JOINT C6ISR AND EXPLOITATION OF SPACE DOMAIN - A ROADMAP TO ADDRESS THE CAPABILITY GAPS

Lt Gen Anil Kapoor, AVSM, VSM (Retd)*

Abstract

The New Tech World Order is defined by Four Ds – Data, Digitization, Digitalization and Disruption. While these have fueled digital transformation globally giving rise to a large number of dual use technologies which are drivers of automation & autonomous applications, it is disruption which is not only transforming technologies at an unprecedented pace, but also transforming business concepts, models, processes and practices. While automated systems are rule based, the autonomous systems are designed and programed to take decisions and act. Supported by AI, IoT, Augmented Reality (AR), Virtual Reality (VR), big data analytics and block chain technology and driven by cloud and quantum computing, 5G, the ICT based system of systems have revolutionized military and dual use technologies. Convergence of Info-Communication Technologies and their combination has fueled Disruption in Military Affairs (DiMA).

DiMA has transformed automated decision support systems (DSS) to autonomous DSS and resulted in the design and development of Command, Control, Communication, Computers, Cyber and Combat Intelligence, Surveillance and Recce (C6ISR). C6ISR is a combination of technologies to generate an autonomous integrated Tri Services decision support system. Concurrent with C6ISR is the Space Domain which is the mainstay for geo-spatial enabled situational awareness, and uses satellites and other outer space technological applications to support

civilian, military and dual usage operations. Presently, India has around 15 military-application satellites, with the latest GSAT-7A dedicated to the Air Force and shared by the Army, with a revisit time of up to 96 hours. This is proposed to be reduced to six hours approximately by a number of satellite launches in the next five years. While high resolution imagery facilitates a number of military and disaster management applications, there are immense dual use applications.

Given the C6ISR and space domain technology driven pay offs, the counter measures for cons in terms of cyber, EW and anti-satellite (ASAT) threats are equally important. The paper analyses the technology landscape for creation of C6ISR and exploitation of the space domain and development of counter measures. This calls for a National and Tri Services Technology Strategy to achieve the paradigm of C6ISR as future technology landscape for future warfare.

Introduction

General. Over the past decade, technology has given the flesh to an age old product adage, 'whatever can be defined can be designed', albeit in a shorter time frame, in intent, context and content, given the unprecedented technological disruption. The manifestation of the technology outreach whether obtrusively or unobtrusively, by kinetic and non-kinetic means, has redefined on what constitutes an act of war. That said, the New Tech World Order is defined by Four Ds – Data, Digitization, Digitalization and Disruption. While these have fueled digital transformation globally giving rise to a large number of dual use technologies which are drivers of automation & autonomous applications, it is disruption which is not only transforming technologies at an unprecedented pace, but also transforming business concepts, models, processes and practices. While automated systems are rule based, the autonomous systems are designed and programed to take decisions and act. Supported by AI, IoT, Augmented Reality (AR), Virtual Reality (VR), big data analytics and block chain technology and driven by cloud and quantum computing, 5G, the ICT based system of systems have revolutionized military and dual use technologies.

The Revolution in Military Affairs, powered by digital transformation and niche disruptive technologies which impact the entire bandwidth of military activities be it info gathering, intelligence, recce, surveillance, training, logistics, decision support, control of resources both for defensive and offensive operations, has given rise to Disruption in Military Affairs. Further, the spectrum of conflict has enhanced from land, sea, air to cyber, space, psychological (Informational / mis-informational) and hybrid. In an overall analysis, the disruptive technologies, with or without man in the loop, is about enhancing velocity of OODA loop, as the driver of decisive proactive actions for enhanced situational awareness and combat effectiveness. The paradigm of future warfare is best defined as C6 ISR – Command, Control, Communication, Computers, Cyber, and Combat ISR in a close knit autonomous loop. This Disruption in Military Affairs has ushered an era with the concept that "Victory is measured by Digital Footprint", for all those of us who would still like to believe that victory is measured by foot.

