA experts' visions of intelligentisation appear to overestimate the transformative potential of AI. It could set the army up for failure in the long-term.
- Intelligentisation will bring about new set of vulnerabilities for the PLA that may reduce any effective advantage gained.

China's AI capabilities

US Secretary of Defense, Lloyd Austin, said in July 2021 that the US urgently needs to develop responsible artificial intelligence technology at a faster pace. He stated that a new $1.5bn investment would expedite the Pentagon's adoption of AI over the next five years. 600 AI efforts were already under way.

Nicolas M Chaillan, a member of the US Air Force and the Pentagon's former first Chief Software Officer, caused a furore when after resignation, he stated the following:[16]

- China will dominate numerous aspects of emerging technologies over the next few decades, especially when it comes to artificial intelligence, synthetic biology and genetics.
- China has won the artificial intelligence battle with the US and is heading towards global dominance because of its technological advances.
- China is set to dominate the future of the world, controlling everything from media narratives to geopolitics.
- We have no competing fighting chance against China in 15 to 20 years. Right now, it's already a done deal; it is already over in my opinion. Whether it takes a war or not is kind of anecdotal.
- Regarding the readiness level of government agencies in cyber security and defence, some departments were operating at a "kindergarten level".
- Many senior officials with little experience were allowed to run cyber security programs.
- Part of the reason the US was behind in technology race was the unwillingness of large American companies like Google to work with the government due to ethics related issues surrounding the use of AI and extensive ethical debates over technology and sluggish innovation.
- Chinese tech companies are making "massive investments" in AI and are not taking ethics into account.
- The US would be unable to match China's rapid pace of technological advances.

However, not all agree with the views of Nicolas Chaillan.

US Army CIO Ray Iyer vehemently denied this. He said "It's absolutely not true… If you looked at both what we have in the Department of Defense and Intelligence Community, across the federal government and our industrial partners, we have the best AI technology".

The US and its partners share "trade intelligence information and other things", helping both sides. Ray Iyer added, "I can tell you the Chinese don't have that. They're operating in a vacuum, and they're relying on nefarious methods and cyber attacks to be able to get to, you know, what they think they know that we have".[17]

As per the testimony of independent analyst and former US Army attaché to Beijing and Hong Kong Lieutenant Colonel Dennis J Blasko: in certain areas, such as some categories of ballistic and cruise missiles, air defence, electronic warfare, and cyber capabilities, the PLA ranks among the world's leaders. However, in many other battlefield functions, the PLA trails advanced militaries by one to multiple decades of experience".[18]

Bloomberg reports that China watchers shouldn't think that its position is unassailable or that the US. is weaker.[19] China's expertise is somewhat limited in scope. Artificial intelligence has many sub-fields, including robotics, machine learning, natural language processing and computer vision. The US has broad toolkit that is deployed across each of these disciplines and used around the world. China excels mostly in computer vision, an area that helps Beijing build out its surveillance state.

US asserts its dominance by creating products that help clients around the world become more profitable or efficient. The US is the world leader in the following:

- Machine learning that leverages data and algorithms to learn and improve accuracy. Lion's share of the world's leading and widely adopted frameworks were developed in US by companies like Google, Microsoft, Facebook and the University of California, Berkeley.
- The best natural language processing engines also come from US tech giants like Microsoft, Google, Amazon and IBM. Globally these tools are used for voice recognition in smart speakers, improve translation and search results or detect fraud in the financial industry and run chatbots in customer service.
- US is a world-beater in process automation, which replaces staff in call centres and customer service.

- US companies are leaders in enterprise deployments. The recent surge in Work From Home usage has driven demand for cloud computing and networking technologies.

