CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

NEW GENERATION TECHNOLOGY TRENDS ON THE ROAD TO REALISATION OF MILITARY GOALS 2035 OF THE PEOPLES LIBERATION ARMY – A REALITY CHECK

Mr Neelotpal Mishra, DIS is an alumnus of the Royal Military College of Science and University of Oxford U.K. His expertise's are Information and Cyber, Warfare and Technologies.

Scope

Peoples Republic of China (PRC) has grabbed the world's attention with the unveiling of 'Made in China 2025' plan on 19 May 2015. This is essentially to transform PRC from being looked at as 'Copied in China' to 'Engineered and made in China'. Since the implementation of this plan PRC has reportedly made significant progress towards achieving its military goals of 2027 i.e. 'Chinese Communist Party plan to make PLA at par with US military by 2027'.[i] This would primarily be done by the use of the Fourth Industrial Revolution (4IR) dual purpose technologies (for both military and civil purpose).

As reported by Xinhua 4IR technologies concern smart (intelligent) connected objects, the Internet of Things, big data, 5G communication and artificial intelligence (AI) which are transforming the global economy and having a profound impact across many sectors, from manufacturing to healthcare to transport, defence & security etc.[ii]

On July 26, 2018, at the tenth BRICS summit, held in Johannesburg, South Africa, Xi Jinping delivered an important speech titled 'Making a Beautiful Vision a Reality', revealing the prominent features of the new industrial revolution. "From the mechanization of the first industrial revolution in the

18th century, to the electrification of the second industrial revolution in the 19th century, to the informationization of the third industrial revolution in the 20th century, each round of disruptive technological innovation has shaped history. Today, we are experiencing a broader and deeper technological revolution and industrial change. Breakthroughs have been made in cutting-edge technologies such as big data and artificial intelligence, and new technologies, new business forms, and new industries have emerged one after another." [iii]

In 1997 President Jiang Zemin articulated a 'Cross-century goal' for modernising the military in three steps. Step one (1997-2010) was to streamline by efficient structure and acquire advance equipment and weaponry. Step two (2010-2020) was to enhance quality of the defence forces through the development of more advanced weapons and equipment. Step three (2020-2050) is to realise the modernisation of defence forces. In November 2017, President Xi Jinping, called for mechanisation and making major progress towards informatisiation by 2020. By 2035 (mid way through Step Three) PRC would complete military modernisation and by 2050 they would have a 'fully transformed' world class military. A new milestone of 2027 has been added to coincide with the centenary of the People Liberation Army's (PLA). PLA was founded on 1st August 1927. The four elements of this milestone are firstly accelerating the integrated development of mechanisation, informatisation and intelligentisation, secondly accelerating the modernisation of military doctrine, organisation, personnel & weapons, thirdly adhering to quality & prioritising efficiency and fourthly promoting the simultaneous improvement of national defence & economic strength.[iv]

The scope of the paper is to do a reality check i.e. identify the current stage and future trends of 4IR technologies by PRC. Some legacy related / interlinked technologies would also be touched upon.

The paper attempts a reality check on the developments in PRC and how it is leveraging the current technology to realize its Military goals of 2035.

Organisational Enablers

The main military agency for leveraging and implementing all kinds of 4IR technologies is currently the Strategic Support Force (SSF) in PRC. To fully understand the current and the future state of the PLA use of 4IR technologies, it is imperative to gain an understanding of the SSF.

In November of 2015, as part of broader PLA organizational reforms, China established the SSF as a military service level organization reportedly "equal in standing to China's army, navy, air force and missile service." [v]

The SSF has been designed as a force optimized for dominance in space, cyberspace, and the electromagnetic domain, which are considered critical "strategic commanding heights" for the PLA. It has seemingly consolidated control over a critical mass of the PLA's space-based and space-related assets and thereby taking over responsibility for strategic-level information support for the PLA in its entirety, enhancing its capability to engage in integrated joint and remote operations. The SSF has also integrated the PLA's capabilities for cyber, electronic, and psychological warfare into a single force for enhancing / generating synergy in operations in these domains. Thus SSF integrates the force structure and operations in these vital new domains, to fight and win future "informatized" wars.

The "integrated reconnaissance, offense, and defense" may serve as an organizing concept, which could involve the integration of disciplines together to enhance full-spectrum war-fighting capabilities. The SSF operations range from strategic information operations, satellite information attack and defense, electronic assault, Internet assault, campaign information operations, electronic warfare, anti-radiation, battlefield cyber warfare and tactical information operation to "paralyze enemy operational system of systems" and "sabotage the enemy's war command system of systems." [vi]This would be achieved by space and cyber attacks against political, economic, and civilian targets as a deterrent.

As the classification of the SSF is always an operational service, the assets are used for military, political and commercial cyber espionage. The missions may be of military importance or, in some cases at the behest of local state-owned enterprises for technology and commercial gains. It is conducting asymmetric warfare, such as cyber-electromagnetic confrontation and space-electronic confrontation [vii]

This strategy is of "active defense," a concept it describes as strategically defensive but operationally proactive in orientation.[viii]

The insignia of the SSF consists of a depiction of a spacecraft super imposed on a structure of an 'Atom' with 'Electrons' revolving. This signifies the emphasis on the use of space, cyberspace and electromagnetic (quantum) aspects of warfare in the mandate of SSF.

The main strength of the SSF is to conduct Basic Operational Forms of "Information System-Based System of Systems Operations". These are: [ix]

- **Information-firepower** strike, which is an attack that combines soft-kill and hard-kill methods, where information is the initiative and firepower are the mainstay. Use of firepower is focused on long-range precision attacks employing mainly precision-guided munitions. Focus is placed on electronic, cyber, and psychological-cognitive attacks to destroy the enemy's operational Systems.

- **Multi domain / dimensional assault** enables the SSF to attack an enemy's operational targets in multiple domains, such as land, sea, air, space, electromagnetic, psychological-cognitive and cyber. This form of attack combines soft-kill and hard-kill methods in multi-dimensional domains against the key nodes of the enemy's operational Systems.

- **Network-electronic integrated confrontation** activities are used for weakening and destroying enemy's and defending ones networks and EW (EW) equipment / systems. This is aimed to gain information dominance by network electronic reconnaissance, attack and defense.

- **Psychological-cognitive attack** is aimed at psychological cognition and uses the information media as a weapon to influence psychological cognition and create a state of psychological cognition that is advantageous to ones units and disadvantageous to the opponent. Targets range from enemy military & civil leaders, dignitaries, troops, civilians, enemy allies, and third countries. It can be combined with information-firepower strikes and multi domain-dimensional assaults to enhance its effectiveness.

- **Special operations** using cyber, space and electromagnetic resources to target enemy's strategic and campaign targets for specific military, political, economic, or psychological purposes to affect all phases of the war. Missions include special reconnaissance, destruction and assault of key targets, seizure and control of key targets, precision attack guidance, psychological disintegration warfare, and cyber attacks.

- All the above are driven by the technological and industrial revolution and the application of cutting-edge technologies such as artificial intelligence (AI), quantum information, big data, cloud computing and the Internet of Things.

The SSF runs tracking, telemetry, and command stations in Namibia, Pakistan, and Argentina. The SSF also has a handful of Yuan Wang space support ships to track satellite and intercontinental ballistic missile (ICBM) launches.[x]

It could be inferred that SSF is still in the process of fully refining its functional attributes and is also trying to complete its organisational and administrative setup. With the limited open source material available there is a large expertise that the SSF has gained in the sphere of Cyber Espionage and also offensive cyber operations. These details have been discussed in detail in the paper. The creation of the SSF may have also complicated the chain of command and also the increased the turf war over the Area of Operations and / or responsibility. This is due to the possibility of the SSF being responsible to a dual chain of command.

Historical Technology Trends – U.S Perspective

To fully understand PRC's approach to handle 4IR technologies we would have to understand the historical technology trends that the PRC and PLA have had over the past decade.

The change in PRC's capabilities in 2009, 2016, 2020 and 2021 as assessed by United States, Department of Defence, China Military Power report. This puts into perspective the transformation and the trajectory of the progress made on the key subjects of Science and Technology Thrust / Innovation, Foreign Technology Acquisition and Sourcing Science & Technology for Military Modernisation.

A clear trend is established on how the PRC's policy at the national level is formulated in such a way that the interests of the PLA influence each facet of the policy. This in turn leads to PRC using many vectors to acquire sensitive, dual use technologies and military-grade equipment to advance its military modernization goals, including both licit & illicit means.

A plain comparison of the same topics of the report across several years establishes many things in common and also highlights to a great extent that the aggressive targets set in the plans are not always met.

Science and Technology Thrust/ Innovation

In 2009 PRC was focusing on IT, New Materials, Advance Manufacturing, Advanced Energy Technologies, Laser and Aerospace Technologies and 16 Major special items including core electronic components, high-end universal chips and operating system software, very large-scale integrated circuit manufacturing, next-generation broadband wireless mobile communications, high-grade numerically controlled machine tools, large aircraft, high resolution satellites, manned spaceflight and lunar exploration.

In 2016 PRC's National Medium and Long-Term Program for Science and Technology Development (2006-2020), issued by the State Council in February 2006, seeks to transform China into an “innovation-oriented society” by 2020.

In 2020 PRC aimed to build national corporate champions that achieve rapid market dominance across a range of technologies directly complements the PLA’s modernization efforts. As part of the 13th Five-Year Plan (2016–2020), focus areas include aerospace engines, including turbo fan technology and gas turbines; quantum communications and computing; innovative electronics and software; automation and robotics; special materials and applications; nanotechnology; neuroscience, neural research, and artificial intelligence (AI) and deep space exploration and on-orbit servicing and maintenance systems. China also was said to be applying substantial R&D resources to nuclear fusion, hypersonic weapons technology, and the deployment and hardening of its expanding multipurpose satellite constellation.

In 2021 A top-level push was there to master advanced technologies and become a global innovation superpower, this push directly supports the PLA’s ambitious modernization efforts and its goal of becoming a “world-class” military capable of “intelligentized” warfare such as AI, autonomous systems, advanced computing, quantum information sciences, biotechnology and advanced materials and manufacturing. As of 2020, the PLA has **funded multiple AI projects** that focus on applications including machine learning for strategic and tactical recommendations, AI-enabled wargaming for training, and social media analysis.

Foreign Technology Acquisition

In 2009 China has identified certain industries and technology groups with potential to provide technological breakthroughs, remove technical obstacles across industries and improve international competitiveness. Specifically, China’s defence industries were pursuing advanced manufacturing, information technology, and defence technologies.

Examples include radar, counter-space capabilities, secure C4ISR, smart materials, and low-observable technologies.

In 2016 PRC drew resources from diverse sources to support PLA modernization, including domestic defence investments, indigenous defence industrial development, a growing research and development (R&D)/ science and technology (S&T) base, dual-use technologies and foreign technology acquisition.

In 2020 the PRC continued to pursue many vectors to acquire sensitive and dual use technologies and military-grade equipment to advance its military modernization goals, including both licit & illicit means, foreign investments, commercial joint ventures, mergers and acquisitions, and state-sponsored industrial and technical espionage, and the manipulation of export controls for the illicit diversion of dual-use technologies. In 2019, the PRC's efforts included efforts to acquire dynamic random access memory, aviation, and anti-submarine warfare technologies.

In 2021 The PRC uses imports, foreign investments, commercial joint ventures, mergers and acquisitions, and industrial and technical espionage to help achieve its military modernization goals by acquiring technologies that will be foundational for future commercial and military innovations including AI, robotics, autonomous vehicles, quantum information sciences, augmented and virtual reality, financial technology, and biotechnology.

Sourcing Science & Technology for Military Modernisation

In 2009 China's defence industry had benefited from integration with China's rapidly expanding civilian economy and science and technology sector, particularly elements that have access to foreign technology. IT companies, including Huawei, Datang, and Zhongxing, maintain close ties to the PLA and collaborate on R&D.

In 2016 China continues to supplement indigenous military modernization efforts through the acquisition of targeted foreign technologies, including engines for aircraft, tanks, and naval vessels; solid state electronics and microprocessors, guidance and control systems; enabling technologies such as cutting-edge precision machine tools; advanced diagnostic and forensic equipment; and computer-assisted design, manufacturing, and engineering. China often pursues these foreign technologies for the purpose of reverse engineering or to supplement indigenous military modernization efforts. China seeks some high-tech components and major end items from abroad that it has difficulty producing domestically, particularly from Russia and Ukraine.

In 2020 the PRC continued to undermine the integrity of the U.S. S&T research enterprise through a variety of actions such as hidden diversions of research, resources, and intellectual property. The PRC continues to undermine the integrity of the U.S. S&T research enterprise through a variety of actions such as hidden diversions of research, resources, and intellectual property.

In 2021 PRC based intrusions continued to target computer systems around the world, including those owned by the U.S. Government, throughout 2020. These and past intrusions focus on accessing networks and extracting information. The PRC uses its cyber capabilities to not only support intelligence collection against U.S. political, economic, academic, and military targets, but also to exfiltrate sensitive information from the defence industrial base to gain military advantage and possibly for cyberattack preparations. The targeted information can benefit the PRC's defence high-technology industries, support the PRC's military modernization, provide China's leadership with insights into U.S. plans and intentions, and enable diplomatic negotiations.

For further details, a table comparing the change in PRC's capabilities in 2009, 2016, 2020 and 2021 with respect to Science and Technology Thrust/ Innovation, Foreign Technology Acquisition and Sourcing Science & Technology for Military Modernisation is shown in the Appendix.

China's growing military muscle and its drive to end American predominance in the Asia-Pacific is rattling the U.S. defence establishment. American officials see trouble quickly accumulating on multiple fronts like space, cyber and missile technologies and threats to Taiwan. "The pace at which China is moving is stunning," says Gen. John Hyten, the No. 2-ranking U.S. military officer, who previously commanded U.S. nuclear forces and oversaw Air Force space operations. He further added that at the current pace of China's military investment and achievement, Beijing "will surpass Russia and the United States" in overall military power in coming years "if we don't do something to change it, it will happen."

PRC has been marshalling the resources, technology and political will to make rapid gains, so rapid that the Biden administration is attempting to reorient all aspects of U.S. foreign and defence policy.

The latest example of surprising speed was China's test of a hypersonic weapon capable of partially orbiting Earth before re-entering the atmosphere and gliding on a manoeuvrable path to its target. The weapon system's design is meant to evade U.S. missile defences.[xi]

Cyber & Information Warfare and Cyber Espionage

Cyber Warfare

With PRC & PLA embracing the concept of 'Unrestricted War' and the creation of SSF it is amply clear that wrecking havoc on the internet is amongst the primary instruments of semi-warfare, quasi-warfare, and sub-warfare, that is, the embryonic form of another kind of warfare. The SSF maintains dedicated regional branches at the five joint force Theatre Commands and national-level elements of the Rocket Forces, the Air Force and the Navy, with distinct cyberspace command elements down to the Independent Operational Group (IOG) level in order to support combat operations particularly during major wars against sophisticated militaries.[xii]

The wartime information support missions include centralizing collection and management of intelligence collected by technical means; providing strategic intelligence support to theatre and IOG commands; enabling very long distance and power projection operations; supporting strategic defence in the space and nuclear domains and enabling three-dimensional joint operations through the intelligence, communications and informatization domains. The status of the SSF is defined as "perpetual mobilization" thereby denoting constant operations such as the collection and analysis of strategic intelligence. Thus "Network Reconnaissance" i.e. mapping computer networks and their communication nodes, as well as retrieving, collecting and analyzing information found in them and in associated computers and data collections.[xiii]

Targeted information could enable PLA cyber forces to build an operational picture of defense networks, military disposition, logistics, and related military capabilities that could be exploited prior to or during a crisis. The skills required for these intrusions are similar to those necessary to conduct cyber operations in an attempt to deter, delay, disrupt, and degrade operations prior to or during a conflict. In aggregate, these cyber-enabled campaigns threaten to erode military advantages and imperil the infrastructure and prosperity on which those advantages rely.[xiv]

Cyber Warfare Attacks against military and civilian computer networks are a main tenet in China's doctrinal precept to win the information superiority battle at the outset of any campaign. This can occur through a variety of ways including hacking, denial of service, and viruses, resulting in individual systems being taken offline or even the disruption of entire command and control networks. Cyber warfare could also be used as a standalone event or as a part of a larger offensive operation.[xv]

Information Warfare / Influence Operations

In the 2019's Annual Report to Congress: Military and Security Developments Involving the People's Republic of China a special topic on Influence Operations it has been brought to light that the PLA has emphasized the development of its Three Warfares strategy in its operational planning since 2003. Three Warfares is comprised of psychological warfare, public opinion warfare, and legal warfare. China views the cyberspace domain as a platform providing opportunities for influence operations and the PLA likely seeks to use online influence activities to support its overall Three Warfares strategy and to undermine an adversary's resolve in a contingency or conflict. Consistent with this strategy, China conducts influence operations against cultural institutions, media organizations, and the business, academic, and policy communities of the United States, other countries, and international institutions to achieve outcomes favorable to its security and military strategy objectives. The CCP seeks to condition domestic, foreign, and multilateral political establishments and public opinion to accept China's narrative surrounding its priorities like OBOR and South China Sea territorial and maritime claims. Chinese influence operations are coordinated at a high level and executed by a range of actors, such as the United Front Work Department, the Propaganda Ministry and the Ministry of State Security. [xvi]

China's response to the COVID-19 pandemic provides a below-the-threshold-of-war example of how it applies the IW trinity and attack vectors to achieve effective control. Under the CCP's guidance, China's informatized organizations used all means at their disposal to shape public opinion by controlling access to information, generating uncertainty about narratives that depicted China negatively, and appealing to the biases in each targeted population through misinformation.