In the recent past events, military actions have demonstrated that the VUCA of military or military-like interventions have been executed by embracing disruptive technologies. To recount a few major ones, the explosion damaging a centrifuge assembly plant last July and the recent large-scale blackout at Natanz, which the country's Atomic Energy Agency acknowledged had damaged the electricity grid or the killing of Iran's chief nuclear scientist, have portrayed the shape of things to come, in the spectrum of conflict.[1] In a similar vein, though by non-state actors, Yemen's Iran-backed Houthi rebels attack on Aramco refinery in the Saudi capital on 12 Apr 21 (and earlier on 14 Sep 19), using bombs and missiles laden drones, is an offensive act on the Kingdom's energy and security installations[2]. These drones reportedly flew more than 500 kms in an autonomous mode and hit their targets with precision. But

1 Chulov Martin, Israel appears to confirm it carried out cyberattack on Iran nuclear facility, The Guardian, April 11, 2021

2 Mohammed Hatem and Zaid Sabah. Houthi rebels attack Saudi Aramco sites for the second time in a week, World Oil, April/15,2021

an apt example of a decisive war through technology is the Armenian -Azerbaijan War. It is, in effect, the first war in the history of modern warfare that has been won almost entirely on the strength of drone warfare[3]. While Armenia only fought with tanks, artillery and air defence systems, Azerbaijan relied heavily on drones, specifically the Turkish-made Bayraktar TB2 and the Israeli-made Kamikaze drones.

Aim

The aim of this paper is to cull out the technology stack for adoption of joint Command, Control, Communication, Computers, Cyber, Combat ISR (C6ISR) and exploitation of space domain in Indian Armed Forces.

Scope

The road map for embracing C6ISR and space domain must be driven by a well-defined technology strategy with milestones over a decade of marathon. This calls for a programme akin to Integrated Guided Missile Development Programme, for curating a Tri Service integrated C6ISR plan. Accordingly, the paper is laid out in the following salient technology stack:-

(a) Military Small Satellite Geo Spatial Programme.
(b) Military ICT Transformation Programme.
(c) AI as a Service Programme.
(d) C6ISR Programme.
(e) Military Cyber Programme.
(f) Technologies roll out – the way forward.

C6ISR Technologies & Space Domain

C6ISR is a combination of exponential disruptive technologies of game changing small ideas with a big physical and psychological impact. These

3 Gupta Shekhar, How drones helped Azerbaijan defeat Armenia, and the implications for future modern warfare, The Print, Nov14, 2020

technologies have a dual civil-military application, a Tri Service flavor, align for a joint and integrated military applications and create a paradigm shift in the character of warfare, and design, means, and methods of war fighting, thereby creating an asymmetric advantage through application military power. In the recent past there is an ongoing arms race based on disruptive technologies for military applications, with USA, Russia and China in the lead. The 2018 US National Defence Strategy has echoed the view that the US national security will likely be affected by rapid technological advancements and the changing character of war, " *……..New technologies include advanced computing, "big data" analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology—the very technologies that ensure we will be able to fight and win the wars of the future……"*[4]. That said, there is a need for India to identify disruptive technologies, their military applications and a capability matrix based on a work time for acquisition/ research, design, development and induction plan. This could be based on a capability based mission priority programme akin to Indian Integrated Guided Missiles Development Programme. The intent should be to achieve technology sovereignty over the next decade.