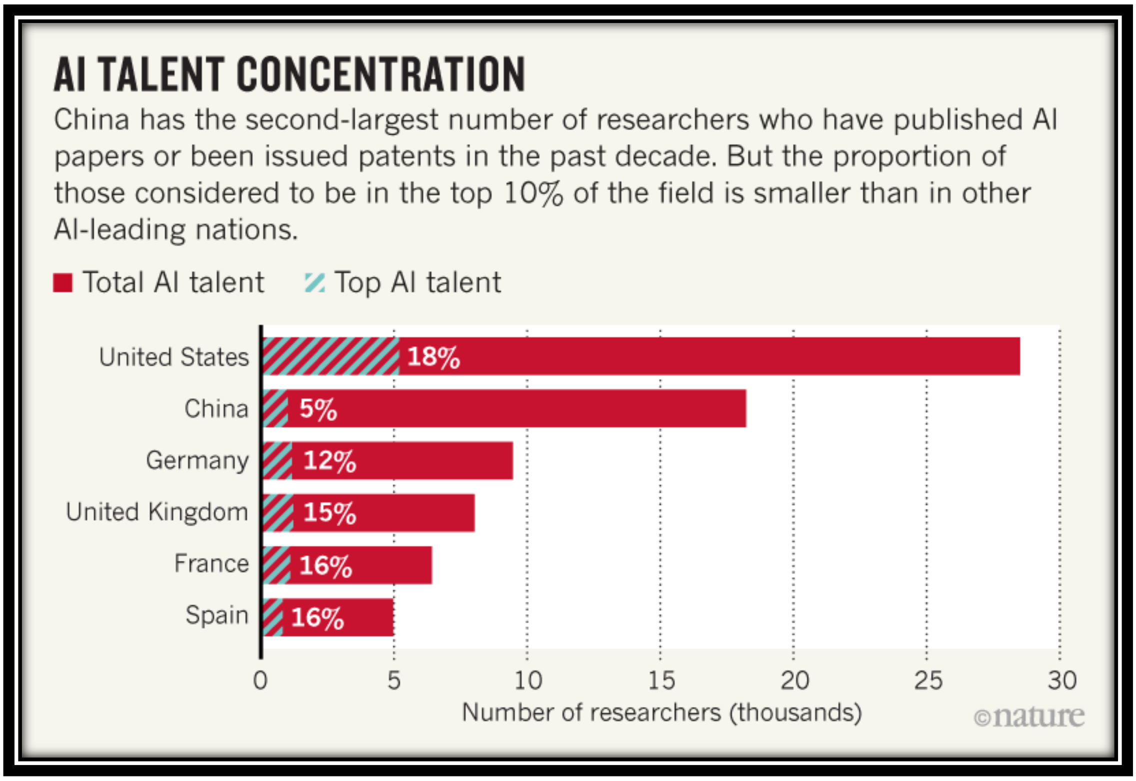
China has world-leading companies in computer vision, speech recognition and natural language processing, including SenseTime, Unisound, iFLYTEK and Face++. But it lags in shaping the core technology tools of AI. For example, the open source platforms like TensorFlow and Caffe are widely used in industry and academia the world over. These are developed by US companies and academies to design, build and train the sets of algorithms that facilitate computers to function more like the human brain. But PaddlePaddle, one of the major open-source platforms developed by Chinese company Baidu, is mostly used to quickly develop AI products.

China lags in AI hardware. Most of the world's leading AI-enabled semiconductor chips are made by US companies such as Intel, Nvidia, Apple, Google and Advanced Micro Devices. China lacks expertise in designing computing chips that can support advanced AI systems. China would take five to ten years to reach the level of innovation in fundamental theories and algorithms occurring in the US and the UK. The key to China meeting its long-term AI goals is contributing to the fundamental theories and technologies of AI.[20]

However, US is now heavily reliant on Taiwan for semiconductors, as is PRC. While South Korea, Thailand and Vietnam have stepped up semiconductor production, the US needs to begin "re-shoring" this industry. [21]

AI talent. An important factor for China’s progress will be its ability to hold onto talented researchers. As per the 2018 China AI Development Report,[22] by the end of 2017, China had the second-largest pool of AI scientists and engineers. They are about 18,200 people in number, ranking behind the US, which had roughly 29,000 people. But China was sixth in its number of top AI researchers.

