VIF PAPER | March 2021

CYBER DNA OF CHINA

Deep, Focussed and Militarised

Dr Gulshan Rai

Vivekananda
International
Foundation

Published in 2021 by

Vivekananda International Foundation

3, San Martin Marg | Chanakyapuri | New Delhi - 110021

Tel: 011-24121764 | Fax: 011-66173415

E-mail: info@vifindia.org

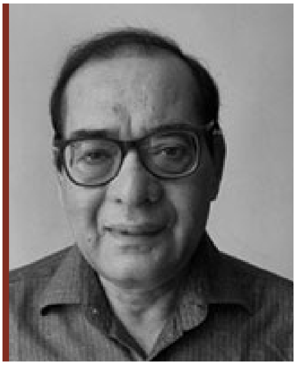
Website: www.vifindia.org

ISBN: 978-81-952151-9-5

Follow us on

Twitter | @vifindia

Facebook | /vifindia



Dr Gulshan Rai is Former National Cyber Security Coordinator, Government of India. He holds an M.Tech and Doctoral degree and has over 35 years of experience in different areas of Information Technology which include different aspects of e-Governance, cyber security, cyber laws and several related fields covering policies and operations.

Previously, Dr. Rai served in the Ministry of Electronics & Information Technology (MeitY), holding the prestigious post of Director General, CERT-In (Indian Computer Emergency Response Team) and heading the E-Security & Cyber Law Division, STQC and other divisions. As Executive Director of ERNET, he led work to connect more than 500 universities in the country and prepared the first blueprint of setting National Knowledge Network.

Dr. Rai authored India's first cyber security policy and served on the Expert Committee on Data Protection chaired by Justice BN Krishna. He also led work to establish India's National Watch and Alert System as part of the country's cyber security initiative and played a lead role in designing India's Income Tax PAN Number and the architecture of the computing system and environment at the Central Board of Direct Taxes (CBDT). Dr. Rai played a key role in planning and implementing the first phase of computerisation of the Bombay Stock Exchange.

Dr. Rai has led delegations to the UN, WTO and ICANN, as well as heading negotiations for bilateral and multilateral agreements with more than ten G20 countries.

Table of Contents

Acronyms

3PLA	General Staff Department's Third Department
3GPP	3rd Generation Partnership Project
4PLA	General Staff Department's Fourth Department
5G	Fifth Generation
APT	Advanced Persistent Threat
AR/VR	Augmented Reality / Virtual Reality
AI	Artificial Intelligence
ASEAN	Association of Southeast Asian Nations
BRI	The Belt & Road Initiative
BRICS	Brazil, Russia, India, China & South Africa
C2	Command and control
CAC	Cyber Space Administration of China
CCP	Chinese Communist Party
CCRA	Common Criteria Recognition Arrangement
CERT	Computer Emergency Response Team
CIPS	Chinese cross border interbank payment system
CMC	Central Military Commission
CNSC	Central National Security Commission
CPEC	China Pakistan Economic Corridor
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service

DNS	Domain Name System
FDI	Foreign Direct Investment
FINTECH	Financial Technology
GDP	Gross Domestic Product
GGE	Group of Governmental Experts
GSD	General Staff Department
ICT	Information and communication technology
IO	Information Operations
IP	Intellectual Property
ITU	International Telecommunication Union
ISO	International Standard Organization
IDC	International Data Corporation
KM	Kilo Meter
M&A	Merger & Accusation
MCF	Military - Civil Fusion
MPS	Ministry of Public Security
MLPS	Multi Level Protection Scheme
MSS	Ministry of State Security
NM	Nano Meter
NEC, Japan	Nippon Electric Company Limited, Japan
NFU	No First Use
NDU	National Defense University
OBOR	One Belt, One Road
OEM	Original Equipment Manufacturer
OECD	The Organization for Economic Cooperation and Development
PBSC	Politburo Standing Committee
PMA	Preferential Market Access

PLA	People's Liberation Army
PLAA	PLA Army
PLAAF	PLA Air Force
PLAN	PLA Navy
PLARF	PLA Rocket Force
PRC	People's Republic of China
R&D	Research and Development
S&T	Science & Technology
SSF	Strategic Support Force
SWIFT	Society for Worldwide Interbank Financial Telecommunications
SPFS	System for Transfer of Financial Messages – Russian Equivalent of SWIFT
TOR	The Onion Routing
TRB	Technical Reconnaissance Bureau
TSMC	Taiwan Semi connector Manufacturing Company
TTP	Tactics Technique & Procedures
UK	United Kingdom
UN	United Nations
UNGGE	United Nation Governmental Group of Experts
US	United States
USA	United States of America
VPN	Virtual Private Network
VPS	Virtual Private Server
WHO	World Health Organization
ZTE	Zhongxing Telecommunications Company Limited

Cyber DNA of China -
Deep, Focussed and Militarised

The strategic goals reconfirmed by the CCP, in late 1970's, included maintaining domestic stability; sustaining economic growth and development; defending national sovereignty and territorial integrity; safeguarding China's interest world over. The focus of the Fifth, Sixth and Seventh Five year Plans, was on investing in export industries, infrastructure, adaption and investment in technology development. China began opening its economy to the outside world and embraced market forces. Since then, China's growth and development have been spectacular. Today, it is the world's second-biggest economy after the US. According to World Bank data based on current exchange rates, China's Gross domestic product (GDP) per capita has grown from the equivalent of US $89.5 in 1960 to US $10,262 in 2019, a 115-fold increase.