Technology Lens I: Military Small Satellite Geo Spatial Programme (MSSP)

Satellites offer huge ISR advantages, which is the centre of gravity of military planning and execution. Military satellites as a part of communication and other application based satellite systems and leasing satellites has been a need based part of military perspective planning. No wonder then, there are satellite for Indian Air Force, Navy, Army and various info systems of systems including AWACs and strategic recce missions and programmes. Presently, India has around 15 military-application satellites, with the latest GSAT-7A dedicated to the Air Force and shared by the Army. By end 2022[5], the $225 million

4 US Congressional Research Service, Emerging Military Technologies: Background and Issues for Congress, Updated November 10, 2020, https://crsreports.congress.gov

5 Neelam Mathews , "India Ramps up Military Satellite Plans", Defence Notes, Shephard

GSAT-7R, an Indian Navy communications satellite, will replace GSAT-7 Rukmini launched eight years ago. It is the last of the Indian Space Research Organisation's seven fourth-generation satellites with a 2,000nmi coverage range over the Indian sub-continent. As the need for maritime domain awareness grows, and as border tensions with China and Pakistan increase, vulnerabilities in Indian space security have made it mandatory to look to build up its minuscule number of military satellites.

With the proliferation in miniaturized small satellites and ease of their launch, an eye in the sky as a low earth orbit satellite is a huge disruptive technology. Given the need to defend vast borders delineated by volatile international border, line of control and line of actual control and the coast line, deep and shallow look capabilities through a technology solution is a dire necessity. A large number of surveillance devices are deployed, but given the porosity and the sheer length of the borders and areas of interest and influences, for round the clock surveillance, Indian Military must develop capability to launch Nano - tech enabled Low Earth Orbit Satellites and have a GIS platform duly integrated as a MSSP. One rationale for miniaturizing satellites is to reduce the cost and being lighter, require smaller and cheaper launch vehicles, which can sometimes be launched in multiples. They can also be launched 'piggyback', using excess capacity on larger launch vehicles. Miniaturized satellites allow for cheaper designs and ease of mass production. A number of academic institutions, startups and private sector are currently developing small satellites and launch mechanisms (vehicles) to perform the increasingly targeted launch requirements of microsatellites. Accordingly, MSSP could be launched, as an adjunct to National Disaster Management Programme, to monitor avalanches and other natural calamities to facilitate disaster relief as a, but primarily keep continuous watch in the areas of interest and influence for military targets of interest. The Programme is recommended as a Joint ISRO – DRDO - Armed Forces Programme, as Public Private Partnership

Press Limited, 31 May 2021

Project by integrating startups and private industries in the field of satellite technology. Given the provisions of DAP 2020, in the short term, key private players may be approached for leasing Space Infrastructure as a Service to empower space based applications and as a long term a dedicated Programme be collaboratively generated[6] . The platform ground station would be geo spatial enabled for accurate position fixes. This Programme could be the vanguard to unleash the Tri Service Space Command.

Pay Offs Envisaged. The following pay offs are envisaged for 24/7 situation awareness:

(a) Red Force Tracking and intelligence collection in real time including tracking key military targets of interest.

(b) Blue Force Tracking in real time thereby facilitating C2.

(c) Seamless all weather EM and satellite communication.

(d) Platform for electronic warfare – electronics surveillance, electronics counter /counter-counter measures.

(e) Weather and met data for artillery and long range vectors though autonomous software systems.

(f) Effective disaster management through proactive forecasting and follow up actions.

Technology Lens II: Military ICT Transformation Programme

Digital transformation can be best accomplished as a Tri Service Programme. The three Services have varied standards, capabilities and capacities of automation. There is a dire need to create a Tri Services ICT Digital Platform with mega data centres duly networked by Network for Spectrum (NFS) currently under execution. The power of digital transformation can be best harnessed by joint Armed Forces Integrated Information System comprising management information

6 Website dhruvaspace.com

systems, operational logistics information systems and operational / combat information systems. There are stand alone information systems that each Service has configured and some of these need to be and can be integrated through well thought through automated programme interfaces (APIs). A case in point is the IAF, Integrated Air Command and Control System (IACCS), which can be combined into a Tri Service Air Defence Combat System which can be integrated with other operational combat management information systems. Given the cyber threats, and ICT convergence a holistic approach to address major voids need a long term action plan are as follows:-

(a) Major information technology voids exist in terms of the Armed Forces Operating System (AFOS). There is a need to revamp a Linux based OS like BOSS which can be scaled up as an exclusive AFOS.