Figure 2: AI Talent Concentration



Source: Sarah O'Meara, Will China lead the world in AI by 2030? Nature, 21 August 2019. Available at: https://www.nature.com/articles/d41586-019-02360-7

Normally, Chinese computer scientists are trained in the US and then stay there to work for global technology companies. However, the situation is changing. AI institutes in China are trying to allure some of these researchers back to the mainland with high salaries. They are also welcoming top scientists from across the globe, including India, by offering lucrative salaries, excellent research facilities and liberty to work independently.

China's three core tech companies, Tencent, Baidu and Alibaba, have become global leaders in AI, although they are still not in the same league as US companies, like Google and Microsoft. China also has at least ten Unicorns which are privately owned AI start-ups valued at more than US$1 billion, including facial recognition firm SenseTime.[23]

Eric Schmidt, former chairman of Google and the chairman of a special commission on artificial intelligence, warned US Congress and stated that the US is only one to two years ahead of China in developing artificial intelligence. Testifying before the Senate Armed

Services Committee, he said that the US needs to maintain a five to ten years advantage over China in AI and other high technology fields like quantum computing. He said he was “worried as US don’t understand the competitive threat from China” that encompasses semiconductor manufacturing, directed energy, 5G technologies and synthetic biology, as well as AI, machine learning and hypersonics.[24]

The advantages of the US are in its innovative private sector and robust university system. A Center for Data Innovation report[25] that looked at talent, research, development, adoption, data and hardware in the AI space found that "despite China's bold AI initiative, the United States still leads in absolute terms; China comes in second, and the European Union lags further behind”. The US leads in AI in four of the six categories: talent, research, development and hardware.

China surpassed the European Union in AI. It is quickly reducing the gap between itself and the US. The Chinese have more data than the EU and US, which fuels AI technology and accurate AI models.

The Center for Security and Emerging Technology (CSET) estimates show that China is likely to spend far less on AI than previously assumed. Most of its AI money is going to non-military-related research, such as fundamental algorithm development, robotics research, and smart infrastructure development. By contrast, US’s planned spending for the fiscal year 2020 allocated majority of its AI budget to defence. It means US could outspend China in that category. These numbers directly oppose the prevailing narrative.

***Change in Thinking about Warfare*.** The Chinese concept of war has changed drastically in last 20 years. However, basic thinking of PLA like stratagems, deception etc. remain as important parts of their concept and are being incorporated with modern technological advances. AI is now being seen as a tool to help the PLA in controlling future conflicts. That will provide PLA with a deterrence to confront other nation states in a conflict scenario. It seems that China’s earlier belief of ‘technology determines tactics’ is now changed to ‘technologies determine strategy’ due to the recent stress on technologies, including cyber technology. PLA’s thought process on use of technologies in warfare is changing, and we would do well to evaluate this thought process.

The emerging theory of intelligentised operations attempts to address what Prussian theorist Carl von Clausewitz called the “Fog of War” on the battlefield. The PLA can thus take credit for thinking big to solve problems that warfighters have grappled with for generations. It is trying to create a strategic doctrine for AI and other cutting-edge technologies in future warfare. China is thinking long term. If successful, the PLA will have an obvious advantage over its adversaries in future conflicts.

China feels that US is its main adversary. The US has tremendous technological capabilities as compared to China. China is trying to match that with its own strength in AI as a leapfrog technology and a new concept of war. But there will be many problems in implementing this concept of ‘Intelligentizing Warfare’ to reality. President Xi Jinping has thrown the gauntlet, and it is up to the US, other adversaries and the rest of the world to follow this concept keenly.