China's filtering and fragmentation of information from health experts and journalists, its global delivery of misinformation narratives using social and mainstream media, and its efforts to generate uncertainty about the nature of the virus by comparing its severity to the common flu while suggesting that it originated from the United States, all demonstrate the aggressiveness and robustness of China's IW capabilities.[xvii]

The PRC's Ministry of Culture and Tourism which filters exposure to China's country and culture by arranging free and low-cost trips for journalists, politicians, sports stars, and other social influencers. This is done with the aim of long term physiological operations in mind to present a non-critical view of China when grassroots foreign support is needed.[xviii]

Simultaneously, China denies access to individuals and corporations who portray China or the CCP in a negative light or who express sympathies contrary to China's interests. This aggressive filtering extends to China's printing industry which openly censors the content of books printed within the country for exportby demanding the removal of content that portrays China negatively or that doesn't align with its strategic goals. It extends to the US sports and movie industries where threats to deny filming as well as lucrative distribution opportunities in China influence US production decisions while suppressing opinions counter to China's aims. It is notable that Hollywood has not made a movie critical of China since 1997; meanwhile China's National Film Administration recently directed the country's cinemas to show propaganda films a minimum of twice per week to commemorate the CCP's centennial anniversary.[xix]

China has a robust IW capability honed from decades of Information Operations (IO) performed against its domestic population and overseas adversaries. It is adept at using all elements of IW to achieve information advantage. This information advantage supports every Chinese national interest, and every national interest serves to reinforce the legitimacy and stability of the authoritarian CCP regime. [xx]

Cyber Espionage

The hacking and cyber espionage units receive their specific tasks and priorities solely from the very top i.e. Xi Jinping's CMC via the JOC in accordance with the national-level decisions made in the Forbidden City. These are mainly spying on foreign governments and institutions and/or acquiring sensitive technologies and know-how. Due to the political and security sensitivity only the SSF is involved in such operations and interaction with the Chinese industry happens only through special channels if there is a need to plant specialized components inside pieces of equipment produced in China.[xxi]

The PLA has invested heavily in offensive and defensive cyber capability. The Chinese cyber attacks and theft, ranges from breaches at the US Office of Personnel and NASA to various research universities and defense contractors. Unit 61398 of the PLA, for example, has stolen hundreds of terabytes of data about military personnel and seeks to disrupt US targets, communications networks, and computer systems. [xxii]
This organization also is meant to assist conventional PLA units with denial and deception efforts.

Logistics data is of great interest to PLA planners, areas such as specific unit deployment schedules, resupply rates and scheduled movement of materiel, unit readiness assessments, lift availability and scheduling,

maritime prepositioning plans, air tasking orders for aerial refueling operations and the logistics status of bases could be accessed. Reporting of attacks on US networks attributed to China suggests that these operators possess the targeting competence to identify specific users in a unit or organization based on job function or presumed access to information. The Chinese Counter Network Operations (CNO) operators may also attempt to attack US perceptions of the validity of data in these networks by uploading false records or corrupting existing records, possibly for intentional detection. The PRC's doctrinal orientation toward attacking an enemy's information flow suggests that if a classified network is attacked, it will likely be intended to impede encrypted traffic flow if it moves across an unclassified backbone rather than attempting to decrypt data or penetrate into the actual network. [xxiii]

Chinese actors are the world's most active and persistent perpetrators of economic espionage. Chinese attempts to collect U.S. technological and economic information will continue at a high level and will represent a growing and persistent threat to U.S. economic security. "The nature of the cyber threat will evolve with continuing technological advances in the global information environment. Sensitive U.S. economic information and technology are targeted by intelligence services, private sector companies, academic/research institutions, and citizens of dozens of countries. China is likely to remain an aggressive and capable collector of sensitive U.S. economic information and technologies, particularly in cyberspace. [xxiv]

The ability of PRC to leverage technology breakthrough, trends and research is by targeting the research and academic communities leveraging a dynamic, opportunistic and highly-competitive indigenous high-tech market environment and entrepreneurial culture, connections to Silicon Valley and the U.S. high-tech community, talent recruitment, especially the repatriation of Chinese nationals from the U.S. The targeting of high-tech industry and academic institutions by lure of China's commercial market for U.S. and Western firms and capacity to force U.S. companies to share data collected in China. [xxv]

To supplement the IW China seeks information advantage through hacking and other illegal *access* to advanced technologies and trade secrets from companies, universities, and the defence sectors of multiple nations. China's intellectual property theft has cost the United States upwards of $250 billion per year over the past decade, with some years exceeding $600 billion.[xxvi] According to the Policy Planning Staff of the Office of the US Secretary of State, China's annual intellectual property theft approaches the US military's annual defence budget and exceeds the total profits of the top fifty US companies. It has been called "the greatest transfer of wealth in history."

The benefits to China include access to specialized knowledge, enabling it to pursue additional information advantages against governments, organizations, and persons across the globe.[xxvii]

This presents the very concerning possibility that China's sustained efforts to gain *access* to the intellectual property of the breadth of US industry and defence contractors may compromise the *root of trust* of US hardware and software systems, generating *uncertainty* about the reliability of US networks and infrastructure. Finally, it presents the possibility that China may have more information about US weapon system capabilities and vulnerabilities than that possessed by the US government. [xxviii]

China's Haiyin Capital, a "government-linked fund," invested $1.2 million in Boston-based Neurala, an AI start-up that has "licensed its mapping and navigation software to NASA and the U.S. Air Force." [xxix]

The continued investment of PRC into technology companies across the globe gives them unprecedented access to the data, technology, knowledge and skilled personnel / talent to carry out research and development in dual use technology.

The scope, breadth and depth of the penetration of and spying on, all computer and communication networks by the PLA SSF is believed to be second only to by the US NSA. The security threats apply equally to all systems and/or components produced and assembled in China no matter if for Chinese companies, for Scandinavian companies, or for anybody else. Banning or limiting one company or another will have zero impact on the real threat to networks, computers and overall communications. Leading security experts have long concluded that all electronic systems, large and small should be considered potentially compromised, and not just by China. Indeed, it has long been the conviction of the UK GCHQ that everything is "dirty" irrespective of where it was produced. The working principle of the GCHQ is that 100% of all electronic systems - from industrial machines to laptops and mobile phones - "had been penetrated by third parties stealing information." [xxx]

Furthermore the report goes on to state China harnesses academia and educational institutions, think tanks, and state-run media to advance its soft power campaign in support of China's security interests. For example, Chinese students abroad and academic organizations are used to spread the Party's narrative on Tibet and the Dalai Lama. Chinese Students and Scholars Associations (CSSAs) and Confucius Institutes organize events to support China's sovereignty claims and lodge complaints and organize protests against academic institutions that conduct activities which differ

from China's polices. China's foreign influence activities are predominately focused on establishing and maintaining power brokers within a foreign government to promote policies that China believes will facilitate China's rise, despite China's stated position of not interfering in foreign countries' internal affairs. China's diplomatic outreach stresses building personal rapport with influential people, providing assistance, and emphasizing "win-win cooperation" through trade and diplomacy. This approach allows China to offer expedited, small-scale accomplishments for partners abroad, often in exchange for seemingly symbolic gestures that support China's long-term strategic goals. Some countries have begun to implement policy responses to Chinese influence activities, including within the European Union as well as Australia and New Zealand.[xxxi]

Thus PRC and PLA are leveraging all aspects of Information Operations and Espionage to enable Cyber, Information and Electronic Warfare. The increase in this capacity in has happened through the creation of the SSF and due to the emphasis laid by the PRC through CPC on these aspects.

Intelligentised Warfare using AI and allied technologies

Informatization and Intelligentization

The CCP is currently preparing its army to win Informatized Local Wars between information-based opponents.[xxxii] Xi restructured the PLA in 2015, including setting up the Strategic Support Force which conducts many aspects of IW. These include intelligence, technical reconnaissance, cyber espionage, cyber-attack, cyber defense, electronic warfare, and aspects of information technology and management. Some researchers claim that when Xi speaks of a "fully modernized force in 2035," he "no doubt envisions a PLA capable of conducting joint informatized operations in the context of systems destruction warfare, giving the CCP a tool to achieve political objectives while controlling the scope and scale of conflict." The PLA sees the information domain as "first and foremost in importance." It treats information dominance in the form of controlled and persistent *access* within the cyber, space, and Electro Magnetic Spectrum (EMS) domains early in a conflict as a pretext for achieving victory, while seeking to *fragment* or otherwise deny the same to its enemies.[xxxiii]

The Military Power of the People's Republic of China 2020, Annual Report to Congress, Office of the Secretary of Defense, United States of America covered a special topic of PLA'S Approach toward Informatization and Intelligentization, including Artificial Intelligence (AI). The report concludes that the PLA sees emerging technologies as driving a shift to "intelligentized" warfare from today's "informatized" way of war. Their strategists broadly describe intelligentized warfare as the operationalization

of AI and its enabling technologies, such as cloud computing, big data analytics, quantum information, and unmanned systems, for military applications.

These technologies, according to PRC leaders—including Chairman Xi Jinping— represent a “Revolution in Military Affairs” for which China must undertake a whole-of-government approach to secure critical economic and military advantages against advanced militaries. PRC would enable this shift by leveraging MCF development strategy and by reforming both its research and development (R&D) as well as strategy and doctrine organizations. In 2015, MCF was elevated to a national strategy, and it continues to establish new organizations and promulgate policies to drive development of dual-use technologies and further integrate civilian and military administration. In 2017, the PLA reorganized its military research and education institutes to synchronize advances in emerging technologies with the development of new operational concepts. The **Academy of Military Science (AMS), which has traditionally been responsible for writing new doctrine, now oversees several PLA science and technology institutes.**

According to the PLA, the implementation of “intelligentized” capabilities will increase the speed of future combat, necessitating more rapid processing and fusing of information to support quick and efficient command decision making after observation and orientation of the dynamic operating environment by using big data for more effective battle space management. Thus the PLA is concentrating on fusion of technologies like AI, autonomous command and control systems, more sophisticated and predictive operational planning and intelligence, surveillance & reconnaissance (ISR) to build a command information systems and decision aids for battlefield commanders.

Information superiority can only be achieved by targeting and degradation of the adversary’s command and control systems and future AI systems. This targeting and degradation would be done by autonomous unmanned systems and conduct information operations. These new unmanned aerial, surface, sub-surface and ground vehicles will enable new operational concepts and would require new C2 models.

The PLA is pursuing greater autonomy for unmanned platforms, to include swarm intelligence and manned-unmanned teaming capabilities, to provide more lethal kinetic that and non kinetic strike options that can saturate adversary defenses as well as more survivable and long-distance ISR capabilities, among other applications. The PLA also intends to improve its cyber and EW capabilities through AI-assisted network vulnerability analysis, countermeasure identification, and electromagnetic spectrum

management. PLA discussions of “intelligentized warfare” also acknowledge the difficulties of developing future technologies and implementing new capabilities. **The delegation of decision-making authorities to lower echelons may run counter to the PLA’s traditionally hierarchical and centralized C2 structure.** The PLA’s ability to leverage big data will depend upon its ability to obtain large quantities of high quality data on foreign militaries. Additionally, the complexity of future conflict probably will challenge the PLA to recruit, train, and retain the highly competent and technically proficient personnel necessary to understand and operate future “intelligentized” systems.

Digital Silk Road

The Military Power of the People’s Republic of China 2021, Annual Report to Congress, Office of the Secretary of Defense, United States of America covered a special topic of Digital Silk Road. The PRC’s **Digital Silk Road initiative**, announced in 2015 as a digital subset of One Belt One Road (OBOR), seeks to **build a PRC-centric digital infrastructure, export industrial overcapacity, facilitate expansion of the PRC’s technology corporations, and access large repositories of data.** The PRC also hopes the Digital Silk Road will increase international e-commerce by reducing cross-border trade barriers and establishing regional logistics centers by promoting e-commerce through digital free trade zones. **The PRC is investing in digital infrastructure abroad, including next-generation cellular networks—such as fifth-generation (5G) networks / fiber optic cables, undersea cables, and data centres.** The initiative also includes **developing advanced technologies including satellite navigation systems, artificial intelligence (AI) and quantum computing for domestic use and export.**

The 2017 National Artificial Intelligence Plan describes steps for the PRC to become the “world’s major AI innovation center” by 2030 and calls for the country to accelerate the integration of AI throughout the economy, society, and national defense. In **2020, the CCP reaffirmed its commitment to “intelligentization,” the PRC’s concept of future warfare based emerging and disruptive technologies, particularly AI.** In 2020, the PRC’s **Ministry of Science and Technology approtioned approximately $85 million to fund AI research.** It identified **22 research tasks including brain-inspired software and hardware, human-machine teaming, swarming, and decision making.**

Leveraging Private Sector breakthroughs in advanced dual-use technologies, and major PRC companies have significant research efforts aimed at generating breakthroughs in key fields. Under Beijing’s MCF strategy, the PLA seeks to exploit China’s private sector achievements to

further its force modernization plans. The **PRC has designated 15 companies as the country's official 'AI Champions' which include Alibaba, Baidu, Huawei, Sense Time and Tencent.** This designation tasks these companies to facilitate industry-wide coordination with the PRC government. **Each champion is responsible for a specific AI focus area,** including autonomous vehicles, smart cities and cyber security.

Tech giants Alibaba, Baidu and Tencent have been researching quantum computing since 2018, with Alibaba offering one of the world's few quantum computing clouds services. The PRC has two leading **quantum communications start-up companies, Quantum CTek and Anhui Qasky.** Quantum CTek, which had its initial public offering in June 2020, is becoming one of the largest manufacturers in the commercial quantum-communications technology sector. **The 2017 National Intelligence Law requires PRC companies, such as Huawei and ZTE and others, to support, provide assistance, and cooperate in the PRC's national intelligence work, wherever they operate**. [xxxiv] The PLA will certainly have access to the products of their AI investments. [xxxv]

The Chinese military is working hard to investigate, develop, and operationalize AI for military reasons, as part of Xi Jinping's mandate to become "completely modernised" by 2035 and at par with the US military by 2050. [xxxvi]

AI talent and technology acquisition

PRC's AI talent gap problem is being solved through recruitment of skilled Chinese citizens from abroad with experience and expertise in AI-related fields to support industry development. Many of these repatriated individuals were included in a June 2017 list published by Forbes of the 20 leading technologists driving China's AI revolution; a list that demonstrates the scale and impact of the repatriation of AI scientists and entrepreneurs from the United States to China. Eight of the top 10 named individuals had professional and/or educational links to the United States in the biographical profiles provided by Forbes. Overall, 16 of the 20 listed individuals had previous educational and/or professional experience in the United States, Japan or Western Europe. [xxxvii]

Chinese companies have in 2018 reportedly invested $700 million across 51 U.S. AI companies with some of these companies having links to the U.S. military and other strategically important government organizations. [xxxviii] This gives them access to all the technology developed by these companies.

AI on the Battlefield

The PLA's main strategy to defeat an adversary on the battleground is by creating disruption or paralysis of the adversary side through a system of systems operations. AI would play a central role in intelligentized warfare to target and crash key elements of opponent operational systems. A PLA Senior Colonel Li Minghai pointed out that algorithms, unmanned platforms and extreme domains are emerging factors contributing to the form of intelligentized warfare [xxxix]. Guo Ruobing, dean of the National Security College of the National Defense University of China, points out that the PLA should have a unique way of intelligentized warfighting, based upon Mao Zedong's concept that "You fight your way and we'll fight our way." Guo argues that only in this way can the PLA successfully develop technological and military abilities to seize a new force posture and create its advantages of "exploiting strength to defeat weakness" in the intelligentization era by developing its own AI military capabilities and target the vulnerable underbelly rather than competing in a full-spectrum confrontation.[xl]

The future information battlefield would be characterized by the seamless integration of "sensor-to-shooter" operations. PRC plans to achieve information dominance through the control of major combat front, key geographic location and critical timing of adversary operations by the use of EW throughout the various phases of campaigns. Successful EW also hinges on an accurate understanding of the interconnectedness of the geographic and information domains. Thus PRC doctrine advises "imposing cross-domain effects" on the adversary's weapon systems that rely on unimpeded access to the spectrum. [xli] To achieve the "reversed" cross-domain effect and information dominance, regional firepower strikes against critical targets at the right time are key, and should destroy the adversary's "intelligence, surveillance, reconnaissance, and early warning, navigation and positioning, command communications, and electronic countermeasures platforms." To achieve this PRC aims to have flexibility, controllability, and pervasiveness in such attacks, thus enabling warfighters to consolidate their capabilities to attack the enemy's "center of gravity" and destroy key nodes of enemy operation systems to paralyze their combat capabilities. The nodes identified are command hubs, critical information nodes, communications hubs, and critical networks. Creating advantages early in an assault is emphasised, therefore this needs to be achieved though the exploitation of vulnerabilities within the adversary's operational system of systems. As per the PRC the advancement of AI and machine learning can significantly accelerate the processing of thousands of unknown, new and unusual emitters that exist in a complex and constantly changing electromagnetic spectrum battlefield. Strategic Support Force-affiliated academic Wang Shafei [xlii]and his team reportedly have been focusing on cognitive EW for years. Maj. Gen. Lv Yueguang,[xliii] one of the

People's Liberation Army's foremost EW authorities, sits on China's national AI strategy advisory committee. [xliv]

PRC perceives speed of military decision making using AI as one of AI's major advantages. More specifically, AI is particularly fit for blitz tactics, where PLA could take advantage of speed in the attack so that it can de-motivate the adversary. Taking advantage of AI, the PLA is expected to focus on algorithms, unmanned platforms and extreme domains and develop the intelligentized "assassin's mace" weapons, mainly including precision guided missile, hypersonic glide vehicle (HGV), UAV, cyberattack, targeting vulnerabilities of battle network systems, to exploit its relative advantages to fulfill Anti-Access/Area Denial (A2/AD).