(b) A Tri Service GIS needs to be created for effective geo referencing through digital maps.

(c) A Tri Service Data Base is yet another building block. Blockchain technology based systems for enterprise resources planning need to be designed and developed.

(d) A Tri Service software defined radios (SDR) – hand-held, man pack and vehicle/ship/aircraft based.

(e) **Quantum Computing Technologies.** Quantum computing systems are the mainstay of design and development of future SDRs, software defined radars and ICT systems for military and space applications. As an extension, chip and nano technologies need to be developed to produce miniaturized man pack and mobile platforms for effective military exploitation of state of the art technologies.

(f) **Laser Based Communication System (LBCS).** The VUCA of electronics warfare environment calls for design and development of LBCS. This could be used for creating

redundancies in critical communication links voice, data and video. The laser wave is coherent, line of sight and agnostic of any interference.

(g) HAM Radios as a formal means of communication with encryption could also be developed in select areas of operations for effective communication. There is a need to develop theatre based HAM clubs for augmenting all weather communication.

Technology Lens III: Artificial Intelligence (AI) as a Service Programme

AI is best exploited as a multi-faceted platform offering algorithms and deep learning systems for voice, text and video data[7] as a service, AIaaS. A systemic platform would typically choose algorithms and deep learning combinations to analyse data, structured, unstructured, for pre-defined or online queries and actionable outputs. There is a dire need to develop AI as a Tri Service platform which can run applications to include the following:

(a) **Imagery Interpretation.** The manual process for a satellite image with a raster of 64 sq km takes approximately six hours of laborious slog. AI based platforms can list out the military targets of interest in less than 10 minutes. This can be enhanced to identification and image processing on the fly for manned aircraft or unmanned aerial platforms on the fly.

(b) **ISR.** AI can be effectively used for intelligence collation, analysis and synthesis from all sources electronics, optical, thermal and human to create an actionable intelligence picture both augmented reality (AR) and virtual reality (VR). This capability can help in identifying military targets of interest and build operational scenarios. As an example, seek and strike missions based on target-shooter mapping and post-strike damage assessments.

7 Kai-Fu Lee, AI Super-Powers China, Silicon Valley and The New World Order, PP 140-141

(c) **War Gaming.** AI platforms can be best configured for Tri Service scenario building and net assessment exercises and create contingencies from tactical to strategic levels through AR and VR.

(d) **Swarms of Unmanned Systems.** AI platforms are being used to configure ground based unmanned systems (robots), aerial unmanned systems and both sea based and under-water / submersible unmanned systems and hybrid systems like, ground and aerial swarms. These technologies are game changers in future warfare and a paradigm shift from automation (business intelligence) to autonomous systems.

(e) **Asset Management and Operational Logistics.** Operational logistics and supply chain in the Tri Services are based on manual and just in case methods which are location based and cost prohibitive, The time dimension of inventory, assets and supply chain management could be electronically driven for huge optimization and cost effective solutions using e asset systems, Block chain and AI. Blockchain technology is best suited system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A Blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Convergence of Blockchain and AI can enhance machine learning and enable AI to create and trade financial products. While Blockchain enables secure storage and sharing of data or anything of value. AI can analyze and generate insights from data to generate cost effective value[8].