PLA Strategic Support Force (PLASSF)

Established in 2015, the Strategic Support Force has integrated and consolidated China's previously disparate cyber, electronic, space and psychological warfare units under a unified command structure. The PLASSF's Network Systems Department has combined technical reconnaissance bureaus (TRBs) responsible for cyber espionage and signals intelligence and elements of the former GSD Fourth Department (4PLA) responsible for electronic countermeasures and offensive cyber operations. The structure of the PLASSF incorporates the concept of 'integrated network and electronic warfare’.[26]

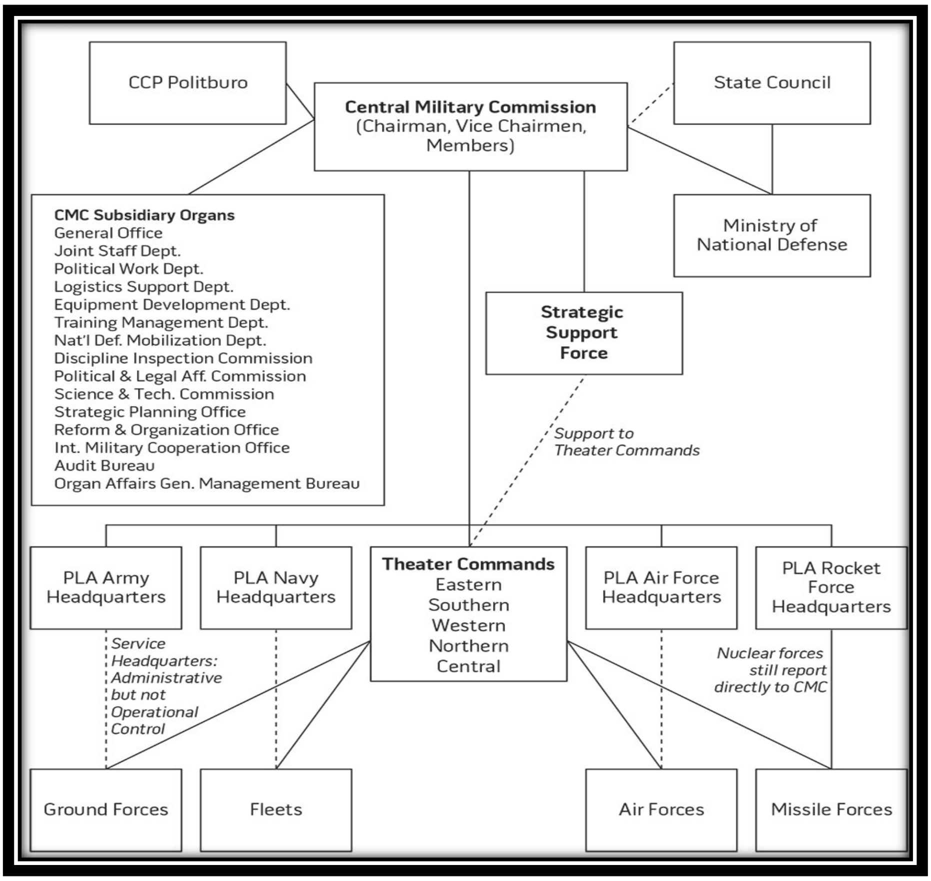
The Strategic Support Force is responsible for collecting and managing technical intelligence, including from cyber and space assets; supporting joint operations and carrying out attacks against an adversary’s command network.

The PLA’s cyber capabilities of defence, offence and reconnaissance, all have been centralised under the SSF. The PLA looks for using offensive cyber operations to disrupt, degrade or damage adversary systems, including critical infrastructure, preceding and during multiple stages of a conflict and in various conflict scenarios. PLA wants to use defensive cyber operations to defend against the same capability from an adversary . Reconnaissance includes a broader set of capabilities, including those used in peacetime. This includes cyber espionage against military, civilian or commercial targets, theft of military technological know-how, intellectual property, etc. In some instances, espionage and reconnaissance intrusions can be leveraged later for destructive capability. According to US DOD, "the PRC presents a significant, persistent cyber espionage and attack threat". However, PLA leaders believe PRC cyber warfare capabilities are inferior to those of the US.

PLA, through the SSF seeks to integrate Electronic warfare more thoroughly with cyber warfare.