PLA would likely apply AI to the domain of cognitive warfare, a psychological approach which is in line with the traditional Chinese military wisdom that "the supreme art of war is to subdue the enemy without fighting" and "it is better to win the heart of the people than to capture the city."

PRC would use out-of-the-ordinary tactics such as disinformation, misinformation and influence strategies in propaganda warfare as a part of Cognitive warfare.

Deep fake, is one AI technology currently being developed by China to generate fake news, even video and satellite pictures, against rivals in an attempt to misguide opponents and regulate public opinion at home and abroad. [xlv]

Advancement over 2020 by the PLA is it seeing networked, technologically advanced C4I systems as essential to providing reliable, secure communications to fixed and mobile command posts, thereby enabling rapid, effective, multi-echelon decision-making. These systems are designed to distribute data including intelligence, battlefield information, logistical information, and weather reports via redundant, resilient communications networks to improve commanders' situational awareness. The PRC is also fielding the Integrated Command Platform to units at multiple echelons across the force to enable lateral and cross-service communications required for joint operations. Digital databases and command automation tools allow commanders to simultaneously issue orders to multiple units while on the move and enable units to quickly adapt to shifting conditions in the battle space.[xlvi]

PRC plans to apply AI at both the operational decision-making level and for frontline combatants for AI to work side-by-side with commanders. This may happen is through "battlefield perception systems" in which the computer

provides the commander with possible target sets to choose from, thus future warfare will become an arms race for which the state can produce computers that have the quickest computing capacity. Wartime commanders will be armed with supercomputers that will come to surpass the decision-making abilities of the humans directing them. PLA theorists call this “algorithmic warfare.” In PLA strategists view, frontline combatants will be gradually phased out and replaced with intelligent swarms of drones that will give operational commanders complete control over the battlefield. [xlvii] Chinese theorists believe that drones will have the strongest impact in the air domain, where unmanned aerial vehicles (UAVs) would have two major impacts on air warfare. The first is called “swarm warfare,” wherein masses of intelligent robots overwhelm the enemy. The second, called “unmanned-manned cooperation,”envisions “mothership” fighters directing groups of unmanned systems. The tactical level of warfare will almost entirely be comprised of robots, with computer-enhanced commanders perfectly directing automated robotic frontline combatants. The PLA’s goal will be to outsmart the enemy and reduce the adversary’s will to resist. The CCP recognizes the extraordinary potential of quantum computing and is investing billions of dollars into its development, directing the cooperation between the public and private sectors with “Military-Civil Fusion” and drawing the greatest minds to efforts with the “Thousand Talents Plan”. The “The Thousand Talents Plan” website was established in June 2010, under the guidance of office of high-level overseas talents recruitment, the organizing department of the Central Committee of the Communist Party of China. The aim was to gather the global wisdom. This website served as a bridge between the talents and the service institutions, to promote the innovation and development of the talents and their recruitment. The web site was aimed at high-end talent and service agencies. [xlviii]

The use of AI in military decision making is analysed by Jiang Zhu, Chuanhua Wen, Jun Chen, Xiangyuan Huang, “A Personality-Based Combat Behaviour Modeling Architecture and Methods”, Artificial Intelligence and Robotics Research, Vol. 08, No.04, 2019. [xlix] A group of military experts from PLA’s Army Command College at Nanjing, Jiangsu has sought to model a combat system or entity, based on a personality. Since psychological and physical behaviour are intricately linked, their study uses Boyd’s OODA loop sequence as a heuristic device by creating corresponding internally driven psychological model along the lines of ‘Necessity-Motivation-Behaviour-Effect’ (NMBE). The experts concluded that AI will help trained commanders, whose personalities are mapped, providing a rich model for algorithm-based genetic optimisation that captures the complexities of commanders and how they respond to tactical situations. It will, according to Chinese analysis, potentially improve combat training for new recruits by creating realistic operational and combat scenarios tailored for a variety of missions. [l]

PLA's orientation to use AI supported decision making has been in the making for some time now, however at the moment tangible evidence is not available in the public domain to demonstrate full and effective usage of AI technologies by the PLA.

The current state of AI Weapons

In the new paradigm of Intelligentized warfare the "Confrontation of systems as the fundamental manner of confrontation" would be the norm and would not be limited to the defense sector or armed units. It is confrontational to all aspects of country i.e. political, economic, social and legal systems as well.

A paper by The Brookings Institution, has researched in great detail on "AI Weapons" and their relation to China's Military Innovation. [li] The specifics they give out about use of AI and other cutting edge technology of the PRC are:-

1. Chinese military officers with legal expertise have advocated a more direct incorporation of legal experts into the chain of command to provide legal support for operations and decision making.[lii] The PLA's Academy of Military Science also organized a conference in September 2019 to address the legal issues that arise with military applications of AI. [liii]

2. Historically, Chinese leaders have prized centralized, consolidated control over the military. They may therefore be generally disinclined to relinquish control to individual humans, let alone machines, fearing loss of the Party's "absolute command."[liv]

3. China is converting old Soviet tanks into autonomous vehicles [lv]

4. PRC's policy linking AI with nations socio-economic environment. It states that integration of (three modernizations) mechanization, informatization, and intelligentization of weapons and equipment by creating an integrated development environment for the "three modernizations" of weapons and equipment that is fully coordinated, open to crowd intelligence, and effective supervision. The integrated development of the "three modernizations" of weapons and equipment requires not only a good development model, but also a good development environment. An overall coordinated national socio-economic environment, national defense and security needs, and national development strategies.[lvi]

5. Within the PLAAF, the GJ-1 and its successor GJ-2 (frontline attack drones) are used for integrated reconnaissance and precision strike, including in support of joint operations. According to its designer, the GJ-2 is “highly intelligentized” and capable of operating autonomously, including in identification of the enemy and judgement of threats. [lvii]

6. In the near term, human involvement in command and control appears to be deemed necessary for technical reasons, and the Chinese military is actively exploring concepts that leverage synergies between human and artificial intelligence, such as that of “humanmachine” intelligent integration (人机智能融合).[lviii]

7. China’s stated commitment to ethical AI use principles is contradicted by the CCP prioritization of AI as an instrument for maintaining social control and coercion, enabling crimes against humanity in Xinjiang and beyond. [lix]

8. A notable nexus can exist between security/defense (安防) applications and the leveraging of these technologies for military purposes, including techniques for monitoring and manipulating public opinion with applications in influence operations.[lx]

   Therefore as of now it can be safely concluded that AI/ML techniques are being evaluated for use in a target detection and decision support in all the PLA services.

Electronic Warfare, Jamming, Satellite and PNT Technology

Electronic Warfare

PRC’s signals intelligence (SIGINT) has a large staff of trained linguists and technicians which make it well suited for oversight of the Computer Network Defence (CND) and Computer Network Exploitation (CNE) missions in the PLA. Since approximately 2002, the PLA has been creating IW militia units, [now called the Military Civil Fusion (MCF)] comprised of personnel from the commercial IT sector and academia, and represents an operational nexus between PLA CNO and Chinese civilian information security professionals. In early 2003, AMS published an account of a probable proof of concept initiative in the Guangzhou Military Region to establish IW militia units using local telecommunications companies as a base from which to draw personnel, financial support and infrastructure access, suggesting that the PLA was tapping its growing pool of civilian commercial IT expertise to aid military information warfare requirements. The Guangzhou Garrison created

four “Militia Information Technology Battalions” in local firms comprising of CNO and offensive and defensive EW units. [lxi]

Deception has always been a part of the CPC and PLA’s strategy. Thus it is but natural that the dark arts of EW and the invisible, complex, and congested electromagnetic spectrum battlefield provide them with a perfect tool. Therefore the use of highly technical, covert and deceptive SSF is truly appropriate to their goals. Electromagnetic dominance is about people & deception targets human decision-makers. PLA could target satellite by spoofing uplinks and downlinks supporting intelligence, surveillance, reconnaissance, communications, early warning, and navigation systems. The consequences could be significant for a joint force component commander’s planning, decision, and execution cycle, and complicate effective air, ground, and naval operations. To achieve this objective, PLA’s EW theory emphasises the deception strategy of “hide the real and inject the false,” affecting signals and information to mislead enemy operators and decision-makers. They also highlight the importance of surprise, as the perceived weaker side in a competition, PRC strategists advise employing asymmetric means to defeat the stronger rival, via a fast electromagnetic spectrum attack against a key vulnerability when least expected. PLA thinkers continue to emphasize integrated electronic and network operations, with added emphasis on the application of intelligent technological means such as big data analytics, cloud computing, and deep learning. EW is described as an “external disruption” while computer network attack is considered “destruction from within.”

EW utilizes electromagnetic energy to isolate, obstruct, and destroy enemy’s electronic systems, confusing enemy sensors, disrupt command and control and degrade joint operations while computer network operations injects viruses and malware into enemy systems to achieve the same effect on enemy combat system of systems. [lxii]

PLA is rapidly integrating special operations, EW and information-operations units into its joint structures. Additionally, the Peopels Armed Police and militia organizations are increasingly conducting operations in conjunction with conventional PLA forces. Over 60 percent of the conscripts have civilian jobs in engineering, chemical manufacturing or communications, they play key roles in the mobilization of active units. PRC’s unrestricted way of war relies heavily on proxy methodology and the use of forces with increasingly looser ties to the state. Those actors (cyber hackers / thieves) often receive significant financial and technological aid and, in some cases, benefit from PLA advisors who are directly involved to protect Chinese interests. [lxiii]

At the tactical level, the PLA is focused exclusively on detection of radio emissions in frequencies at the small-unit level. Additionally, the PLA developed acoustic and optical sensors that can quickly identify and track equipment currently in use by the West. Electronic-warfare battalions / individuals with easily procured handheld devices are embedded with PLA units to conduct jamming of radios and to interfere with other digital systems. The PLA developed the capability to physically target satellites critical to GPS systems. By targeting satellites, the PLA can drastically interfere with the thousands of devices that enable land navigation, the delivery of guided munitions, and the encryption of communications. Much of the technology can be transferred to anyone operating against our forces (Pakistan). This is in the same way that China's ancient tribute system forced foreigners seeking business to support policy objectives, the BRI creates infrastructure in developing countries through financial entrapment that fundamentally increases the mobility and power projection of PLA forces. The use of hybrid tactics by the PRC is increasing and this leads to reliance on proxy methodology and the use forces with increasingly looser ties to the state. These actors often receive significant financial and technological aid and, in some cases, benefit from PLA advisors who are directly involved to protect Chinese interests. [lxiv] The BRI creates infrastructure in developing countries through financial entrapment that fundamentally increases the mobility and power projection of PLA forces. In addition, China is increasingly exporting arms to nonaligned actors, which helps the PLA break out of the perceived Western encirclement by building relationships with other actors. Hezbollah, Iran, Pakistan, and several African states currently possess Chinese-made air defense and missile systems. These arms sales, totaling $20 billion in just four years, typically accompany other BRI projects and have few strings attached [lxv]

The PLA's desired end state is likely to have every squad/ section to be equipped with a secure, reliable radio communications capability and to extend a secure, reliable network data capability down to the platoon level mounted on backpack or vehicle systems. The Air defence & Artillery combat systems are part of a theatre wide sensor-to-shooter network on a two-way system that integrates observers and guns over secure data and voice networks. Electromagnetic attack and defense capabilities are linked to tactical commanders, and they support tactical-level operations.

Company and battalion radio networks are built around a powerful tactical command post radio, with a series of either man-packed or vehicle-mounted radios connecting to an encrypted network. PLA communications units employ both satellite-based tactical communications and terrestrial data networks. Satellite communications have a limit on bandwidth, and they and are reserved for the highest-priority networks. [lxvi]

PRC has formed new military units to achieve dominance in the spectrum and centralized space, cyber, electromagnetic warfare capabilities and potentially psychological warfare. PRC has fielded several types of unmanned aerial vehicles with electromagnetic warfare systems and also begun to practice, evaluate, and improve the use of spectrum-related capabilities in training events where units jam or confuse communications, sensors, and satellite navigation systems. [lxvii]

To deter adversaries both militarily and psychologically, the PRC has advocate the deeper integration of computer networks into electronic warfare, to be used alongside precision kinetic strikes. Anticipating a fast-paced future battlefield, they appear to be poised to apply advanced technology such as AI and machine learning to the task of strengthening their EW capabilities. The “soft” and “hard” kill capabilities of EW are discussed in the Chinese writings. The term “soft” refers to operations causing disruptions to enemy’s electronic information systems, while “hard” mainly refers to the use of electronic weapons, such as anti-radiation missiles, high-energy lasers, and electromagnetic pulse weapons, to cause direct damage to enemy equipment. PRC prioritizes “national and military decision-makers” as key targets for strikes under its EW operations. Other important targets are identified as “national information infrastructure,” “strategic early warning systems,” “the military information system,” and “communications systems within the financial, energy, and transportation systems.” The “soft” kill is the exploitation of the electromagnetic spectrum, to “paralyze” and / or “hijack” the adversary’s systems to achieve a holistic objective of influencing enemy decision-makers. This may be used in conjunction with other political, diplomatic, economic, science and technology or cultural tools that are non-military in nature to achieve maximum effect. [lxviii]

PLA EW units routinely train to conduct jamming and anti-jamming operations against multiple communication and radar systems and Global Positioning System (GPS) satellite systems during force-on-force exercises. These exercises test operational units’ understanding of EW weapons, equipment, and performance but they also enable operators to improve confidence in their ability to operate effectively in a complex electromagnetic environment. In addition, the PLA reportedly tests and validates advances in EW weapons’ R&D during these exercises. The PRC presents a sophisticated, persistent cyber espionage and attack threat to military and critical infrastructure systems. The PRC seeks to create disruptive and destructive effects— from denial-of-service attacks to physical disruptions of critical infrastructure— to shape decision-making and disrupt military operations at the initial stages and throughout a conflict. Authoritative PLA sources call for the coordinated employment of space, cyber, and EW as strategic weapons to “paralyze the enemy’s operational system of systems”

and “sabotage the enemy’s war command system of systems” early in a conflict. The PLA also considers cyber capabilities a critical component in its overall integrated strategic deterrence posture, alongside space and nuclear deterrence. PLA studies discuss using warning or demonstration cyber strikes against select military, political, and economic targets with clear awing effects—as part of deterrence. [lxix] Accordingly, the PLA probably seeks to use its cyber warfare capabilities to collect data for intelligence and cyber attack purposes; to constrain an adversary’s actions by targeting network-based logistics, C2, communications, commercial activities, and civilian and defence critical infrastructure; and, to serve as a force-multiplier when coupled with kinetic attacks during armed conflict. The PLA’s recent structural reforms may further change how the PLA organizes and commands IO, particularly as the SSF continues to develop its capabilities and further integrate into joint planning, exercises, and operations with other PLA forces. The SSF likely is generating synergies by combining national-level cyber reconnaissance, attack, and defence capabilities in its organization, alongside other strategic IO capabilities. [lxx]

Weapons such as non-nuclear electromagnetic pulse weapons or high energy lasers are frequently noted by influential military as a disruptive means to paralyze an adversary’s military and entire society. The trend of putting [lxxi] conventional electromagnetic bombs and strategic laser weapons into use has accelerated, which highlights the role of strategic countermeasures as a winning factor, providing military planners with new means for strategic deterrence.

Jamming

Satellite images of China’s island fortresses in the Spratly and Paracel Islands have revealed the presence of large arrays of antennas and satellite dishes. Now China’s been seen rapidly expanding facilities near a town called Mumian on Hainan Island. It’s a battle on many electronic fronts. It’s a domain co-ordinated by China’s Strategic Support Force. Their sensor arrays can detect record and analyze any transmission such as radar in the region. They can attempt to decipher intercepted communications. They can track and communicate with satellites. They can blast targeted areas of the radio spectrum with raw energy to jam signals and the operations of specific electronics. They can manipulate the data being transferred over the airwaves. [lxxii].