Technology Lens IV: C6 ISR Programme

Future warfare is autonomous technology based action interspersed with

8 Raj Shroff, When Blockchain Meets Artificial Intelligence, Start it Up, Feb 14, 2020

military troops intervention, based on criticality of the mission. With man in the loop and man out of the loop missions, in effect, C6 ISR based autonomous weapons systems are lethal devices that have been empowered by their human creators to survey their surroundings, identify and track potential enemy targets, and independently choose to attack those targets on the basis of sophisticated algorithms. These systems typically comprise a *seek and respond* system. *Seek* is an autonomous pivot which could be land, ship or aerial platform with computer based systems, application software configured as C6ISR based decision support tightly integrated with the *respond* strike autonomous system mobile maneuver arm comprising combat platforms both kinetic and non-kinetic in automated system with man in the loop or autonomous systems with man out of the loop. Such systems require the integration of several core elements: a mobile combat platform, such as a drone aircraft, ship, or ground vehicle; sensors of various types to scrutinize the platform's surroundings; processing systems to classify objects discovered by the sensors; and algorithms directing the platform to initiate attack when an allowable target is detected. The U.S. Department of Defence describes an autonomous weapons system as a "weapons system that, once activated, can select and engage targets without further intervention by a human operator."[9]

C6ISR, is, therefore, a programme which will encapsule a number of disruptive technologies. Many semi-autonomous weapons in use today rely on autonomy for certain parts of their system but have a communication link to a human that will approve or make decisions. In contrast, a fully Autonomous Weapon System (AWS) could be deployed with an established communication network and would independently respond to a changing environment and decide how to achieve its pre-programmed goals. AWS may create a paradigm shift in how we wage war. This revolution will be one of software; with advances in technologies such as facial recognition and computer vision, autonomous navigation in congested environments, cooperative autonomy or swarming,

9 US Department of Defence, "Autonomy in Weapons Systems," Directive No 3000.09, November 21, 2012

these systems can be used in a variety of assets from tanks, ships, submarines to small commercial drones. They would allow highly lethal systems to be deployed in the battlefield that cannot be controlled or recalled once launched. Unlike any weapon seen before, they could also allow for the selective targeting of a particular group based on pre-defined target parameters. In effect, AWS will facilitate a deep strike with precision, thereby reducing collateral damage. Viewing AWS from a technology lens, it comprises almost all niche disruptive technologies, sensor technologies and IOT, unmanned autonomous aerial and ground based platforms, cyber, electronics warfare, directed energy weapons, quantum technologies, big data analytics, nanotechnologies, geo- spatial technologies an AI . The ongoing conflict between Israel and Hamas is an apt example in the use of C6ISR and precision in targeting.

Technology Lens V: Military Cyber Programme

Digital eco system is essentially creating a virtual platform of info systems with many points of vulnerability increasing the attack surface, thereby giving rise to growing cybersecurity concerns. In fact, cyber has been major disruptor – a cyber warrior may be a bermuda clad professional who can execute cyber maneuvers at anytime from anywhere. According to the annual IBM X-Force Threat Intelligence Index, India reported the second highest number of cyber-attacks after Japan in the Asia-Pacific region in 2020, accounting for 7 percent of all cyber-attacks observed in Asia in 2020. Likewise, organizations have also incurred heavy financial losses due to disruptions and data breaches. A 2019 report by IBM revealed that cyberattacks cost India ₹12.8 crores on an average between July 2018 and April 2019. During the same period, the average cost globally of a data breach was ₹ 27 crore. Besides these financial losses, cyberattacks can and have caused huge dents in an organization's overall brand value. With digital adoption breaking grounds especially in the Armed Forces, the corresponding cyber maturity must keep pace with the technological strides – greater exposure to cyber risks calls for a greater focus on cybersecurity.

That said, cyber threat is a 24/7 phenomenon globally. The report titled, 'Shadows in the Cloud', in 2010, documented a complex ecosystem of cyber espionage that systematically targeted and compromised computer systems in India, the United Nations and several other countries. The investigation recovered a large quantity of stolen documents which included sensitive and classified info belonging to the government, business, academic, and other computer network systems and other politically sensitive targets. The report analyzed the malware ecosystem employed by the Shadows' attackers. The system leveraged multiple redundant cloud computing systems, social networking platforms, and free web hosting services in order to maintain persistent control while operating core servers located in the People's Republic of China (PRC). Although the identity and motivation of the attackers remain unknown, the report provides evidence that the attackers operated or staged their operations from Chengdu, PRC[10]. Given the invisible nature of a cyber threat, its huge proliferation and the capability to disrupt C2 and compromise operationally sensitive info (data), Tri Services Cyber Command has been planned. The following technology landscape is imperative to energize the cyber command:-