PLA Structure after Reform

Figure 3: PLA Structure after Reform


CCP Politburo
Central Military Commission
(Chairman, Vice Chairmen, Members)
State Council
CMC Subsidiary Organs
General Office
Joint Staff Dept.
Political Work Dept.
Logistics Support Dept.
Equipment Development Dept.
Training Management Dept.
Nat'l Def. Mobilization Dept.
Discipline Inspection Commission
Political & Legal Aff. Commission
Science & Tech. Commission
Strategic Planning Office
Reform & Organization Office
Int. Military Cooperation Office
Audit Bureau
Organ Affairs Gen. Management Bureau
Ministry of National Defense
Strategic Support Force
Support to Theater Commands
PLA Army Headquarters
PLA Navy Headquarters
Theater Commands
Eastern
Southern
Western
Northern
Central
PLA Air Force Headquarters
PLA Rocket Force Headquarters
Service Headquarters: Administrative but not Operational Control
Nuclear forces still report directly to CMC
Ground Forces
Fleets
Air Forces
Missile Forces

Source: Phillip C. Saunders and Joel Wuthnow, China's Goldwater-Nichols? Assessing PLA Organizational Reforms, National Defense University, April 2016, http://inss.ndu.edu/Portals/68/Documents/stratforum/SF-294.pdf

Cyber Security Management

Deficiencies in China's Cyber Security Mechanisms. China is acutely aware of its weakness in cyber security. President Xi Jinping complained when he said, "The control of core technology by others is our biggest hidden danger".[27] Chinese experts assess that the US holds advantage in cyber capabilities in overall IT industry dominance, control of Internet infrastructure, malware design and training of cyber forces. Chip, network switch, processor and other core technologies of US are superior to other countries. Big US companies like Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle, and Qualcomm dominates the IT industry, which the Chinese media call 'eight guardian warriors'. China feels that the dominance of these companies would give US access to the critical information infrastructure of any country that US can exploit during conflicts.

According to China's statistics, 80 per cent of Chinese chips, high-end components, universal protocols, and standards depend on imports; 65 per cent of information security products like firewalls, encryption machines and others are also imported. China's leaders consider its cyber defences weak.

According to the annual report from the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC), in 2020 about 5.31 million hosts on the Chinese mainland were controlled by a total of about 52,000 overseas malicious program command & control servers, and the top three origins of overseas servers in terms of the number of compromised Chinese hosts are all from NATO member states.[28]

Tencent, one of the world's largest internet firms, in a report from Tencent Security Response Centre, gave out reasons for the weakness of China's cyber security sector:

- High cost.
- Focus on profit instead of security.
- A general lack of talent.
- Poor cyber security threat technology.
- Concentration of the sector in Tier 1 and Tier 2 cities such as Beijing, Shanghai and Guangdong.

- Reliance on foreign imports for main information infrastructure.
- Poor capability to track hostile activity especially advanced persistent threats.
- Reliance on outdated methods of protecting data.
- Limited legal foundations for thwarting and tracking illegal access of data.
- Lack of national control in core technologies.
- Under developed identity-authentication systems.
- Cyber security investment of Chinese firms as a share of total investment (1.78 per cent) was far lower than that in the US (4.78 per cent) and the rest of the world (3.75 per cent).

Edward Snowden's Revelation. Edward Snowden, in June 2013, revealed widespread successful penetration of Chinese systems with the help of the National Security Agency (NSA) and the FBI. This dramatic disclosure put US in an embarrassing situation. Edward Snowden exposed the following: [29]

- The NSA has been hacking majority of Chinese government and private systems since 2007. They relied on routers of the US Company- Cisco Systems.
- NSA penetrated Huawei's headquarters in Shenzhen to exploit the routers and switches made by Huawei that are used by third of the world's Internet population.
- NSA had hacked Chinese universities, telecommunications firms and submarine cables.
- 14 American secret cyber agencies had been closely tracking secret cyber operations by China for several years.
- NSA broke into a Chinese telecommunication company to obtain mobile phone messages and repeatedly attacked the backbone network of Tsinghua University and computers of the telecommunications company Pacnet in their Hong Kong headquarters.