The J-16D can effectively counter hostile advanced air defense systems of early warning, command and communications as well as interception and strike.[lxxiii]

SLC-7 L-band 3D surveillance radar system can track stealth aircraft, helicopters, drones, cruise missiles, near-space targets, and artillery shells and rockets, and can detect and track multiple targets simultaneously, withstand saturation attacks, adapt to jamming & rapidly identify targets.[lxxiv]

CHINESE SLC-7 RADAR AND YLC-48 PORTABLE MULTIPURPOSE RECONNAISSANCE RADAR

China is pushing to develop anti satellite weapons with capabilities from "dazzling to jamming, to kinetic kill from-the-ground, from space – all that, they're on the march," Rear Admiral Michael Studeman [lxxv]

A non-kinetic capability involves using directed-energy weapons such as lasers, high-powered microwaves, and particle beams. Specially configured lasers, for example, can be aimed at satellites with EO sensors and "dazzle" those sensors, temporarily blinding them while they are within the line of sight of the laser source. Co-orbital spacecraft can also engage in non-kinetic "blinding" operations. For example, these spacecraft could employ "umbrellas" or "spray paint" to block the view of an adversary's sensors. The PLA can also rely on jamming of enemy space assets. China, for example, can already jam the GPS signal. Another example of non-kinetic capabilities in space involves cyberattacks, which could be directed at targets such as satellite ground control stations. [lxxvi]

Space and Satellite Technology

To understand the current state and the future state of PRC's space capabilities the best source of information is a white paper titled "China's Space Program: A 2021 Perspective" on Jan 28, 2022. [lxxvii]

The paper sets out PRC's vision as strengthening its space presence in an all-round manner, to enhance its capacity to better understand, freely access, efficiently use, and effectively manage space; **to defend national**

security, lead self-reliance and self-improvement efforts in science and technology, and promote high-quality economic and social development; to advocate sound and efficient governance of outer space, and pioneer human progress; and to make a positive contribution to China's socialist modernization and to peace and progress for all humanity.

The paper also states China's space industry serves its **major strategic needs** and targets cutting-edge technology that leads the world. Spearheaded by the major space projects, the country has accelerated research into core technologies, stepped up their application and redoubled its efforts to develop space technology and systems. As a result, China's capacity to enter and return from space, and its ability to engage in space exploration, utilization and governance have grown markedly along a sustainable path.

The paper adds capabilities like high resolution multi-mode imaging satellite, a hyper-spectral observation satellite, satellite communications & broadcasting system, navigation and positioning satellite technologies. These are all dual purpose technologies.

In the next five years, PRC will continue to implement its manned spaceflight project, lunar exploration and planetary exploration. Build commercial launch pads and launch sites to meet different commercial launch needs and also strengthen the deep-space Telemetry, Tracking and Command communications network to support missions probing the moon and Mars. Currently PRC has launch sites covering both coastal and inland areas, high and low altitudes and various trajectories to satisfy the launch needs of manned spaceships, space station modules, deep space probes and all kinds of satellites. In addition, its first sea launch site has begun operation. These activities are aimed at positioning PRC as a space super power.

Further targets for the next five years are focus on new technology engineering and application, conduct in-orbit tests of new space materials, devices and techniques and test new technologies like Smart self-management of spacecraft, Space mission extension vehicle, Innovative space propulsion, In-orbit service and maintenance of spacecraft and Space debris cleaning. PRC would use space experiment platforms such as the Tiangong space station, the Chang'e lunar probe series, and the Tianwen-1 Mars probe to conduct experiments and research on biology, life, medicine, and materials, to expand humanity's understanding of basic science. To add PRC would employ its space station to conduct space-based astronomical observations, earth science and research, and space science experiments under conditions of microgravity and would also

promote more extensive international cooperation in astronaut selection, training, joint flights and other fields.

Since 2016, China has signed 46 space cooperation agreements or memoranda of understanding with 19 countries and regions and four international organizations. It has actively promoted global governance of outer space, and carried out international cooperation in space science, technology and application through bilateral and multilateral mechanisms. It also aims to step up its efforts to become a world centre for talent and innovation in space science, and create favourable conditions for the development of professionals and the expansion of their ranks. It will improve the personnel training mechanism fostering a pool of strategic scientists, leading and young scientists, and teams with strong innovation capacity, and cultivating a large number of outstanding engineers, top technicians championing fine craftsmanship, and visionary entrepreneurs with a sense of social responsibility.

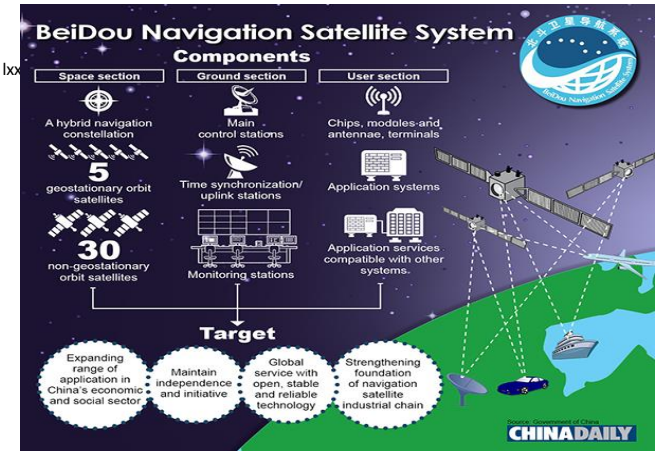
The above have and would invariably help them gain access to space technology and talent across the world.

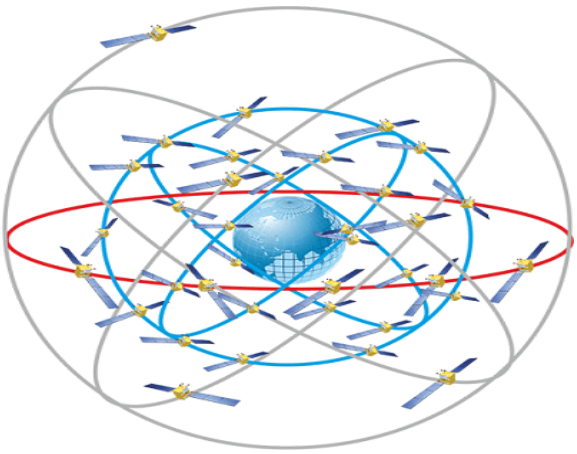
PNT Technology

BeiDou satellite constellation was originally slated to be fully operational in 2020, but the date was brought forward. BeiDou deliver accuracy down to five metres in Asia-Pacific and ten metres elsewhere. Its velocity accuracy is 0.2 metres per second, its timing accuracy is 20 nanoseconds. BeiDou has 33 satellites – 15 BDS-2 satellites and 18 BDS-3 satellites. Another twelve satellites, which will improve accuracy, are scheduled to be launched. The next country to get a satellite navigation system is expected to be India which is building the Indian Regional Navigation Satellite System (IRNSS), dubbed NAVIC. [lxxviii]

The BeiDou Navigation system has 5 Geostationary & 30 non Geostationary satellites. [lxxix]

lxx





China plans to launch numerous new communications satellites in the coming years and this may expand the availability of satellite networks to lower echelons. The PLA's relationship with Chinese civilian telecommunications networks has enabled civilian networks were built with PLA requirements and as a result, the PLA can employ domestic cellular and landline networks for both voice and data communications.[lxxxi]

The science of avoiding detection has progressed rapidly, including a new proposal to coat a satellite in composite materials to absorb radar waves. A research team in Nanjing, Jiangsu province has developed stealth technology for use by small satellites to blind radar detection.[lxxxii]

This provides a very clear indication on the importance on the militarization of space by the emphasis on leveraging space for strategic and military needs, by the implementation of dual use technology.

Quantum Communications

PRC's apprehensions on U.S surpassing them in the field of quantum technology and overwhelm China's air defences and assault its command-and-control systems, therefore China's central and provincial governments, the Chinese Communist Party (CCP), all PLA branches, and the country's state-owned and privately-owned industries are all working together. As a result, China's central and provincial governments, the CC, and all branches of the party are taking part in a whole-of-society strategy. [lxxxiii]

Satellite based

In 2016, China launched its first quantum satellite, nicknamed "Micius" from its Jiuquan Satellite Launch Center. A few months after this Quantum Experiments at Space Scale (QUESS) mission took place, it was reported that by beaming photons between the satellite and two distant ground stations, scientists had shown that particles could remain in a linked quantum state at a record breaking distance of more than 1,200 kilometers. That phenomenon, known as quantum entanglement, could be used as the basis of a future secure quantum communications network. [lxxxiv]

This satellite was to be in orbit for two years i.e. 2018 and was to be followed by the launch of Micius 2 and Micius 3 satellites. [lxxxv] There seems to be no evidence of any other satellite launched. The only purpose for using the satellite was for 'unhackable' secure communication.

Total bandwidth of the ground network is around 20 kilobits per second, while the speed of ground-space transfer is about five kilobits per second.[lxxxvi]

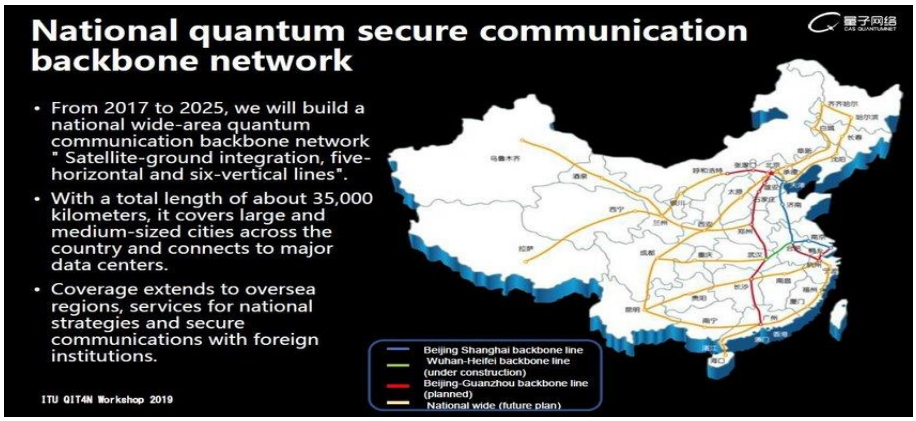
In Sep 2021, PRC has sent a packet of quantum information from Tibet to the Micius satellite in orbit, up to 870 miles (1,400 kilometers) above the Earth's surface — a record for teleportation. Scientists (Munro[lxxxvii] & Wiseman[lxxxviii]) note that often people think of teleportation as moving an actual object (or a photon) form one place to another. "People have this 'Star Trek' approach," Munro said. "They think of atoms being teleported. "What we're moving is information from one [quantum] bit to another [quantum] bit. There's not matter — only information. That's hard to get your head around." [lxxxix]

Chinese researchers have already built a satellite that can send quantum-encrypted messages between distant locations, as well as a terrestrial network that stretches between Beijing and Shanghai. [xc]

Ground based

Professor Pan Jianwei, a quantum physicist at the University of Science and Technology of China in Hefei, noted, "We learnt after the Edward Snowden affair that we are always being hacked." Pan added that "since most of the products we buy come from foreign companies, we wanted to accelerate our own program. This is very urgent because classical encryption was not invented in China, so we want to develop our own technology." This almost certainly lead to the start of the Quantum Experiments at Space Scale (QUESS) program aimed to build a quantum key distribution network by 2020 and a global quantum communication network by 2030. Chinese scientists will also use QUESS to test "other quantum technologies such as photon teleportation, transmission error reduction and random number generators." PRC also reportedly "unveiled the world's first "unhackable computer network," known as the Jinan Project, in August 2017. [xci]

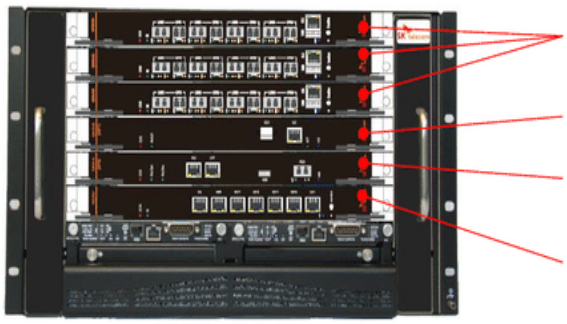
The image shows the quantum communication projects in PRC.[xcii]



The project “uses the city of Jinan as a quantum computer hub” to boost a quantum network between Beijing and Shanghai, due to its central location between the two cities. The network is over 2,000 kilometers (km) (1,250 miles) long and will be used for communications between government entities and the financial districts of the two cities. One test of the system successfully completed a transaction from Shanghai to Beijing at the Bank of Communications over the quantum network. Quantum computing-related projects have focused on quantum radars and remote sensing, quantum navigation and quantum communications. China is also looking at quantum communications as a possible secure underwater communications route. The next stage for China’s quantum satellite project is to launch another satellite into a higher orbit, possibly 20,000 km (about 12,427 miles), to cover a larger part of the Earth’s surface. By 2022, China plans to put a quantum communications payload on its future space station. The payload could be maintained and upgraded on the space station by humans, unlike the systems on satellites. The ultimate goal is a world-spanning network of quantum satellites in geostationary orbits.[xciii] This target was already achieved before the timeline and the details are provide later.

After a test in November 2021, Chinese scientists claimed that their quantum computer completed a task in a little over an hour that would take today’s fastest supercomputer eight years to finish, these machines could serve as the robotic assistants that Chinese strategists envision helping operational commanders draft battle plans and select ideal target sets. [xciv]

The hardware used for quantum communication is also depicted below.[xcv]



ATCA	
Chassis size	19 inch, 12U (14 slot) / 6U (6 slot); Shelf supplier dependent
QKD unit	2 slot
10Gbps encryptor unit	1 slot (bidirectional 4 ch.) ※ Max 80 slot (800Gbps)
Quantum key distribution	
Secure key rate	> 10 kbps @ 50km
Protocol	BB84 with unique phase modulation + decoy protocol and modified Winnow error correction
Random number generator	High speed quantum random number generator (2 Gbps)
Encryption	
Network protocols	10 GbE, STM64 (10 G SONET/OTN, 40G/100G Ethernet/OTN planned to be provided)
Algorithm	AES-GCM or ARIA-GCM
Latency	< 10 microseconds
Random number generator	Quantum random number generator

In July 2018, [xcvi] Chinese scientists claimed to make another breakthrough in quantum communication, demonstrating long-distance free-space quantum key distribution during daylight. In the past, the process could only be performed at night, because sunlight or sunlight noise prohibits quantum communication in transmission under conditions of high channel loss over long distances.[xcvii]

A 48 second video on the command centre of the world's terrestrial line for secure quantum telecommunications, known as the Jing-Hu or Beijing-Shanghai, Trunk Line connecting Beijing, Jinan, Hefei and Shanghai is available in open source. [xcviii]

In ground-based quantum communications, however, the optical fibers that connect two locations absorb transmitted photons, and the rate of absorption increases over distance. “Trusted nodes” placed along the fibers decrypt and reencrypt keys to extend the key-transfer distance. But like Micius in the 2017 demonstration, each of these intermediaries possesses all the quantum keys and is thus vulnerable to hacking. Although prototype devices called quantum repeaters offer better security, the technology is not yet advanced enough to be practical. [xcix]

Underwater

China is reportedly looking at quantum communications as a possible secure underwater communications technique, which could provide China’s future UUVs and submarines with a novel capability to support undersea surveillance/ASW operations as well as more offensive missions. On-going programs in quantum navigation and position offer an opportunity to navigate with greater accuracy in environments in which GNSS satellites are denied or degraded, which would improve capabilities of MaRVs and unmanned systems as well as targeting for HVPs. [c]

There is a grand plan by PRC to use quantum encryption for communication, however translation into military usage, would happen in due course of time. This certainly may lead to more secure military communication within the PLA.

Microwave Weapons

It has been reported that in August 2020 China uses microwave weapons to blast Indian troops in disputed border region, the PLA is said to have used “high-energy electromagnetic radiation” technology to effectively turn “two strategic hilltops that had been occupied by Indian soldiers into a microwave oven”. The attack left the Indian troops “vomiting” and unable to stand within 15 minutes, enabling the People’s Liberation Army to “retake two

strategically important hilltops in the Himalayas without any exchange of live fire". [ci]

Jin Canrong, Professor at the School of International Studies, Renmin University, Beijing, told his students about it this week!

Microwave weapons boil water molecules under the skin, and they do this from up to 1 km (0.6 miles) away. Professor Jin[cii] even waxed lyrical: Chinese technology" turned the mountain tops into a microwave oven". This news was first reported in The Times newspaper, UK on 17 Nov 2020.