(a) There is an increasing need for businesses to adopt a proactive cybersecurity strategy that encompasses everything and helps organizations protect sensitive operational data, personally identifiable information and military information systems, from theft and damage attempted by cyber-criminals.

(b) All Organizations must observe a rigorous enforcement of security policies. This means ensuring and implementing adequate training and awareness on data protection, implementing appropriate security software and keeping it updated, ensuring data encryption, and backing up data regularly.

(c) Adopting a zero-trust security architecture can also help manage cybersecurity incidents. Zero Trust is a security concept

10 https://itlaw.wikia.org/wiki/Shadows_in_the_Cloud:_Investigating_Cyber_Espionage_2.0.

that requires access control for all users, even those inside the organization's enterprise network, to be authenticated, authorized, and continuously validate security configuration and posture, before being granted or keeping access to applications and data.

(d) **Cyber Defence in Depth.** There is a need to protect the data centres and IT assets using encryption for data in rest, software security protocols and cyber security hardware, firewalls and IT asset security systems on the edge, This multi-layer approach would entail new security protocols that every digital soldier should embrace, even if slightly inconvenient.

(e) A Security Operations Centre (SOC) and Network Operations Centre are specialized central teams focusing on protecting the digital assets of organizations. The team comprises cyber-security experts who continuously monitor and analyse the Information & Communication Technologies (ICT) infrastructure as well as the threat landscape. A combination of practices and tools can help assessment, prevention, detection and response to incidents on websites, application/database servers, and networks among other systems. Military organizations must set up SOC - NOC to manage the security of their digital infrastructure and systems. This will enable significant improvement in security preparedness by timely detection of and response to security incidents, by driving preventive and predictive actions.

(f) **Offensive Cyber.** Attack is the best form of defence. Offensive cyber is the key to achieving informational cyber ascendancy over an adversary. There is a need to harness the potential of young IT enabled graduates to create a ready pool of cyber offensive invisible warriors with an aggressive cyber intent. With the next generation of cyberattacks being carried out with greater scale and sophistication, organizations, now more than ever, have a greater responsibility to protect people who have access to essential data.

Technology Roll Out – The Way Forward

There is a huge opportunity in futuristic niche disruptive technologies. Aatmanirbharta, Make in India (MII), Start Up India, industrial corridors and defence industrial bases are Government initiatives to drive consciousness for self-reliance. It is like putting a finger on the jugular vein of technology development for diagnosis, but the answer lies in prognosis and prescription.

Knowing what to do and getting things done are twos sides of the management coin and India has the will and ability for both. The best model to self-reliance is creation of our own unique model which gives homegrown indigenous solutions. The Moot Question is - Do we have a technology strategy to make Aatmanirbharta and MII happen? This requires a well-articulated National Technology Strategy (NTS). Some thoughts on plausible key determinants of the NTS are analysed in succeeding paras.

Tri Service Technology Strategy. A number of initiatives have been taken under the National Technology Development Board to create technology verticals and Centres of Excellence (CoE) in identified technologies. Each Ministry has a few CsoE. These efforts need to be vectored and drawn into a cogent technology strategy with a clear technology forecast, technology development work time action plan with clearly articulated deliverable milestones and end state of each vertical. As a part of this National Technology Strategy, a Tri Service Technology Strategy with a tech forecasting and development implementation plan for C6 ISR must be prepared.

Consortium Approach. A number of R&D Orgs within the Govt, private sector and academia exist, employing subject matter experts (SMEs) and deploying huge amounts of funds on R &D. These resources can be optimized through a two pronged strategy.