According to a scholar at the China Institute of Contemporary International Relations, "The United States holds the power of determining anyone's life or death in cyberspace and has the capability of dominating cyber information. China is aware that some of the most sophisticated malware like Stuxnet and Flame have been developed in American labs. The broadband information infrastructure development gap with developed countries has widened; the level of government information sharing and business collaboration is not high; the core technology is controlled by others; . . . insufficient strategy coordination; weak critical infrastructure protection capability; mobile Internet and other technologies pose serious challenges". China had to deal with the humiliating exposure of a PLA cyber espionage. Mandiant, a US cyber security firm, gave a detailed report of China's cyber espionage activities and its main organization— Unit 61398. This report also showed critical gaps in PLA's cyber security system.[30]

Indigenous Digital Industrial Base. China wants to decrease its reliance on foreign cyber technology. It has a much weaker cyber industrial base than the US, lower levels of nationwide informatisation and less advanced & fertile educational system. China has no cyber military allies, where the US leads an impressive cyber military alliance network. The US- China Security and Economic Review Committee, 2019 Report to Congress states: To achieve security in the long run, China must domestically produce chip technology, operating systems, and cryptographic techniques with independent intellectual property. Only with these steps can China guarantee the real safety of national networks.[31]

China has a modest domestic cyber security industry, a fraction of the size of its American counterpart. The leading cyber security firms in China have much lower revenues than those in the US and much smaller global footprints.

President Xi Jinping has been pragmatic on this issue. He seems to be accepting the time and effort it will take to overcome the challenge posed by the US. In 2019, he summarised it succinctly, "No matter how large an internet company is, no matter how high its market value is, if it is heavily dependent on foreign countries for its core components, and if the major artery of the supply chain is in the hands of others, it is like building a house on someone else's foundation. No matter how big and beautiful it is, it may not stand up to wind and rain, and it may be so vulnerable that it collapses at the first blow. [32] The free market would not be sufficient. Market exchange cannot bring us core technologies, and money cannot buy core technologies. We must rely on own research and development. In a globalised environment such research and development could not be expected to take place behind closed doors. Only when we fight against masters can we know the gap in ability. China would not reject any new technology. It would strategically determine which ones can be introduced [from abroad], digested, absorbed, and then re-innovated versus which must be indigenously innovated on their own".[33]

China has been taking action to improve its cyber security. China's Ministry of Industry and Information Technology, in July, 2021 released a draft three-year cyber security plan. It is the most detailed strategy for the development of China's cyber security industry. This mandates that key industries, such as telecommunication industry, must devote 10 percent of their budget to cyber security by 2023.[34]

Conclusion

China's People's Liberation Army (PLA) has understood that 'dominance in the information domain is the priority in modern conflict'. Through the re-organisation of the PLA and the establishment of the Strategic Support Force, China has brought space, cyber, electronic warfare, and psychological warfare under one umbrella to use these capabilities more efficiently and effectively. No other country, including the US has done this.

China has no threat from land. Presently, its main aim is to secure Taiwan. All its modernisation, organisational changes and concepts of warfare are meant for this conflict, which will also involve the US, and has systematically developed these capabilities keeping in mind this scenario.

End Notes

[1] Cyber Capabilities and National Power: A Net Assessment, *IISS*, 28 June 2021. Available at https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

[2] "China's Cyber Power in a New Era", in Tim Huxley and William Choong, eds. *Asia-Pacific Regional Security Assessment 2019*, (London, UK: Routledge, International Institute for Strategic Studies, 2019). Available at https://www. iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5.

[3] Hearing before the subcommittee on oversight and investigations of the committee on energy and commerce house of representatives one hundred thirteenth congress first session, cyber espionage and the theft of US Intellectual property and technology, 09 July 2013. Available at https://www.govinfo.gov/content/pkg/CHRG-113hhrg86391/html/CHRG-113hhrg86391.html.