This news was dismissed as fake by Press Information Bureau & ADGPI of the Indian Army. [ciii]

Cloud Seeding

A study by Tsinghua University [civ] reveals that the Chinese government used 'cloud seeding' to control rain and reduce pollution in Beijing, in preparation for its Communist Party centenary event. In this instance, the cloud-seeding operation in Beijing was extensive - taking two hours overall. The study said rockets were carrying silver iodine into the sky to stimulate the rainfall. So cloud seeding is a common procedure for clearing the skies in China - with the government having spent billions of Chinese Yuan on efforts to manipulate the weather over the last 13 years, ever since the 2008 Olympic Games. Xu Xiaofeng, a former deputy director at the China Meteorological Administration stated that "Weather modification is not only a scientific problem but also a social engineering project closely related to [a country's] interests, environment and responsibilities," in an October 2021 paper published in Chinese journal Advances in Meteorological Science and Technology. [cv]

China arguably has one of the largest cloud seeding and weather modification operation in place with reports saying that in the five years till 2017 Beiijing had spent more than USD 1.3 billion on the technology to induce more than 200 billion cubic meters of rain it wouldn't have otherwise received.

In fact, in December 2020, the Chinese government said that "by 2035, China's weather modification should arrive at a worldwide advanced level in terms of operation, technologies, and services" and that the "total area of artificial rainfall (snowfall) operation will reach beyond 5.5 million sq.km, and for hail suppression it should go beyond 580,000 sq.km". [cvi]

This technology could be used to hamper military operations and also to create heavy rainfall to destroy certain areas by triggering landslides / cloud bursts.

Other Technologies

New Military Technologies[cvii] that the PLA plans to use in war fighting are a mix of 4IR and interrelated technologies.

According to Military Power of the People's Republic of China 2021, Annual Report to Congress, Office of the Secretary of Defense, United States of America, the PLA is pursuing a number of advanced military capabilities with disruptive potential such as autonomous systems, hypersonic weapons, electromagnetic railguns, directed energy weapons and counter space capabilities. Many technologies associated with the 4IR such as AI, smart sensors, 3D printing, Internet of Things platforms, and wearable electronics hold significant developments involving the PRC's promise for battlefield applications.

The PRC is developing unmanned systems in all domains and has tested unmanned air, ground, and maritime systems with limited AI capabilities. Potential military applications of some emerging technologies include AI and Advanced Robotics, enhanced data exploitation, decision support, manufacturing and unmanned systems integration to support C4ISR. Semiconductors and Advanced Computing possibly used for enhanced cyber operations and weapons design, and shortened R&D cycles.

Quantum Technologies to secure global communications, enhanced computing and decryption capabilities, enhanced position, navigation, and timing (PNT) capabilities.

Biotechnology used as a precision medicine, biological warfare, enhanced soldier performance, human-machine teaming.

Hypersonic and Directed Energy Weapons to conduct global strike and defeat of missile defense systems, and anti-satellite, anti-missile, and anti-unmanned aircraft system capabilities.

Advanced Materials and Alternative Energy for improved military equipment and weapon systems Military requirements are part of China's rail development, and the PLA actively participates in the design and planning of China's high-speed rail (Xinhua News Agency, December 7, 2010). Chengdu Railway Bureau had 14 military officers to take lead positions in key departments at all major stations, such as coordinating railway planning,

design, construction, timing of requirements and track implementation (Xinhua News Agency, December 7, 2010) [cviii]

Technology has enabled wars to be conducted remotely by means of Mid and long range accuracy strike as the determining method of operation. Unification of information and artillery as the main method of operation as Information technology enhances the accuracy of distance striking, and informational attacks can cripple the ISR of an adversary. The Area of operation expands from three-dimension to five-dimensions i.e. the land, air, sea, space and cyberspace. Time is a key component in modern war as the fast-movers dominate the slow-movers using unmanned, invisible and inaudible weapons and military operations technology.

As of May 2018 several core technical areas in which PRC had reached a stage of substantial development in individual advanced weapons systems programs like Anti-satellite (ASAT) missiles, Co-orbital satellites, Directed energy weapons, commercial and military unmanned aerial systems, Maneuverable Re-entry Vehicles (MaRVs), Hypersonic glide vehicles, Anti-ship ballistic missiles, Directed Energy Weapons with a capability of close-in defense, jamming of platforms and systems, missile defense, non lethal weapon for crowd control during civil unrest, Lasers, Microwave and radio frequency weapons and also Electromagnetic (EM) Railguns (like Naval railguns, Land based railguns and Handheld railguns) which use electromagnetic energy rather than a chemical reaction to strike targets with projectiles at speeds up to Mach 6. As on date these systems would have surely developed to an advanced stage.

In addition to the above PRC could use 3D printed payloads and parts, Shape-shifting and self-healing platforms, Biomaterial-infused “invisibility cloaks” and also to harness the power of emerging technologies for military purposes like Artificial intelligence (AI), Big data analytics, Internet-of-Things, Virtual and augmented reality (VR and AR), Smart sensors, 4D printing and synthetic biology manufacturing, robotics and unmanned systems, Novel and smart materials, Quantum computing and encryption, Semiconductors and Energy capture and storage technologies [cix]

Hypersonic Weapons

In 2019, China displayed a hypersonic glide vehicle designated the DF-17 at a military parade, leading experts to believe the weapon was in service with the People’s Liberation Army (PLA). The DF-17 is mounted atop a ballistic missile. According to US intelligence estimates, the DF-17 has a range of around 2,500km and moves at between five and 10 times the speed of sound. US experts have postulated that the DF-17 could be equipped with either conventional or nuclear warheads. They have also expressed

concern China could develop a variant of the DF-17 meant to target aircraft carriers at sea. [cx]

Technology

To aid research and development into hypersonic technology, the Chinese Academy of Sciences' Institute of Mechanics (IMECH) launched the JF-12 "shock tunnel reproducing hypersonic flight conditions" program in 2008. It became operational in 2012. The JF-12 tunnel is reportedly being used to develop Starry Sky, which can carry nuclear warheads and travel at six times the speed of sound. The JF-12 can duplicate flight conditions from Mach 5 to 9 speeds and altitudes from 25km to 50km. The tunnel can sustain test times of more than 130 milliseconds, which is enough to support the data collection of flow field, shock structure and other high-speed aerodynamic parameters to help design hypersonic weapons.[cxi]

China reportedly conducted successful tests of the Starry Sky-2 (Xingkong-2) hypersonic cruise missile in 2018. This system is believed to have a range of 700-800km and a top speed of Mach 6. The missile appears to make use of an experimental "waverider" design that uses powered flight after launch and creates shockwaves to sustain its lift. In its test phase, the Starry Sky-2 vehicle was sent into space by a multi-stage rocket before separating from its booster for maneuvered flight back to Earth. Some analysts have suggested that this technology could emerge in the mid-2020s as an advanced anti-ship missile.[cxii]

Hypersonic weapons can travel much faster than current nuclear-capable ballistic and cruise missiles at low altitudes, can switch direction in flight and do not follow a predictable arc like conventional missiles, making them much harder to track and intercept. A report in mid October 2021 said the Chinese military launched a rocket carrying a hypersonic glide vehicle that flew through low-orbit space, circling the globe before cruising towards its target, which it missed by about two dozen miles. The speculation of the secret launch emerged from the China Academy of Launch Vehicle Technology, which said that it had launched a Long March 2C rocket, the 77th launch in July followed by an August 24, 2021 announcement releasing details of a 79th flight, but there was no detail about the 78th launch, sparking speculations.[cxiii]

PLA missile scientists say the accuracy of hypersonic weapons could be improved by more than 10 times if control is taken out of human hands and given to a machine. The early October 2021 paper in the journal Systems Engineering and Electronics, proposes using artificial intelligence to write the weapon's software "on the fly" through a unique flight control algorithm as it travels at hypervelocity, thereby increasing the overall positioning

accuracy would increase by one to two orders of magnitude. In May 2021 Chinese space authorities announced plans to build a small passenger plane, capable of reaching anywhere on Earth in an hour, by 2035. This would require it to reach a speed of Mach 15. [cxiv]

Some experts also project that over time, China is likely to field conventionally-armed hypersonic vehicles with sufficient range to reach the United States in order to hold at risk key US military assets, critical infrastructure, and other high value targets. Beyond posing a coercive threat to the United States, China's military leaders may see conventionally-armed HGVs as important to developing a global power projection capability.[cxv]

China recognizes that it currently lacks sufficient capabilities in ultra-high-temperature ceramics and is seeking foreign assistance to help address this deficiency. As part of this effort, in 2017, Central South University in Changsha, Hunan announced a collaborative agreement with the University of Manchester from the U.K. to jointly develop a new type of ceramic coating material for use on hypersonic aircraft and spacecraft. [cxvi]

Countermeasures

On November 19, 2021 the US Missile Defense Agency announced Lockheed Martin, Northrop Grumman and Raytheon Missiles and Defense had been selected to design a surface-to-air missile that could intercept hypersonic glide vehicles. The weapon is meant to be fired from the US Navy's destroyers that are equipped with the Aegis battle management system. Russian officials have also claimed that the new S-500 surface-to-air missile system could shoot down hypersonic missiles and satellites. [cxvii]

Faced with an array of increasingly effective anti-missile countermeasures, China likely sees a combination of maneuverable ballistic missiles and hypersonic cruise missiles as necessary to overcome ships' defensive systems. The intensified development of hypersonic technologies should therefore be seen as complementary to the development of Anti-Ship Ballistic Missile (ASBM) technology. [cxviii]

Chinese scientists and engineers have clearly made real progress in both the theoretical and the practical aspects of hypersonic system development. The large number of test flighs and open source information indicate that at least some parts of China's hypersonic weapons programs have reached the last stages of development.

Technology and Espionage Capability Demonstrators

For a realistic understanding on the capabilities of the PRC (Reality vs. Hype) it is necessary to list a few events that demonstrate technology capabilities. These technology demonstrators have been listed starting with older ones first. This has been done so that the reader is able to comprehend the evolution, use and progression of the use of technology and cyber espionage by the PRC over the years.

1. In a June 2004 exercise among units in the Beijing Military Region, a notional enemy “Blue Force” used CNA to penetrate and seize control of the Red Force command network within minutes of the start of the exercise, consistent with the INEW strategy’s emphasis on attacking enemy C2 information systems at the start of combat. [cxix]
2. A long term, persistent campaign to collect sensitive but unclassified information from US Government and US defense industry networks using computer network exploitation techniques, long attributed to China, has successfully exfiltrated at least 10 to 20 terabytes of data from US Government networks as of 2007, according to US Air Force estimates and that figure has possibly grown in the past two years, though no figure is publicly available. [cxx]
3. In 2008, numerous computer systems around the world, including those owned by the U.S. Government, continued to be the target of intrusions that appear to have originated within the PRC. Although these intrusions focused on exfiltrating information, the accesses and skills required for these intrusions are similar to those necessary to conduct computer network attacks. [cxxi]
4. In April 2008, Government of India, confirmed that its Ministry of External Affairs’ computer network and servers were intruded by network traffic that appeared to originate in China. [cxxii]
5. In May 2008, the Belgian Government reported that it had been targeted by PRC hackers multiple times. [cxxiii]
6. Again in May 2008, U.S. authorities investigated whether PRC officials secretly copied contents of a U.S. Government laptop during a visit to China by the U.S. Commerce Secretary and used the information to try to penetrate into Commerce computers. [cxxiv]
7. China uses a variety of methods to acquire foreign military and dual-use technologies, including cyber activity and exploitation of the access of Chinese nationals, such as students or researchers, acting as procurement agents or intermediaries. [cxxv]

8. In 2011, computer networks and systems around the world continued to be targets of intrusions and data theft, many of which originated within China. Although some of the targeted systems were U.S. government-owned, others were commercial networks owned by private companies whose stolen data represents valuable intellectual property. These occurred in key sectors, including companies that directly support U.S. defense programs. [cxxvi]
9. China very likely uses its intelligence services and employs other illicit approaches that violate U.S. laws and export controls to obtain key national security and export-restricted technologies, controlled equipment, and other materials unobtainable through other means. [cxxvii]
    a. In November 2014, U.S. authorities arrested a named Chinese national employed by a U.S. defense contractor en route to China with sensitive proprietary documents containing equations and test results used in the development of technologically advanced titanium for U.S. military aircraft. Earlier, after the individual returned from a trip to China in August 2014, U.S. Customs and Border Protection officers found the individual in possession of undeclared cash, Chinese corporation-establishment documents, and a mostly-completed application for a Chinese state-controlled aviation and aerospace research center. The application claimed work on the engines for the U.S. F-22 and F-35 fighter aircraft.
    b. In May 2015, U.S. authorities arrested Chinese national Zhang Hao based on a 32 count indictment charging Zhang and five other named Chinese defendants with economic espionage and the theft of trade secrets. The indictment alleged Zhang and the other co-conspirators stole source codes, specifications, design layouts, and other documents related to thin-film bulk acoustic resonator (FBAR) dual-use technology from U.S. companies. The stolen material supported the creation of a Chinese FBAR fabrication facility and joint venture providing FBARs to commercial and military entities. [cxxviii]
    c. In addition, multiple U.S. criminal indictments and investigations since 2009 involve non ethnic-Chinese U.S. citizens and naturalized Chinese U.S. citizens or permanent resident aliens procuring and exporting controlled items to China. These activities included efforts to acquire and to transfer sensitive or military-grade equipment such as radiation hardened programmable semiconductors and computer circuits, restricted

microwave amplifiers, high-grade carbon fiber, export restricted technical data, and thermal imaging systems [cxxix]

10. In January 2015, Hu Xiaoxiang (扈晓 翔), a Chinese researcher enrolled in a doctoral program at the University of Agder in Norway, was deported from the country for alleged concealment of his ties to the PLA. Hu had been working on air-breathing hypersonic flight vehicles, supported by a Norwegian government grant for offshore wind energy research. [cxxx]
11. In June 2016, China tested the world's fastest supercomputer, the Sunway Taihu Light, which reportedly can make 93,000,000 calculations per second. The computer was made entirely in China with Chinese-made chips and is expected to be used to support big data analytics, among other tasks. Supercomputers have several military applications. [cxxxi]
12. In 2016, China launched its first quantum satellite, nicknamed "Micius," from its Jiuquan Satellite Launch Center. A few months after this Quantum Experiments at Space Scale (QUESS) mission took place, it was reported that by beaming photons between the satellite and two distant ground stations, scientists had shown that particles could remain in a linked quantum state at a record breaking distance of more than 1,200 kilometers. That phenomenon, known as quantum entanglement, could be used as the basis of a future secure quantum communications network. [cxxxii]
13. In June of 2017, China's CETC set a record for the world's largest drone swarm, successfully testing a swarm of 119 drones. This beat a record previously held by the U.S. Air Force. [cxxxiii]
14. In the first several months of 2017 China's biggest technology and Internet companies introduced digital assistants in January (Baidu's Xiaoyu Zaijia "Little Fish"), April (Tencent's DingDang) and July (Alibaba's Tmall Genie). [cxxxiv]
15. The U.S. Attorney General William P. Barr noted in his announcement of the indictment of People's Liberation Army hackers in early 2020: For years, we have witnessed China's voracious appetite for the personal data of Americans, including the theft of personnel records from the U.S. Office of Personnel Management, the intrusion into Marriott hotels, and Anthem health insurance company, and now the wholesale theft of credit and other information from Equifax.[cxxxv]
16. The best-known case is the surreptitious planting of tiny microchips (the size of a grain of rice) on computer motherboards produced in China for Supermicro, a US

company, and supplied to both sensitive government and corporate entities that was discovered a few years ago. The investigation of the Supermicro motherboards revealed that the actual design of the microchips originated with the PLA and that their insertion during the manufacturing process by SOE subcontractors was done by PLA operatives. This is the case even when the huge production facilities are officially owned by manufacturing private companies, be they Chinese or foreign, as well as SOEs. These companies own the facilities and production lines, however not the people therein. [cxxxvi]

17. After a test in November 2021, Chinese scientists claimed that their quantum computer completed a task in a little over an hour that would take today's fastest supercomputer eight years to finish, although there is no way to publicly confirm these findings. These miracle machines could serve as the robotic assistants that Chinese strategists envision helping operational commanders draft battle plans and select ideal target sets. With these computers, human ingenuity and robotic calculating ability could be married in heretofore unimaginable ways. [cxxxvii]
18. The PRC has a 2,000 km quantum-secure communication ground line between Beijing and Shanghai and plans to expand the line across China. The PRC also plans to have a satellite-enabled, global quantum-encrypted communications capability operational by 2030. [cxxxviii]
19. At the height of the border standoff between the PRC and India in 2020, the PLA installed a fiber optic network in remote areas of the western Himalayas to provide faster communications and increased protection from foreign interception. PLA field commanders view near-real-time ISR and situational data as well as redundant and reliable communications as essential to streamlining decision making processes and shortening response timelines. Digital databases and command automation tools allow commanders to simultaneously issue orders to multiple units while on the move and enable units to quickly adapt to shifting conditions in the battlespace. [cxxxix]
20. Athletes and other officials at the Beijing Winter Olympics (4-20 Feb 2022) were asked to install health apps. This is for certain being used to access to health data and other private information. In addition what the PRC agencies are after is the links / sympathetic attitude of any of them towards Xinjiang and the treatment of the Uighurs or maybe Tibetan activists. [cxl]

The Reality – Plethora of challenges

As dependency breeds weakness, the more PRC, PLA and SSF are dependent on technology, the easier it gets for the opposition to exploit. Informanisation and Intelligisation of the PLA could lead to its targeting and degradation by autonomous unmanned systems which conduct information operations.

