CENTRE FOR AIR POWER STUDIES

In Focus

New Delhi

CAPS InFocus: 06/2022

24 January 2022

Digital Cold War

Air Marshal Anil Chopra PVSM AVSM VM VSM (Retd)
Director General, CAPS

Keywords: AI, Cyber, Connectivity, Digital, China, USA, Russia, Warfare, Technology.

Image Source: Fin Tech Futures

With connectivity technologies allowing the Internet of Things (IoT) and networking of "smart" devices that communicate seamlessly, the way the world does economic and commercial transactions, and the battlefields of the future wars are fast getting transformed. For long, the USA had dominated the Internet and high-end digital technologies, but China is today challenging the tech supremacy. While all major countries continue to invest heavily in physical war-fighting weapons and technologies, a non-kinetic, but perhaps even more lethal digital cold[1] war is now beginning to unfold. Clearly, the one who dominates the digital economy, the cyber and electronic warfare, and the information space will be the global leader.

China's Digital Leap

To catch up with the USA, China is unfolding its "Made in China" plan to achieve capabilities in most digital technologies by 2025[2]. These would include smart manufacturing, automation, robotics, nanotechnology, and chip-making. China has also given a digital direction to its defence industry. Its military engaged in a major transformation[3] the C4ISR (command, control, communications, computers, and intelligence), which includes secure digital communications using fibre-optics, satellite, microwave, and encrypted radios. It is a result of major R&D funding and is closely coordinated with China's flourishing commercial information-technology firms. A 2021 US Department of Défense's annual report on China's military made repeat mentions of "artificial intelligence[4]" and how the People's Liberation Army is heavily funding on secure networks and automation for "intelligentised warfare", in the process changing nature of warfare.

AI is an area of acute competition between the two nations. Indications are that China is on the way to becoming an AI superpower. China is also filing for largest digital technology patents. AI will support decision making, intelligence analysis, autonomous vehicles, automated warfare, and electronic warfare and cyber operations. Beijing has also announced a digital economy plan with targets for core industries to achieve 10 per cent of gross domestic product by 2025 from current 7.8 per cent. Chinese labs are already working on 6G mobile transmission technology. Beijing wants to become independent in digital capabilities, and have ability to set standards. China is also using data for military advantage. By combining space, electronic warfare and cyber under a single agency, the People's Liberation Army's Strategic Support Force, they have synergised the three[5]. China is also making huge investments in space which is the ultimate enabler for digital communications.

USA Unfolds Response

To counter China, the U.S. administration has adopted what is called the "small yard, high fence[6]" strategy" which is essentially meant to decouple from China in high technology areas like artificial

intelligence, quantum computing, bioscience, 5G, etc. which the USA considers has security implications. This is being achieved through export restrictions on items like semi-conductors, tightening spying by employees of Chinese origin. President Biden has proposed an "Alliance for the Future of the Internet[7]" which is meant to promote secure internet connectivity among countries that are open, have democratic values, and respect for human rights, and exclude authoritarian powers who promote disinformation. Effectively it would mean excluding Russia and China for a certain degree of digital access. This has also stemmed from Russian interference in American internal affairs and China's stealing technology through unfair means. The proposal is planned to be discussed with nearly a 100 countries in a special meeting. Russia and China are not included, interestingly Taiwan is included. Clearly the aim is to link digital economic connectivity to ideology, human rights, and geopolitics. The USA will increase engagement with Asian countries to reduce their dependence on China.

Free from its pre-occupations in West Asia, the U.S. military has now looking at Indo-Pacific[8]. It has also begun making major investments in the military, and specifically digital technologies. They are also marshalling the resources, technology and political will to take on China, with the aim to maintain technology lead.

Disinformation and Misinformation

With wider internet connectivity, many countries are using the same to peddle, ideology, as part of moulding minds, and pushing misinformation. Many countries have started questioning digital giants like Facebook, Google and other social media companies for allowing questionable or inflammatory content as news feed, and are re-examining their access to local populations. Google controls 86.6 percent of the search engine market. Facebook has 2.6 billion monthly active users, with 290 million in India alone[9]. Considerable access to personal data is another serious issue engaging the world. There is a demand for giving greater control to users for what they may see. Russia had reportedly used social media to spread false information to meddle in the 2016 US election. In recent times even governments and political parties are using social media to influence both domestic and international public opinion. China's state-controlled Global Times and Pakistan's DG ISPR are known for the same in the Indian sub-continent. China is also planting disinformation and exaggerated own capabilities on internet for propaganda and Psychological Ops. China also used disinformation to try to influence elections in Taiwan, and to discredit protestors in Hong Kong, and hide the origins of Covid-19. Clearly, propaganda is more diffuse and indiscriminate. The cost and technical skills required for online disinformation campaign are relatively low. The number of players and quantum of malicious content is on the rise. Often disgruntled domestic entities are in the fray and can cause greater damage.

Large Technology Companies

As per 2021 global list of large technology companies, Western companies like Apple, Samsung, Alphabet, Foxconn, and Microsoft are in the lead. China's Huawei comes at sixth position, and Tencent and Lenevo are at 13 and 15th position. USA, South Korea, Japan, and Taiwan dominate. There is no Russian company. Among the ten largest internet companies, there are five each from USA and China, with Amazon and Alphabet in the lead by market capitalisation. China is thus catching up.