[4] "Confidential report lists US weapons system designs compromised by Chinese cyber spies", *The Washington Post*, 27 May 2013. Available at https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

[5] PK Mallick, "Chinese Cyber Exploitation in India's Power Grid: Is There a linkage to Mumbai Power Outage? Strategic Study India, *Issue Brief*. Available at https://indianstrategicknowledgeonline.com/web/Chinese%20Cyber%20Exploitation%20in%20India%E2%80%99s%20Power%20Grid%20.pdf.

[6] "2020 Report to Congress of the US-China Economic and Security Review Commission, December 2020. Available at https://www.uscc.gov/sites/default/files/2020-12/2020_Annual_Report_to_Congress.pdf.

[7] China's Military Strategy", *Xinhua*, 27 May 2015. Available at http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.html.

[8] Elsa Kania and John Costello, "China's Quest for Informatization Drives PLA Reforms", *The Diplomat*, 04 March 2017. Available at: https://thediplomat.com/2017/03/chinas-quest-for-informatization-drives-pla-reforms/.

[9] ROC National Defense Report 2021. Available at https://www.mnd.gov.tw/NewUpload/%E6%AD%B7%E5%B9%B4%E5%9C%8B%E9%98%B2%E5%A0%B1%E5%91%8A%E6%9B%B8%E7%B6%B2%E9%A0%81%E5%B0%88%E5%8D%80/%E6%AD%B7%E5%B9%B4%E5%9C%8B%E9%98%B2%E5%A0%B1%E5%91%8A%E6%9B%B8%E5%B0%88%E5%8D%80.files/%E5%9C%8B%E9%98%B2%E5%A0%B1%E5%91%8A%E6%9B%B8-110/110%E5%B9%B4%E5%9C%8B%E9%98%B2%E5%A0%B1%E5%91%8A%E6%9B%B8-%E8%8B%B1%E6%96%87%E7%89%88.pdf

[10] Joe McReynolds, "China's Military Strategy for Network Warfare", in Joe McReynolds, ed., *China's Evolving Military Strategy*, (Jamestown Foundation, 2016), p. 213 and Shou Xiaosong, ed., *The Science of Military Strategy Military Science*, 2013, p.93.

[11] PK Mallick, "Defining China's Intelligentized Warfare and Role of Artificial Intelligence", *Vivekananda International Foundation*, March 2021. Available at https://www.vifindia.org/sites/default/files/defining-china-s-intelligentized-warfare-and-role-of-artificial-intelligence.pdf.

[12] Edmund J Burke et al, *People's Liberation Army Operational Concepts*, (Rand Corporation, 2020). Available at https://www.rand.org/content/dam/rand/pubs/research_reports/RRA300/RRA394-1/RAND_RRA394-1.pdf.

[13] Ibid.

[14] Ben Non and Chris Bassler, "Schrodinger's Military? Challenges for China's Military Modernization Ambitions", *WOTR*, 14 October 2021. Available at https://warontherocks.com/2021/10/schrodingers-military-challenges-for-the-chinas-military-modernization-ambitions/.

[15] Elsa B Kania , "Testimony before the US-China Economic and Security Review Commission Hearing on Trade, Technology", and "Military-Civil Fusion Chinese Military Innovation in Artificial Intelligence", 07 June 2019.

[16] Justin Klawans , "Pentagon Official Resigns Over Belief China Has Won AI Battle, Heading to Global Dominance", *Newsweek*, 11 October 2021. Available at https://www.newsweek.com/pentagon-official-resigns-over-belief-chin,a-has-won-ai-battle-heading-global-dominance-1637772.

[17] Colin Clark, "Absolutely Not True': Army CIO Answers Claim US Has Already Lost To China In AI", *Breaking Defense*, 13 October 2021. Available at https://breakingdefense.com/2021/10/absolutely-not-true-army-cio-answers-claim-us-has-already-lost-to-china-in-ai/?_ga=2.9853109.1878335474.1634123557-830645661.1600688594&utm_source=pocket_mylist.