Command and Control

The PLA leadership is adjusting to the PLA's senior staff bodies, in part by replacing the four general departments with six joint departments, three commissions, and five offices under the CMC, it may take some time for the transition to be fully functional and a well oiled C2 system. The CMC's tightening of military discipline with reforms to its Discipline and Inspection Commission, its Auditing Office, the PLA judicial system, and a new Politics and Law Commission may lead to larger lack of initiative from its rank to perform need based proactive operations and depend on the CMC to give clear orders.

Successful reform is not assured as many of China's previous attempts at military transformation have failed. The joint force will embrace a model of highly centralized decision making, which could prove ill-suited to the demands of major combat operations. The transformed PLA will struggle to integrate multidomain operations at the joint theater level. PLA could lack the capabilities to project, sustain, or command its forces across the spread of China's global interests. The PLA is currently hindered by a lack of Xi demonstrates a highly centralized style of decision making, even by Chinese authoritarian standards. During routine national management, a mix of negotiation, bargaining, and consensus-building were traditionally required to fully mobilize the Chinese polity. But in times of crisis, this fragmented and somewhat lethargic system would typically transform into a more centralized, autocratic system demonstrating greater ideological decision making, a pronounced monopoly of decision making by senior party leaders, and a severe constraining of any latitude previously granted to subordinates. [cxli]

Xi's reform of the CMC has strengthen political control of the PLA beyond the already high levels as he himself leads through a "CMC chairman responsibility system" in which even day-to-day defense matters elevate to him as CMC chairman thus depriving the government experience with decentralization and delegation. Any conflict with China should seek to maximize the number and variety of strategic challenges it faces to disrupt the CCP's efficient management of war. Enacting measures that promote internal disorder and force the PLA to focus attention and resources on

internal security would be one approach. The complicated relationship between the CCP and the PLA could be targeted. The two should be treated as separate entities; careful targeting may help divide the CCP and the PLA and diminish the overall unity of Chinese command. The creation of PLA into a joint force, increase its readiness for war, and prioritize operations in space, cyber, and electromagnetic domains; in reality, the reform will face significant impediments due to classic Chinese fragmented authoritarianism, the organizational frictions typical in any large structural change and structural vulnerabilities within the reformed PLA will still exist. Another major drawback that could be exploited is the centralised C2 of the Rocket Force and the SSF. These differences have the potential to hinder the integration of effects across all domains at the theater level during both joint training and war. The PLA has known deficiencies in its strategic airlift capabilities, constraining its ability not only to deploy forces out of area but also to redeploy forces the abroad, with command of global operations retained by the CMC. [cxlii]

In the information/ cyber warfare sphere there are many stake holders, the SSF is a directly answerable to the Joint Operations Command (JOC) under the Central Military Commission (CMC) that is chaired and run by Xi Jinping. The raw data that is collected by SSF is analyzed by the Intelligence Bureau within the PLA's Joint Staff Department. For the conduct of their routine operations, the SSF also has direct links to specific departments of the Communist Party of China (CPC), the Ministry of State Security (MSS - that is, Chinese Intelligence), the National Cyberspace Administration of China, etc. At the operational level, the Strategic Support Force is not the only command involved with PLA's integrated network and electronic attack missions. The Joint Staff Department's Network and Electronic Bureau is possibly also playing a part. Similar staff functions likely exist at the theater command level as well. Another entity is the Joint Staff Department Network Electronic Countermeasures Group that is attached to the Central Military Commission's Joint Operations Command and Control Center, which likely coordinates People's Liberation Army Air Force, Army, Navy, Rocket Force, and Strategic Support Force electromagnetic spectrum operations. This may lead to overlooking of certain responsibilities or degraded performance due to overlapping responsibilities. [cxliii]

The PRC believes that modern warfare requires using "all means, including armed force or non-armed force, military or non-military, and lethal and non-lethal means to compel the enemy to accept one's interests." Economic warfare, information warfare, cyber warfare, proxy wars, terrorism, and maneuver warfare all work in concert. Within this context, the Defense Intelligence Agency (DIA) estimates the core strengths of the PLA to be long-range fires, information warfare, and nuclear capabilities. Furthermore, it acknowledges the PLA's ever-improving power-projection capabilities and

SOF. The DIA assesses that the PLA will suffer from their rigid command structure, joint inexperience, and logistical woes in future conflict. [cxliv]

Theatre commands involved in a given contingency will heavily integrate PLA forces, the PAP, militia, and the other arms of its strategic support or rocket forces into the fight. Interestingly, political cadres continue to exist at each echelon and influence every decision. Although this “decision making by committee” may maximize input, it also creates implicit stove piping between party leaders. Furthermore, it likely prevents forthrightness between military leadership and civilian leadership. [cxlv]

The CCP’s vision for AI betrays the PLA’s predilection for over centralization of command authority and top-down orchestration of military assets. With operational commanders advised by computers directing smart swarms of drones, there will be few opportunities for distribution of efforts and lower-level initiative. AI is not destined to provide all of the benefits that the PLA hopes for. All algorithms necessarily mirror the presumptions that the AI designers hold and are often limited by them. In the past, technological revolutions have precipitated kinds of changes in warfare that contemporaries could never imagine. In future warfare, AI may not be able to adjust to the new realities and inherent uncertainties of warfare in the same way that humans can. The elevated status of intelligentization in Chinese doctrine will more closely couple the PLA’s warfighting capabilities with China’s continued technological development. If the PRC cannot continue to introduce new military innovations to the PLA, Chinese military doctrine will float adrift. China is showing accelerating signs of a flagging economy, with the headwinds of immense debt and a heavy demographic burden, among other challenges. In addition to technological limitations, competing resource priorities may also weigh on the PLA’s intelligentization potential. [cxlvi]

The existence of two clear lines of authority under the CMC gives the services authority over “force management” issues while the theatre headquarters command operations a distinction that was ambiguous in the past, however this may lead to conflicting priorities that could be exploited by the use of cyber, EW, Information and physiological operations.

Aggressive Targets

A plain comparison of Science and Technology Thrust/ Innovation, Foreign Technology Acquisition and Sourcing Science & Technology for Military Modernisation of the China Military Power report across 2009, 2016, 2020 and 2021 as accessed by United States, Department of Defence, establish many things in common and also highlights to a great extent that the aggressive targets set in the plans are not always met. This has mainly

been deduced from the transformation and the trajectory of the progress made on the key subjects.

Guo Ruobing, dean of the National Security College of the National Defense University of China suggests that China must be careful to avoid being trapped into an arms race (cyber, AI and quantum) and suffer the same experience of the former Soviet Union during the Cold War. [cxlvii]

Gen. Mark Milley, chairman of the Joint Chiefs of Staff of the U.S, said the Hypersonic missile test was “very close” to being a Sputnik moment, akin to the 1957 launching by the Soviet Union of the world’s first space satellite, which caught the world by surprise and fed fears the United States had fallen behind technologically. What followed was a nuclear arms and space race that ultimately bankrupted the Soviet Union.[cxlviii]

An Archaic Military, institutional shortcomings and lack of combat experience

Due to the rapid pace of modernisation and aggressive posture of the PRC, observers inside and outside the PLA cite China’s lack of recent combat experience as a significant weakness, as China last fought a war in 1979. PLA officials frequently refer to a “peace disease” endemic in the force, and worry that troops who have never seen battle will become complacent and struggle to maintain readiness. Due to as insufficiently realistic training and exercise regimen, and PLA leaders have long called for more complex and sophisticated training and exercises to better prepare an untested force for potential conflicts.

The PLAA in particular is struggling to train personnel to operate an influx of new, advanced equipment that is replacing legacy systems, to develop commanders’ ability to manage new combined arms units; and to develop smaller, more agile, and more modular formations in order to meet the requirements of “new-type operations.”

Xi’s reform and reorganization is designed to improve the PLA’s ability to “fight and win,” the initiative is still ongoing. As the PLA reorganizes itself, the force is undergoing a period of significant disruption, leading some observers to question whether the PLA might be acutely unprepared for conflict while the reorganization process is ongoing.

The reform and reorganization’s effort to achieve jointness is also ongoing, and jointness remains a major challenge. Even as the services conduct more exercises than ever before, relatively few are
Joint.[cxlix]

Less than 30 percent of China's surface forces, air force, and air defence forces and 55 percent of its submarine fleet were modern in 2011. Subsequently, nothing much has changed, as a substantial percentage of China's military remains obsolete. China's military faces institutional shortcomings arising from obsolete command structures, low quality of personnel, and corruption. The military has weaknesses centring on supporting capabilities such as logistics, inadequate airlift, and deficient air defence and antisubmarine warfare. The PLA's loyalty to the CCP has hampered its competence. China's military training and operational capabilities and competences do not match US standards. PLAAF pilots fall short on the requirement of executing sophisticated aerial manoeuvres during unplanned operations.

PRC cannot project power globally through a rigid command-and-control system as the PLA's structure presents significant cultural challenges, as it emphasizes control above command. To this effect a political commissar is positioned on PLAN warships and submarines. A culture of risk aversion and low levels of trust in subordinates impacts the PLA effectiveness. A highly centralized structure does not allow the PLAN to operate autonomously during a war.

PLAN submarines have the worst safety record in the world. The PLAN's rudimentary nuclear missile submarine fleet carries a limited number of missiles. The PLAN submarine power is outdated, compared to the overwhelming USN undersea warfare capabilities.

Soviet weapon systems were much sought after by the United States to learn their strengths and weaknesses. However, US intelligence is not similarly orchestrating any defections of PLAAF fighter aircraft, as the United States is not interested in obsolete Chinese technology. Instead, China is stealing weapon data or reverse engineering US weapon systems. The CCP-controlled military press described the Shenyang J-15 Flying Shark fighter aircraft as a "flopping fish" and criticized it for lacking the stealth capabilities of the F-35 Lightning.

However, the PLAAF has not operationally inducted the J-31 fighter aircraft while the J-20 fighter aircraft (comparable to the MiG 31) has not yet proven its capabilities in any bilateral or multilateral military exercise. [cl]

Dissatisfaction with Chinese manufactured Military Hardware Jordan, had purchased six CH-4B unmanned combat aerial vehicles (UCAV) produced by the China Aerospace Science and Technology Corporation (CASC) in 2016. However, within just three years, the kingdom had put them up for disposal, with their sale advertised in June 2019 as it was not happy with the aircraft's performance and was looking to retire them. Other known

users of the CH-4 UCAV are Algeria, Egypt, Saudi Arabia, the UAE and Iraq. [cli]

Bangladesh, had purchased 23 Nanchang PT-6 basic trainer aircraft in two batches from China National Aero-technology Import and Export Corporation or CATIC for its air force is facing problems. The Bangladesh Air Force had bought 12 in 2016 and 11 in 2018 and they are riddled with defects and the lack of after-sales service and also, poor maintenance by the Original Equipment Manufacturer, Hongdu Aviation. [clii]

The Economic Times reported on Oct 15, 2021 that China-Pakistan military relations are under strain due to substandard servicing, maintenance. In a display of cooperation, three armed drones, designed by Chengdu Aircraft Industry Group of China and sold by China National Aero-Technology Import & Export Corporation (CATIC), were inducted into the Pakistan Air force (PAF) in January 2021. But, the purchase of unmanned combat aerial vehicles (UCAVs) and its addition to Pakistan's growing range of military equipment has entered a deadlock. The Chinese-made Wing Loong II Unmanned Aerial Systems (UCAVs) had been grounded due to crippling defects within days of induction.[cliii]

Citizen Welfare & Economic Impact

During the current war in Ukraine, PRC has not been able to support and evacuate a large number of it’s citizens like India has done. Such repeated disregard for safety and security of its citizen’s welfare may lead to long term discontentment among its population.

Corruption is rampant and another target of the reform and reorganization. It also presents a persistent vulnerability in PLA.

Water has become scarce, and PRC is importing more energy and food than any other nation, having ravaged its own natural resources. Economic growth is therefore becoming costlier: According to data from DBS Bank, it takes three times as many inputs to produce a unit of growth today as it did in the early 2000s. To make matters worse, China is turning away from the package of policies that promoted rapid growth. Under Xi, Beijing has slid back toward totalitarianism. Xi has appointed himself “chairman of everything,” destroyed any semblance of collective rule, and made adherence to “Xi Jinping thought” the ideological core of an increasingly rigid regime. And he has relentlessly pursued the centralization of power at the expense of economic prosperity. The country’s official growth rate declined from 14 percent in 2007 to 6 percent in 2019, and rigorous studies suggest the true growth rate is now closer to 2 percent.[cliv]

On 15 April 2022, China's Ministry of Industry and Information Technology said it would help more than 600 companies in Shanghai to restart operations. They included firms in the computer chip, car making and medical industries. This is due to the fact that Retail sales fell by 3.5% in March 2022 compared to a year earlier as reported by China's National Bureau of Statistics. It also added that was the first decline since July 2020. For the same period unemployment rose to 5.8%, the highest level since May 2020. Richard Yu, an executive at Chinese technology giant Huawei, last week warned that technology, industrial and automobile supply chains "will come to a complete halt" if the city did not resume production by May 2022. In recent weeks people have taken to social media to complain about the restrictions and the lack of food supplies, while video footage has shown confrontations between police and residents. [clv]

An ill prepared Shanghai municipal government and its inconsistent policy have triggered a food crisis and widespread public outcry. The day before the lockdown was announced, local health authorities were still telling the press that the city was too important to the national economy and thus a city-wide lockdown would not be considered as costs would be too high. The production of virtually all goods and services in Shanghai, except in certain industries considered strategically important like semiconductors and financial services, has come to a sudden stop that will undoubtedly result in significant losses of people's livelihoods and to the entire Chinese economy. Results from a recent flash survey conducted by the German Chamber of Commerce in early April 2022 show the lockdowns have already significantly disrupted the entire supply chain within China, with over half of German companies' logistics and warehousing completely disrupted or severely impacted by the government's preventive measures, and 40 percent reporting complete disruption or severe impact on upstream supply chain operations due to a lack of raw materials or upstream products. [clvi]

Power Shortages

China has been hit by power shortages as reported by the BBC. This is largely due to the inability to balance electricity supplies with demand. This year a number of factors have come together to make the issue especially serious. As the world starts to reopen after the pandemic, demand for Chinese goods is surging and the factories making them need a lot more power. Due to the rules imposed by Beijing in its attempt to make the country carbon neutral by 2060, the coal production has slowed, even as the country still relies on coal for more than half of its power. With the government strictly controlling electricity prices, coal-fired power plants are unwilling to operate at a loss, with many drastically reducing their output instead. Homes and businesses have been affected by power cuts as electricity has been rationed in several provinces and regions. The state-run

Global Times newspaper said there had been outages in four provinces - Guangdong in the south and Heilongjiang, Jilin and Liaoning in the north east. There are also reports of power cuts in other parts of the country. The impact on PRC's economy as the official figures have shown that in September 2021, Chinese factory activity shrunk to the lowest it had been since February 2020, when coronavirus lockdowns crippled the economy. Concerns over the power cuts have contributed to global investment banks cutting their forecasts for the country's economic growth. Goldman Sachs has estimated that as much as 44% of the country's industrial activity has been affected by power shortages. It now expects the world's second largest economy to expand by 7.8% this year, down from its previous prediction of 8.2%. The China Electricity Council, which represents generating firms, has also said that coal-fired power companies were now "expanding their procurement channels at any cost" in order to guarantee winter heat and electricity supplies. However, finding new sources of coal imports may not be straightforward as Russia is already focused on its customers in Europe, Indonesian output has been hit by heavy rains and nearby Mongolia is facing a shortage of road haulage capacity. [clvii] Since electric power is used for any component to do with informenised and / or intelligensied war fighting, it may have a direct or indirect bearing on them.

Espionage

PRC is deeply apprehensive of cyber espionage as it itself is involved in large scale activities of cyberspace espionage and hacking itself. Therefore in 2019, Beijing ordered all government offices and public institutions to replace all their foreign equipment and software including Windows (even though there is a Beijing-approved Chinese version of Windows 10). Earlier in 2017, the CPC had ordered the PLA SSF to develop a purely Chinese operating system specifically in order to replace Windows and other Microsoft software because of the hacking and back-door threats that CPC was convinced had been integrated into the software by the US NSA. PLA's substitute software was ready for use in mid-2019, Beijing ordered the quick replacement of some 20-to-30 million hardware units within three years at a pace of 30% in 2020, 50% in 2021, and the remaining 20% in 2022.[clviii] Such acts are putting a lot of burden on the economy and stress on people using the systems owing to frequent changes and new skill set requirements.