(a) Build synergies between academia, public sector, private industry, startups, R and D Orgs and Government Institutions like CoE, STPI etc dealing with technology development where

technologies are incubated and churned out as prototype use cases.

(b) Create a legislation and control regime to synergize the efforts of these R and D synergies with the concept of One technology One team (OTOT). R and D efforts must become a meaningful engagement through agencies complementing and not competing with each other. As an example, all agencies dealing with space applications need to register with an appropriate vertical under the Technology Development Board for creating synergies and jointness among SMEs. Based on the areas of research and development, consortiums of SMEs will reduce the chances of reinvention of the same wheel and facilitate faster development and quick impact utilization of each wheel optimally. In any case this is the need of the disruptive times – think big, start small, fail fast, recover faster – be first, be agile.

Corporate Professional Responsibility (CPR) Funding R &D. R&D and technology development is a painstaking exercise of design and redesign - an exercise requiring huge funds to go through iterations of trials and errors bereft with failure cycles in an arduous journey to fruition. There is, therefore, a requirement of large funds to develop and sustain niche disruptive technologies. Govt would do well, in the interest of the Aatmanirbharta, to institutionalize a fund titled CPR Technology Development Fund under Companies Act 2013 for technology development as a National initiative. This fund, in effect, would be akin to Corporate Social Responsibility Fund- two percent which Companies deploy based on turn overs and profit margins. The Technology Incubation Centres, Technology hubs, start ups need to be funded by industrial houses and Government in joint ownership and guided by identified sub matter experts.

Conclusion

The New World Order respects Nations with the strength to manage VUCAD (Volatility, Uncertainty, Complexity, Ambiguity and Disruption).

Bewildered and worried by the struggle, a child opens the cocoon to let the butterfly fly off. Alas, the butterfly failed to fly and died since the wings did not develop the intrinsic strength afforded by the Nature in the struggle moments of decocooning. With a good intent but inadequate knowledge of hows and whys of the child, a potential creation was dead. Aatmanirbharta and MII is a great strategic intent. In the backdrop of a strong tech base provided by ISRO, DRDO, Technology and Innovation Centres of industries & PSUs, Startups and T Hubs, the time is ripe to strengthen the cocoon through a well thought through technology strategy and fly out the indigenous technology butterfly globally.

Towards this end, the industrial corridors pan India and two defence industrial corridors need to be developed with the thought of Made in India. The C6ISR is a tech sojourn for future jointness in warfare and must become an illustrious lasting tech journey. Let us do it!

***Lt Gen Anil Kapoor,** AVSM, VSM, is a former Director General Electronics and Mechanical Engineering (EME), Indian Army

Bibliography

1. Chulov Martin, Israel appears to confirm it carried out cyberattack on Iran nuclear facility, The Guardian, April 11, 2021
2. Mohammed Hatem and Zaid Sabah. **H**outhi rebels attack Saudi Aramco sites for the second time in a week, World Oil, April/15, 2021
3. Gupta Shekhar, How drones helped Azerbaijan defeat Armenia, and the implications for future modern warfare, The Print
4. Raj Shroff, When Blockchain Meets Artificial Intelligence, Start it Up, Feb 14, 2020
5. US Congressional Research Service, Emerging Military Technologies: Background and Issues for Congress, Updated November 10, 2020, https://crsreports.congress.gov
6. Neelam Mathews , "India Ramps up Military Satellite Plans", Defence Notes, Shephard Press Limited
7. Kai-Fu Lee, AI Super-Powers China, Silicon Valley and The New World Order
8. US Department of Defence, "Autonomy in Weapons Systems," Directive No 3000.09, November 21, 2012
9. The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower Paperback ,31 May 2019
10. https://itlaw.wikia.org/wiki/Shadows_in_the_Cloud:_Investigating_Cyber_Espionage_2.0
11. Website dhruvaspace.com