[18] Testimony of independent analyst and former US Army Attaché to Beijing and Hong Kong Lieutenant Colonel (ret.) Dennis J Blasko, in US-China Economic and Security Review Commission, "What Keeps Xi Up at Night: Beijing's Internal and External Challenges", hearings, 07 February 2019.

[19] Tim Culpan, "China isn't the AI juggernaut the West fears", *Bloomberg*, 13 October 2021.

[20] Sarah O'Meara, "Will China lead the world in AI by 2030? Nature", 21 August 2019. Available at https://www.nature.com/articles/d41586-019-02360-7.

[21] Committee on Armed Services United States Senate Hearing to Receive Testimony on Emerging Technologies and Their Impact on National Security, 23 February 2021. Available at https://www.armed-services.senate.gov/hearings/21-02-23-emerging-technologies-and-their-impact-on-national-security.

[22] "China AI Development Report", *China Institute for Science and Technology Policy at Tsinghua University*, July 2018. Available at http://www.sppm.tsinghua.edu.cn/eWebEditor/UploadFile/China_AI_development_report_2018.pdf.

[23] John Grady, "US Holds Slim Edge over China in Artificial Intelligence, Former Google Chairman Says", 23 February 2021. Available at https://news.usni.org/2021/02/23/u-s-holds-slim-edge-over-china-in-artificial-intelligence-former-google-chairman-says.

[24] Committee on Armed Services United States Senate Hearing to Receive Testimony on Emerging Technologies and Their Impact on National Security, 23 February 2021. Available at https://www.armed-services.senate.gov/hearings/21-02-23-emerging-technologies-and-their-impact-on-national-security

[25] Daniel Castro, Michael McLaughlin and Eline Chivot, "Who Is Winning the AI Race: China, the EU or the United States?" *Center for Data Innovation*, 19 August 2019. Available at https://datainnovation.org/2019/08/who-is-winning-the-ai-race-china-the-eu-or-the-united-states/.

[26] John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era", *Institute for National Strategic Studies*, China Strategic Perspectives, no. 13, 02 October 2018. Available at www.inss.ndu.edu.

[27] "President Xi Says China Faces Major Science, Technology Bottleneck", *Xinhua*, 01 June 2016. Available at http://en.people.cn/n3/2016/0601/c90000-9066154.html.

[28] "GT investigates: Hacking China's medical institutes at COVID-19 outbreak, targeting aerospace firms during China's space missions – Cyber attacks from India disclosed", *Global Times*, 05 November 2021. Available at https://www.globaltimes.cn/page/202111/1238218.shtml.

[29] Kurt Eichenwald, "How Edward Snowden Escalated Cyber War with China", *Newsweek*, 01 November 2013.

[30] APT1, "Exposing One of China's Cyber Espionage Units". Available at https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[31] "US–China Security and Economic Review Committee", *2019 Report to Congress of the US– China Economic and Security Review Commission, 116th Congress, 1st Session*, November 2019, p. 135. Available at https://www.uscc.gov/sites/default/files/2019-11/2019 percent20Annual percent20Report percent20to percent20Congress.pdf.

[32] "China's Xi Jinping warns of new "long march" as trade war with US intensifies", *Straits Times*, 22 May 2019. Available at https://www. straitstimes.com/asia/east-asia/chinese-president-xi-jinpingwarns-of-new-long-march-as-trade-war-intensifies.

[33] "The Full Text of Xi Jinping's Speech at the Forum on Cyber security and Informatisation Work".

[34] N.28.

The views expressed and suggestions made in the article are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with author.

CENTRE FOR LAND WARFARE STUDIES (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Tel.: +91-11-25691308, Fax: +91-11-25692347, CLAWS Army No. 33098; Email: landwarfare@gmail.com
Website: www.claws.in