A variety of multilateral anti-China initiatives

The Quadrilateral Security Dialogue; supply chain alliances; the new so-called AUKUS alliance with Washington, London, and Canberra; and others—are in the works. The United States' "multilateral club strategy," hawkish and well-connected scholar Yan Xuetong acknowledged in July, is "isolating China" and hurting its development. The world is becoming less

conducive to easy Chinese growth, and Xi's regime increasingly faces the sort of strategic encirclement that once drove German and Japanese leaders to desperation. An array of actors is gradually joining forces to check Beijing's power and put it in a strategic box. China, in other words, is not a forever-ascendant country. It is an already-strong, enormously ambitious, and deeply troubled power whose window of opportunity won't stay open for long.[clix]

China confronts an increasingly hostile external environment. The combination of COVID-19, persistent human rights abuses, and aggressive policies have caused negative views of China to reach levels not seen since the Tiananmen Square massacre in 1989. Countries worried about Chinese competition have slapped thousands of new trade barriers on its goods since 2008. More than a dozen countries have dropped out of Xi's Belt and Road Initiative while the United States wages a global campaign against key Chinese tech companies—notably, Huawei—and rich democracies across multiple continents throw up barriers to Beijing's digital influence. [clx]

End Note

The above description and arguments clearly highlight the possibility of some progress made by PRC and PLA utilizing New Generation technology for military use. A clear trend has also been established of PRC leveraging dual use technology for military use. Furthermore the use of espionage / coercion / investments as a means to gather technology is increasingly becoming the new norm with PRC.

In line with the traditional Chinese military wisdom, PRC / PLA is leveraging 4IR and interlinked technologies and moving towards "the supreme art of war is to subdue the enemy without fighting" and "it is better to win the heart of the people than to capture the city".
It may hold true that, in many instances PRC's propaganda machinery (read: physiological warfare and military deception) is hard at work to project to the world what it wants the world to believe.

By 2050, China most likely will have experienced some mixture of successes and failures, and the most plausible scenarios would be an ascendant China or a stagnant China. In the former scenario, China will be largely successful in achieving its long term goals, while, in the latter scenario, China will confront major challenges and will be mostly unsuccessful in implementing its grand strategy [clxi]

Appendix

Topic	2009[clxii]	2016[clxiii]	2020[clxiv]	2021[clxv]
Science and Technology Thrust / Innovation	China is focusing on the following technologies for rapid development: **IT:** intelligent perception, ad hoc networks, and virtual reality technologies. **New Materials:** Smart materials and structures, high-temperature superconducting technologies and highly efficient energy materials technologies **Advanced Manufacturing:** extreme manufacturing technologies and intelligent service robots. **Advanced Energy Technologies:** hydrogen energy and fuel cell technologies, alternative fuels, and advanced vehicle technologies **Laser and Aerospace Technologies** are also high priorities. China has also identified 16 "**major special items**" for which it plans to develop or expand indigenous	PRC's National Medium- and Long-Term Program for Science and Technology Development (2006-2020), issued by the State Council in February 2006, seeks to transform China into an "innovation-oriented society" by 2020. The plan defines China's S&T focus in terms of basic research, leading-edge technologies, key fields and priority subjects, and "**major special items**," all of which have military applications. The PLA is developing and testing new intermediate- and medium-range conventional ballistic missiles as well as long range, land-attack, and anti-ship cruise missiles, which once operational would extend the military's reach and push adversary forces further from potential regional conflicts. China is also focusing on counter space, offensive cyber operations and EW capabilities meant to deny adversaries the advantages of modern, information technology-driven warfare.	PRC aims to build national corporate champions that achieve rapid market dominance across a range of technologies directly complements the PLA's modernization efforts. They seek to be a **leader in key technologies** with military potential, such as AI, autonomous systems, advanced computing, quantum information sciences, biotechnology, and advanced materials and manufacturing. **China continues to undermine the integrity of the U.S. science and technology research enterprise** through a variety of actions such as hidden diversions of research, resources, and intellectual property. **China has also reorganised its military research institutions and key military think tanks** to provide the PLA advanced capabilities and a modern war fighting doctrine. As part of the **13th Five-Year Plan (2016–2020)**, focus areas include aerospace engines—including	A top-level push to master advanced technologies and **become a global innovation superpower**, this push directly supports the PLA's ambitious modernization efforts and its goal of becoming a **"world-class" military capable of "intelligentized" warfare** such as AI, autonomous systems, advanced computing, quantum information sciences, biotechnology, and advanced materials and manufacturing. The **14th Five-Year Plan maintains the PRC's focus on technological independence and indigenous innovation** in fields associated with the Fourth Industrial Revolution. As of 2020, the PLA has **funded multiple AI projects** that focus on applications including machine learning for strategic and tactical recommendations, AI-enabled wargaming for training, and social media analysis.

	capabilities. These include core electronic components, high-end universal chips and operating system software, very large-scale integrated circuit manufacturing, next-generation broadband wireless mobile communications, high-grade numerically controlled machine tools, large aircraft, high□resolution satellites, manned spaceflight and lunar exploration.		turbo fan technology—and gas turbines; quantum communications and computing; innovative electronics and software; automation and robotics; special materials and applications; nanotechnology; neuroscience, neural research, and artificial intelligence (AI); and deep□space exploration and on-orbit servicing and maintenance systems. China also is applying substantial R&D resources to nuclear fusion, hypersonic weapons technology, and the deployment and hardening of its expanding multipurpose satellite constellation.	
Foreign Technology Acquisition	China has identified certain industries and technology groups with potential to provide technological breakthroughs, remove technical obstacles across industries and **improve international competitiveness.** Specifically, China's defence industries are pursuing advanced manufacturing, information technology, and defence technologies. Examples include **radar, counter-space capabilities, secure C4ISR,**	PRC draws from diverse sources to support PLA modernization, including domestic defence investments, indigenous defence industrial development, a growing research and development (R&D) / science and technology (S&T) base, **dual-use technologies and foreign technology acquisition**.	The PRC pursues many vectors to acquire sensitive and dual use technologies and military-grade equipment to advance its military modernization goals, **including both licit & illicit means, foreign investments, commercial joint ventures, mergers and acquisitions, and state-sponsored industrial and technical espionage, and the manipulation of export controls for the illicit diversion of dual-use technologies.** In 2019, the PRC's efforts included **efforts to acquire**	The PRC uses imports, foreign investments, commercial joint ventures, mergers and acquisitions, and industrial and technical espionage to help achieve its military modernization goals **by acquiring technologies that will be foundational for future commercial and military innovations including AI, robotics, autonomous vehicles, quantum information sciences, augmented and virtual reality, financial technology, and biotechnology.**

	smart materials, and low-observable technologies.		**dynamic random access memory, aviation, and anti-submarine warfare technologies.**	
Sourcing Science & Technology for Military Modernisation	China's defence industry has benefited from integration with China's rapidly expanding civilian economy and science and technology sector, particularly elements that have access to foreign technology. **IT** companies, including Huawei, Datang, and Zhongxing, **maintain close ties to the PLA and collaborate on R&D.** Commercial off-the-shelf technologies, such as computer network switches and routers, increasingly provide the PLA with state-of-the-art telecommunications equipment.	China continues to supplement indigenous military modernization efforts through the acquisition of **targeted foreign technologies, including engines for aircraft, tanks, and naval vessels; solid state electronics and microprocessors, guidance and control systems; enabling technologies such as cutting-edge precision machine tools; advanced diagnostic and forensic equipment; and computer-assisted design, manufacturing, and engineering**. China often pursues these foreign technologies for the purpose of **reverse engineering or to supplement indigenous military modernization efforts**. China seeks some high-tech components and major end items from abroad that it has difficulty producing domestically—particularly from Russia and Ukraine.	The PRC continues to undermine the integrity of the U.S. S&T research enterprise through a variety of actions such as hidden diversions of research, resources, and intellectual property. The PRC continues to undermine the integrity of the U.S. S&T research enterprise through a variety of actions such as hidden diversions of research, resources, and intellectual property.	PRC-based intrusions continued to target computer systems around the world, including those owned by the U.S. Government, through 2020. These and past intrusions focus on accessing networks and extracting information. The PRC uses its cyber capabilities to not only **support intelligence collection against U.S. political, economic, academic, and military targets, but also to exfiltrate sensitive information from the defence industrial base to gain military advantage and possibly for cyberattack preparations.** The targeted information can benefit the PRC's defence high-technology industries, support the PRC's military modernization, provide China's leadership with insights into U.S. plans and intentions, and enable diplomatic negotiations.

CERTIFICATE

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

Disclaimer: Views expressed are of the author and do not necessarily reflect the views of CENJOWS.

References

[i] https://economictimes.indiatimes.com/news/defence/chinese-communist-party-unveils-plan-to-make-pla-on-par-with-us-military-by-2027/articleshow/78983356.cms, Nov 01, 2020, 06:40 PM IST

[ii] http://www.xinhuanet.com/english/2020-12/10/c_139580140.htm, Source: Xinhua, 2020-12-10 23:01:50, Editor: huaxia

[iii] "What is the Fourth Industrial Revolution? Xi Jinping described the blueprint like this! 第四次工业革命什么样？习近平这样描绘蓝图！]." Qiushi [求是网], July 27, 2018. http://www.qstheory.cn/zhuanqu/2018-07/27/c_1123186013.htm.

[iv] https://jamestown.org/program/chinas-2027-goal-marks-the-plas-centennial-not-an-expedited-military-modernization/ China's 2027 Goal Marks the PLA's Centennial, Not an Expedited Military Modernization, Publication: China Brief Volume: 21 Issue: 6, By: Brian Hart, Bonnie S. Glaser, Matthew P. Funaiole, March 26, 2021 03:45 PM

[v] Jane's by IHS Markit, China's Advanced Weapons Systems; May 12, 2018

[vi] The Strategic Support Force and the Future of Chinese Information Operations; The Cyber Defense Review by Elsa B. Kania John K. Costello; Spring 2018

[vii] NIDS China Security Report 2022, The PLA's Pursuit of Enhanced Joint Operations Capabilities

[viii] Military and Security Developments Involving the People's Republic of China 2016, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[ix] NIDS China Security Report 2022, The PLA's Pursuit of Enhanced Joint Operations Capabilities

[x] Military Power of the People's Republic of China 2021, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[xi] Pentagon rattled by Chinese military push on multiple fronts, https://apnews.com/article/technology-china-asia-united-states-beijing-aea288656fab23253ee0397dc21ba68a By Robert Burns November 1, 2021

[xii] The Real Culprit – The PLA's Strategic Support Force , The Institute for strategic, political, security and economic consultancy (ISPSW) Berlin, February 2020

[xiii] The Real Culprit – The PLA's Strategic Support Force , The Institute for strategic, political, security and economic consultancy (ISPSW) Berlin, February 2020

[xiv] Military Power of the People's Republic of China 2021, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[xv] Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation Prepared for The US-China Economic and Security Review Commission, 9 October 2009

[xvi] Military and Security Developments Involving the People's Republic of China 2019, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[xvii] The Third Road Threat: Towards a Comprehensive Theory of Information Warfare, Over the Horizon, Air Command and Staff College, United States, 26 Aug 2021

[xviii] Magic Weapons: China's Political Influence Activities Under Xi Jinping by Anne-Marie Brady (Paper presented at the Taiwan Foundation for Democracy Conference, Arlington, VA, September 16-17, 2017)

[xix] The Third Road Threat: Towards a Comprehensive Theory of Information Warfare, Over the Horizon, Air Command and Staff College, United States, 26 Aug 2021

[xx] The Third Road Threat: Towards a Comprehensive Theory of Information Warfare, Over the Horizon, Air Command and Staff College, United States, 26 Aug 2021

[xxi] The Real Culprit – The PLA's Strategic Support Force , The Institute for strategic, political, security and economic consultancy (ISPSW) Berlin, February 2020

[xxii] Interagency Performance in Counterterrorism Operations: Implications for the "Gray Zone", by J. Paul Pope, July 2018

[xxiii] Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation Prepared for The US-China Economic and Security Review Commission, 9 October 2009

[xxiv] Military and Security Developments Involving the People's Republic of China 2012, , Office of the Secretary of Defense, United States of America

[xxv] Jane's by IHS Markit, China's Advanced Weapons Systems; May 12, 2018

[xxvi] Commission on the Theft of American Intellectual Property, Update on The Theft of American Intellectual Property Report, National Bureau of Asian Research, February 2017, p. 2, http://www.ipcommission.org/ report/IP_Commission_Report_Update_2017.pdf. Quoted in Office of the U.S. Trade Representative, Findings of the Investigation Into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974, PDF page 203, https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF#page=203.

[xxvii] US Office of the Secretary of State, Policy Planning Staff, The Elements of the China Challenge, 6-7. December 2020

[xxviii] The Third Road Threat: Towards a Comprehensive Theory of Information Warfare, Over the Horizon, Air Command and Staff College, United States, 26 Aug 2021

[xxix] Jane's by IHS Markit, China's Advanced Weapons Systems; May 12, 2018

[xxx] The Real Culprit – The PLA's Strategic Support Force , The Institute for strategic, political, security and economic consultancy (ISPSW) Berlin, February 2020

[xxxi] Military and Security Developments Involving the People's Republic of China 2019, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[xxxii] People's Liberation Army Operational Concepts, by Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, Mark Cozad, https://www.rand.org/pubs/research_reports/RRA394-1.html

[xxxiii] The Third Road Threat: Towards a Comprehensive Theory of Information Warfare, Over the Horizon, Air Command and Staff College, United States, 26 Aug 2021

[xxxiv] Military Power of the People's Republic of China 2021, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[xxxv] The US and China are in a quantum arms race that will transform warfare, MIT Technology Review, 3 Jan 2019

[xxxvi] The US and China are in a quantum arms race that will transform warfare, MIT Technology Review, 3 Jan 2019

[xxxvii] These 20 Leading Technologists are Driving China's AI Revolution, Forbes, June 21, 2017 by Adelyn Zhou, https://www.forbes.com/sites/adelynzhou/2017/06/21/chinese-leaders-in-artificial-intelligence/2/#39ec77287568.

[xxxviii] Jane's by IHS Markit, China's Advanced Weapons Systems; May 12, 2018

[xxxixxxxix] http://www.mod.gov.cn/big5/jmsd/2019-01/15/content_4834525.htm, 2019-01-15 09:06

[xl] How Does China Aim to Use AI in Warfare?, thediplomat.com 28 December 2021

[xli] http://www.81.cn/theory/2018-04/11/content_8000765.htm, 2018-04-11 10:34

[xlii] http://www.81it.com/2018/0222/8552.html, 2018-02-22 10:10:08

[xliii] https://www.cae.cn/cae/html/main/colys/00855664.html, Elected as Academician of Chinese Academy of Engineering in 2011

[xliv] To Rule the Invisible Battlefield: The Electromagnetic Spectrum and Chinese Military Power, Texas National Security Review, 05 Jan 2022

[xlv] How Does China Aim to Use AI in Warfare?, thediplomat.com 28 December 2021

[xlvi] Military Power of the People's Republic of China 2021, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[xlvii] China's Ambitions for AI-Driven Future Warfare, Jewish Policy Center, Washington, Winter 2022,

[xlviii] http://www.1000plan.org/en/, The Recruitment Program for Innovative Talents (Long Term) [Accessed 18 March 2019]

[xlix] A Personality-Based Combat Behavior Modeling Architecture and Methods (Artificial Intelligence and Robotics Research), Vol. 08 No. 04 (2019), Article ID: 33207 by Jiang Zhu, Chuanhua Wen, Jun Chen, Xiangyuan Huang; Combat Experiment Laboratory, Army Command College, Nanjing Jiangsu and Postgraduate Team, Army Command College, Nanjing Jiangsu, Received: Nov. 8th, 2019; accepted: Nov. 22nd, 2019; published: Nov. 29th, 2019, 7 pages

[l] Observer Research Foundation, https://www.orfonline.org/research/a-i-in-the-chinese-military-current-initiatives-and-the-implications-for-india-61253/#_edn15 . The original paper can be viewed on https://image.hanspub.org/Html/9-2610169_33207.htm

[li] AI WEAPONS" IN CHINA'S MILITARY INNOVATION by The Brookings Institution, New York in partnership with Center for Security and Emerging Technology, based at Georgetown University's School of Foreign Service April 2020.

[lii] Wang Zhixue, "**构建**军事行动法律保障力量" [Building legal support forces for military operations"], PLA Daily, December 8, 2015, http://www.81.cn/jfjbmap/content/2015-12/08/content_131480.htm.

[liii] Wang Zhixue, "**构建**军事行动法律保障力量" [Building legal support forces for military operations"], PLA Daily, December 8, 2015, http://www.81.cn/jfjbmap/content/2015-12/08/content_131480.htm.

[liv] Wang Zhaobing and Chang Sheng, "**塑造人工智能**军事应用的政治属性" [Shaping the Political Attributes of Military Applications of Artificial Intelligence], Study Times, November 14, 2018, http://www.qstheory.cn/defense/2018-11/14/c_1123713007.htm.