Future Warfare will Be Digital

Despite Russian forces being massed on Ukraine's borders, and China making threatening forays into Taiwanese airspace, most countries are making greater defence investments in digital technology, artificial intelligence, space and cyber. There will be equivalent cuts in traditional hardware. Alongside the Army, Air Force and Navy, digital is now a vital domain for confronting a nation's enemies. While hypersonic weapons are being tested by all advanced nations, and they are carrying out missile tests to attack targets in space, the number of daily cyber-attacks are simultaneously increasing exponentially. These are part of the no-war no-peace scenario prevailing all the time. Disruptive cyber-attacks are being used to shape adversary populations' minds, and steal sensitive data. The world has to prepare for both a defensive and offensive cyber-warfare. Future war will begin with a massive cyber-strike to block communications, blind satellites, and jam sensors. They would also incapacitate utilities like water and electricity grids, create havoc in logistic supply chains, to destroy the will of the people. The target will be to disrupt decision making chains. The targets will be whole societies and not just the military. In all this, Artificial Intelligence (AI) will play an important role[10]. AI will support unmanned systems and man-machine teaming. That is where digital capabilities become important, and the race for digital dominance. On some of these counts, China is investing much more and tending to pull ahead.

Way Ahead

Warfare of future will be more technology-driven. It is time for all to re-focus on emerging digital technological capabilities which will have huge operational impact. Combating disinformation would need coordination between the government agencies and the private organisations. Countries are criminalising disinformation and promoting media literacy[11]. Technology companies would have to understand the sensitivities related to fake news and deep-fakes and introduce checks and balance, lest countries are forced to curb their operations through regulations. Like minded countries would have to apply minds together and take a collaborative approach. It is time to plan and prepare for multi-domain operations. Digitisation of the militaries will be important. In

digital world it will have to be an all-country approach. The digital scientist is now a combatant. The boundary between conflict and non-conflict is blurring. Machine learning, quantum computing, and block-chain will have to be mastered and applied. Events will unfold much faster, and decision making will have to be quicker supported by AI. Digital and AI will support situational awareness. They will also be required for autonomous weapons. There are many countries of the free world that have advanced digital technologies. These include European, Israel, Japan, Taiwan, and South Korea. India has great potential and needs to invest more. Digital is where the actions is, and the Digital Cold War is already beginning between the free world and close controlled autocracies.

NOTES

1. Orange Wang, China must brace for 'digital cold war' with US as battle for tech supremacy heats up, South China Morning Post, January 23, 2022, https://www.scmp.com/economy/china-economy/article/3164367/china-must-brace-digital-cold-war-us-battle-tech-supremacy Accessed on 23 January 2022.

2. Anjani Trivedi, The Made in China plan is back, and its better, The Economic Times, January 07, 2022, https://economictimes.indiatimes.com/small-biz/trade/exports/insights/the-made-in-china-plan-is-back-and-its-better/articleshow/88702912.cms Accessed on 23 January 2022.

3. Evan S. Medeiros, Roger Cliff, Keith Crane and James C. Mulvenon, A New Direction for China's Defense Industry, Rand Corporation, Chapter 5, Page 205, https://www.jstor.org/stable/pdf/10.7249/mg334af.12.pdf Accessed on 23 January 2022.

4. Ryan Fedasiuk, We Spent a Year Investigating What the Chinese Army Is Buying. Here's What We Learned., Politico, November 10, 2021, https://www.politico.com/news/magazine/2021/11/10/chinese-army-ai-defense-contracts-520445 Accessed on 23 January 2022.

5. Frank Gardner, What does future warfare look like? It's here already, BBC, December 30, 2021. https://www.bbc.com/news/world-59755100 Accessed on 23 January 2022.

6. Wang Dong, Reluctant Rival: Beijing's Approach to US-China Competition, Global Asia, December 2021 (Vol.16 No.4), https://www.globalasia.org/v16no4/cover/reluctant-rival-beijings-approach-to-us-china-competition_wang-dong#:~:text=%E2%80%9CSmall%20yard%2C%20high%20fence%E2%80%9D,to%20protect%20its%20technological%20competitiveness. Accessed on 23 January 2022.

7. Thomas Macaulay, What we know about Biden's Alliance for the Future of the Internet, The Next Web (TNW), December 30, 2021, https://thenextweb.com/news/what-is-alliance-for-the-future-of-internet-joe-biden-web-plans Accessed on 23 January 2022.

8. ROBERT BURNS, Pentagon rattled by Chinese military push on multiple fronts, Associated Press, November 1, 2021 https://apnews.com/article/technology-china-asia-united-states-beijing-aea288656fab23253ee0397dc21ba68a Accessed on 23 January 2022.

9. Leading countries based on Facebook audience size as of January 2021, Statista, December 13, 2021, https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/#:~:text=Facebook%20%E2%80%93%20the%20most%20used%20social,revenue%20is%20generated%20through%20advertising. Accessed on 23 January 2022.

10. James Lawrence, A vision for the digital future of warfare, Global Intelligence for Digital Leaders, January 2021, https://www.i-cio.com/strategy/digitalization/item/a-vision-for-the-digital-future-of-warfare Accessed on 23 January 2022.

11. Research Briefs, Disinformation That Kills: The Expanding Battlefield of Digital Warfare, CB Insights, October 21, 2020, https://www.cbinsights.com/research/future-of-information-warfare/ Accessed on 23 January 2022.