[lv] https://www.popsci.com/robot-tanks-china/ , 9 June 2018

[lvi] Zheng Yufu, "**武器装**备机械化、信息化、智能化怎么融" [How to integrate mechanization, informatization, and intelligentization of weapons and equipment], PLA Daily, October 10, 2019

[lvii] "访"**翼**龙"总设计师：平时工兵战时尖兵" [Interview with Chief Designer of Pterosaur: Peacetime Engineers Wartime Soldiers], Xinhua, April 14, 2017, http://news.xinhuanet.com/politics/2017-04/14/c_1120807914_2. htm; "**翼**龙Ⅱ无人机首露真容" [Pterodactyl II drone first revealed], Science Times, September 30, 2017, http://

news.sciencenet.cn/htmlnews/2017/9/390010.shtm; “翼龙”无人机是如何制造的？听听总设计师怎么说” [How is the ‘Pterosaur’ drone made? Listen to how the Chief Designer speaks], Southern Network, November 11, 2019, http://kb.southcn.com/content/2019-11/11/content_189485801.htm. For initial developments in Chinese military research institutes and the Chinese defense industry on this front, see: “人的使命在于 追求完美” [The Human Mission is to Pursue Perfection”], Xidian University, https://mobile.xidian.edu.cn/ info/1439/31879.htm.

[lviii] Zhao Xiaozhe, “指挥控制系统中的自然智能和人工智能” [Natural intelligence and artificial intelligence in command and control systems], Sohu, April 23, 2017, http://wemedia.ifeng.com/13425965/wemedia.shtml; “认知域下智能化战争制胜机理” [The Winning Mechanisms of Intelligentized Warfare in the Cognitive Domain, PLA Daily, December 24, 2019, https://m.chinanews.com/wap/detail/zw/mil/2019/12-24/9041718.shtml.

[lix] “China’s Algorithms of Repression,” (New York: Human Rights Watch, May 1, 2019), https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance.

[lx] A notable nexus can exist between security/defense (安防) applications and the leveraging of these technologies for military purposes, including techniques for monitoring and manipulating public opinion with applications in influence operations.

[lxi] Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation Prepared for The US-China Economic and Security Review Commission, 9 October 2009

[lxii] To Rule the Invisible Battlefield: The Electromagnetic Spectrum and Chinese Military Power, Texas National Security Review, 05 Jan 2022

[lxiii] Competition and Conflict: Implications for Maneuver Brigades, Modern War Institute at West Point, June 2021

[lxiv] Competition and Conflict: Implications for Maneuver Brigades, Modern War Institute at West Point, June 2021

[lxv] Competition and Conflict: Implications for Maneuver Brigades, Modern War Institute at West Point, June 2021

[lxvi] Chinese Tactics, Headquarters, Department Of The Army, Washington 09 August 2021

[lxvii] Electromagnetic Spectrum Operations, Testimony Before the Subcommittee on Cyber, Innovative Technologies, and Information Systems, Committee on Armed Services, House of Representatives, United States Government Accountability Office, 19 March 2021

[lxviii] To Rule the Invisible Battlefield: The Electromagnetic Spectrum and Chinese Military Power, Texas National Security Review, 05 Jan 2022

[lxix] Military Power of the People’s Republic of China 2021, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[lxx] Military Power of the People’s Republic of China 2021, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[lxxi] http://www.xinhuanet.com/mil/2018-02/13/c_129811999.htm, 2018−02-13, 13:14:35

[lxxii] https://nypost.com/2021/12/21/satellite-photos-reveal-worrying-antennas-in-south-china-sea/ , 21 Dec 2021

[lxxiii] https://www.globaltimes.cn/page/202109/1235286.shtml, 28 Sep 2021

[lxxiv] https://www.spsmai.com/experts-speak/?id=1083&q=Chinas-Anti-Stealth-Radar, 2 Nov 2021

[lxxv] https://www.bloombergquint.com/politics/pentagon-sees-china-s-offensive-space-technology-on-the-march, 10 July 2021

[lxxvi] PLA Aerospace Power: China Aerospace Studies Institute, July 2019

[lxxvii] http://www.gov.cn/archive/whitepaper/202201/28/content_WS61f35b3dc6d09c94e48a467a.html

[lxxviii] https://engineersforum.com.ng/2018/12/31/beidou-satellite-becomes-fully-operational/ , 31 Dec 2018

[lxxix] Thursday, June 16, 2016, 14:20, BeiDou system to go global around 2020, https://www.chinadailyasia.com/nation/2016-06/16/content_15449675.html

[lxxx] https://www.everythingrf.com/community/what-is-beidou

[lxxxi] Chinese Tactics, Headquarters, Department Of The Army, Washington 09 August 2021

[lxxxii] https://www.scmp.com/news/china/science/article/3142902/chinese-researchers-look-how-keep-satellites-under-radar, 29 July 2021

[lxxxiii] The US and China are in a quantum arms race that will transform warfare, MIT Technology Review, 3 Jan 2019

[lxxxiv] PLA Aerospace Power: China Aerospace Studies Institute, July 2019

[lxxxv] https://www.aerospace-technology.com/projects/micius-quantum-communication-satellite/

[lxxxvi] https://news.cgtn.com/news/7a49544d33557a6333566d54/share_p.html

[lxxxvii] Bill Munro, senior distingished scientist and group leader, Nippon Telegraph and Telephone Corporation, Basic Research Laboratories, https://www.brl.ntt.co.jp/people/bilmun/

[lxxxviii] Howard Wiseman, director of the Center for Quantum Dynamics at Griffith University in Brisbane, Australia

[lxxxix] https://asiatimes.com/2021/09/shanghai-scientists-set-space-teleportation-record/

[xc] The US and China are in a quantum arms race that will transform warfare, MIT Technology Review, 3 Jan 2019

[xci] China Has Unveiled the World's First 'Unhackable Computer Network', World Economic Forum, Tom Ward, August 14, 2017. https://www.weforum.org/agenda/2017/08/why-china-is-leading-the-world-in-developing-quantum-communication-networks

[xcii] https://www.researchgate.net/figure/actual-deployments-and-plans-for-further-extension-of-the-terrestrial-QKD-network-in-China_fig3_337706726

[xciii] Jane's by IHS Markit, China's Advanced Weapons Systems; May 12, 2018

[xciv] China's Ambitions for AI-Driven Future Warfare, Jewish Policy Center, Washington, Winter 2022,

[xcv] https://www.researchgate.net/figure/the-QKD-system-developed-by-SK-Telecom-29_fig5_337706726

[xcvi] https://news.cgtn.com/news/7767444d34637a6333566d54/index.html

[xcvii] https://news.cgtn.com/news/3d67444e326b444e/share_p.html

[xcviii] https://news.cgtn.com/news/3145444f78597a6333566d54/share_p.html . The image on https://twitter.com/MielczarekJakub/status/1029100347070001153/photo/1 depicts how quantum encryption is encrypted.

[xcix] https://www.scientificamerican.com/article/china-reaches-new-milestone-in-space-based-quantum-communications/

[c] Jane's by IHS Markit, China's Advanced Weapons Systems; May 12, 2018

[ci] China uses microwave weapons to blast Indian troops in disputed border region, The radiation technology left soldiers vomiting and incapacitated without breaking no-live-shots rule, The Week U.K, 17 Nov 2020

[cii] The website for professor Jin is http://srs.ruc.edu.cn/English/Teaching/Faculty/b1e519fda44e43caaf6531ae903403e2.htm

[ciii] The denial can be read on https://twitter.com/PIBFactCheck/status/1328727700702302208?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1328727700702302208%7Ctwgr%5E%7Ctwcon%5Es1_ and https://twitter.com/adgpi/status/1328732069598437376?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1328732069598437376%7Ctwgr%5E%7Ctwcon%5Es1_

[civ] https://impakter.com/curing-evil-with-evil-china-successfully-controlled-its-weather-last-year/

[cv] China is now controlling the weather. What's the environmental cost?, euronews.com, 19 Dec 2021

[cvi] https://www.news18.vscom/news/explainers/explained-rocket-science-to-control-weather-how-cloud-seeding-helps-china-bring-rain-clear-pollutants-4546097.html

[cvii] Military Power of the People's Republic of China 2021, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[cviii] The Institute for Strategic, Political, Security and Economic Consultancy, The Institute for Strategic, Political, Security and Economic Consultancy Berlin, 2011

[cix] Jane's by IHS Markit, China's Advanced Weapons Systems; May 12, 2018

[cx] China's hypersonic weapons aren't just hype. India should be worried, By Justin Paul George Updated: December 04, 2021 07:50 IST, https://www.theweek.in/news/india/2021/12/03/chinas-hypersonic-weapons-arent-just-hype-india-should-be-worried.html

[cxi] China's quest for hypersonic arms, By Holmes Liao 廖宏祥, Sun, Oct 17, 2021 page 8, Taipei Times, https://www.taipeitimes.com/News/editorials/archives/2021/10/17/2003766241

[cxii] China's Hypersonic Weapons, by Paul Bernstein and Dain Hancock, January 27, 2021, Walsh School of Foreign Service, Georgetown University, Georgetown Journal of International Affairs, https://gjia.georgetown.edu/2021/01/27/chinas-hypersonic-weapons/

[cxiii] Explained: What is hypersonic glide missile that China tested, India Today Web Desk, October 18, 2021 https://www.indiatoday.in/science/story/explained-what-is-hypersonic-glide-missile-that-china-likely-tested-1866049-2021-10-18

[cxiv] China military researchers pinpoint AI for hypersonic weapons accuracy, Stephen Chen, 13 October 2021, https://sg.news.yahoo.com/china-military-researchers-pinpoint-ai-072341855.html

[cxv] China's Hypersonic Weapons, by Paul Bernstein and Dain Hancock, January 27, 2021, Walsh School of Foreign Service, Georgetown University, Georgetown Journal of International Affairs, https://gjia.georgetown.edu/2021/01/27/chinas-hypersonic-weapons/

[cxvi] A case study of the PRC's Hypersonic Systems Development, China Aerospace Studies Institute & TextOre, Inc. by Peter Wood and Roger Cliff, 25 Aug. 2020

[cxvii] China's hypersonic weapons aren't just hype. India should be worried, By Justin Paul George Updated: December 04, 2021 07:50 IST, https://www.theweek.in/news/india/2021/12/03/chinas-hypersonic-weapons-arent-just-hype-india-should-be-worried.html

[cxviii] A case study of the PRC's Hypersonic Systems Development, China Aerospace Studies Institute & TextOre, Inc. by Peter Wood and Roger Cliff, 25 Aug. 2020

[cxix] Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation Prepared for The US-China Economic and Security Review Commission, 9 October 2009

[cxx] Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation Prepared for The US-China Economic and Security Review Commission, 9 October 2009

[cxxi] Military Power of the People's Republic of China 2009, Annual Report To Congress, Office of the Secretary of Defense, United States of America

[cxxii] Military Power of the People's Republic of China 2009, Annual Report To Congress, Office of the Secretary of Defense, United States of America

[cxxiii] Military Power of the People's Republic of China 2009, Annual Report To Congress, Office of the Secretary of Defense, United States of America

[cxxiv] Military Power of the People's Republic of China 2009, Annual Report To Congress, Office of the Secretary of Defense, United States of America

[cxxv] Military and Security Developments Involving the People's Republic of China 2016, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[cxxvi] Military and Security Developments Involving the People's Republic of China 2012, Office of the Secretary of Defense, United States of America

[cxxvii] Military and Security Developments Involving the People's Republic of China 2016, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[cxxviii] Military and Security Developments Involving the People's Republic of China 2016, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[cxxix] Military and Security Developments Involving the People's Republic of China 2016, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[cxxx] A case study of the PRC's Hypersonic Systems Development, China Aerospace Studies Institute & TextOre, Inc. by Peter Wood and Roger Cliff, 25 Aug. 2020

[cxxxi] Jane's by IHS Markit, China's Advanced Weapons Systems; May 12, 2018

[cxxxii] PLA Aerospace Power: China Aerospace Studies Institute, July 2019

[cxxxiii] Jane's by IHS Markit, China's Advanced Weapons Systems; May 12, 2018

[cxxxiv] Jane's by IHS Markit, China's Advanced Weapons Systems; May 12, 2018

[cxxxv] To Rule the Invisible Battlefield: The Electromagnetic Spectrum and Chinese Military Power, Texas National Security Review, 05 Jan 2022

[cxxxvi] The Real Culprit – The PLA's Strategic Support Force , The Institute for strategic, political, security and economic consultancy (ISPSW) Berlin, February 2020

[cxxxvii] China's Ambitions for AI-Driven Future Warfare, Jewish Policy Center, Washington, Winter 2022,

[cxxxviii] Military Power of the People's Republic of China 2021, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[cxxxix] Military Power of the People's Republic of China 2021, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[cxl] Academic Webinar: Cyberspace and U.S.-China Relations, Council on Foreign Relations, New York, 26 Jan 2022

[cxli] Understanding the Vulnerabilities in China's New Joint Force, 960th Cyber Space Wing, Joint Force Quarterly 103, 14 Oct 2021

[cxlii] Understanding the Vulnerabilities in China's New Joint Force, 960th Cyber Space Wing, Joint Force Quarterly 103, 14 Oct 2021

[cxliii] To Rule the Invisible Battlefield: The Electromagnetic Spectrum and Chinese Military Power, Texas National Security Review, 05 Jan 2022

[cxliv] Competition and Conflict: Implications for Maneuver Brigades, Modern War Institute at West Point, June 2021

[cxlv] Competition and Conflict: Implications for Maneuver Brigades, Modern War Institute at West Point, June 2021

[cxlvi] China's Ambitions for AI-Driven Future Warfare, Jewish Policy Center, Washington, Winter 2022,

[cxlvii] How Does China Aim to Use AI in Warfare?, thediplomat.com 28 December 2021

[cxlviii] Pentagon rattled by Chinese military push on multiple fronts, https://apnews.com/article/technology-china-asia-united-states-beijing-aea288656fab23253ee0397dc21ba68a By Robert Burns November 1, 2021

[cxlix] China's Military: The People's Liberation Army (PLA), June 4, 2021 by Congressional Research Service

[cl] Why China Cannot Challenge the US Military Primacy, https://www.airuniversity.af.edu/JIPA/Display/Article/2870650/why-china-cannot-challenge-the-us-military-primacy/ Dec. 13, 2021 By Mangesh Sawant, Journal of Indo-Pacific Affairs, Air University Press

[cli] Chinese military equipment lack quality, https://www.business-standard.com/article/news-ani/chinese-military-equipment-lack-quality-say-experts-119110500818_1.html November 5, 2019 14:40 IST

[clii] Bangladesh Air Force faces problems over faulty Chinese military equipment https://www.timesnownews.com/international/article/bangladesh-air-force-faces-problems-over-faulty-chinese-military-equipment/828789 Nov 02, 2021 | 19:53 IST

[cliii] China-Pakistan military relations under strain due to substandard servicing, maintenance , https://economictimes.indiatimes.com/news/defence/china-pakistan-military-relations-under-strain-due-to-substandard-servicing-maintenance/articleshow/87037367.cms Oct 15, 2021

[cliv] China Is a Declining Power—and That's the Problem, The United States needs to prepare for a major war, not because its rival is rising but because of the opposite, SEPTEMBER 24, 2021, 4:16 PM, foreignpolicy.com

[clv] Shanghai lockdown: China spending and employment hit, https://www.bbc.com/news/business-61137195 15 April 2022

[clvi] "Zero-COVID" in Shanghai comes at high social and economic costs, https://www.piie.com/blogs/realtime-economic-issues-watch/zero-covid-shanghai-comes-high-social-and-economic-costs by Tianlei Huang of The Peterson Institute for International Economics, April 15, 2022 12:00 PM

[clvii] China power cuts: What is causing the country's blackouts?, bbc.com, 30 September 2021

[clviii] The Real Culprit – The PLA's Strategic Support Force , The Institute for strategic, political, security and economic consultancy (ISPSW) Berlin, February 2020

[clix] China Is a Declining Power—and That's the Problem, The United States needs to prepare for a major war, not because its rival is rising but because of the opposite, SEPTEMBER 24, 2021, 4:16 PM, foreignpolicy.com

[clx] China Is a Declining Power—and That's the Problem, The United States needs to prepare for a major war, not because its rival is rising but because of the opposite, SEPTEMBER 24, 2021, 4:16 PM, foreignpolicy.com

[clxi] China's Grand Strategy: Trends, Trajectories, and Long-Term Competition. (part of project entitled U.S.-China Long-Term Competition sponsored by the Deputy Chief of Staff, G-3/5/7, U.S. Army.) Santa Monica, CA: RAND Corporation, 2020.By Scobell, Andrew, Edmund J. Burke, Cortez A. Cooper III, Sale Lilly, Chad J. R. Ohlandt, Eric Warner, and J.D. Williams

[clxii] Military Power of the People's Republic of China 2009, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[clxiii] Military and Security Developments Involving the People's Republic of China 2016, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[clxiv] Military Power of the People's Republic of China 2020, Annual Report to Congress, Office of the Secretary of Defense, United States of America

[clxv] Military Power of the People's Republic of China 2021, Annual Report to Congress, Office of the Secretary of Defense, United States of America