China considers Cyber space and technology development as strategic domain. Cyber technologies and innovations considered as both threatening and empowering their regime to exercise influence domestically and internationally. Digital technologies and technological innovations are therefore, seen essential by Communist Party of China (CCP) for realising their goals of achieving economic and national security as well as to be largest nation in cyberspace and superpower of the world. Accordingly, Chinese Communist Party and State Councils, in 2015, emphasised the strategic importance of cyber technology for China's economic growth and internal security. They issued new guidelines and called out the use of new high- technologies and cyber technologies for strengthening economic and national security. China has effectively planned, created, and used cyber capabilities to realise the strategic objective of the Chinese Communist Party. All Tech and other industrial giants have set up CCP's committees.

The journey to make China economically and militarily strong started with the modernisation policy proposed in late 1970's by Deng Xiaoping. The emphasis was laid to prioritise to advance development in agriculture, industry, Science &Technology (S&T), and defence. The project 863 was planned and implemented in 1986 to narrow the gaps in computers, communication, biotechnology, nanotechnology, and other areas by investing more than US dollar 200 billion in the high-technology sectors. The China issued the national medium and long-term plan for the development of science and technology in 2010. The Plan encouraged Chinese nationals to go in for patents and publish papers to place China in top five innovators in the world.

1. Military- Civil fusion

The China's national defence paper of China, published in 2004, emphasised the role of cyber technologies and informationisation as key factors in enhancing the technology capabilities of the armed forces. The "Science of Military Strategy" published in 2013 holistically addressed the importance of cyber warfare which was finally incorporated in 2015 in the "China's Military Strategy". The said strategy defined cyberspace as a "new pillar of economic and social development, and a new domain of national security. In line with the goals, Chinese Military revised its "Military Strategic Guidelines "and integrated modern technology, ICT and cyber technologies as important element in their plans and strategy laying the foundation of Military – Civil fusion (MCF). It will bring a top down direction for deeper integration, resource sharing and interoperability between civilian and military sectors. The MCF strategy will lead the shift of warfare to intelligence and information driven warfare. The military research and educational institutions have been restructured to synchronise the development of emerging technologies in civil and military institutions with focus on development of dual use technologies. There is no clear line between military and civil economies. The potential areas of focus of MCF include advance robotic, data exploitation, decision support, design and manufacturing of unmanned systems, command, control, communications, computer, intelligence surveillance and reconnaissance, semiconductors for advance computing, weapon design quantum technologies, encryption and decryption capabilities, undersea targeted detection, and advance material. Such technologies are essential in the 21st century to collect, fuse and transmit Big Data for more effective and generate optimal courses of action. China's national projects of artificial intelligence and Quantum Computing, Made in China 2025 and Digital Silk Road etc. are examples of MCF. All the policies and directives in the recent times have been towards achieving success of the MCF strategy.

China today employs full array of capabilities using policy, regulations, foreign direct investments, innovation, bilateral agreements, national industrial giants in key sectors, conduct industrial espionage, a mass dual use military technology, gain leverage in economic deals, restrict trade and pressure foreign governments through strategic investments, recruiting talents, cataloguing foreign innovations, acquisition of companies, technology, acquiring knowledge through exchange programmes, education in US and other key universities in rest of the world etc. It is reported that as of 2019, China had over 4350 front companies' world over to acquire technologies and companies from

America and Western countries. Billions of dollars (of the order of US$15 billion) have been earned by universities in America, Canada, and Europe in licensing technologies to Chinese companies. China's economic, military and cyberspace operations have emerged part of strategy of complex multipronged technology development. China has truly and uniquely embraced and achieved the objective of Military - Civil fusion.

2. Strategy for Development of ICT and Cyber Technologies

China stressed the importance of ICT industry in their 10th and 11th Five Year plans (2001-2010). This period served as blueprint for development of ICT industry in China. The 12th Five Year Plan (2011-2015) stressed on seven major emerging strategic industries which included energy saving and environment protection, new generation ICT technologies, biology, high end equipment manufacturing, new material, and new energy cars. The focus of the new generation ICT was on next generation communication networks, Edge and Cloud computing, Next Generation Internet technologies, Internet of Things, Network convergence (telecom, computer and Cable TV network, Integrated circuits, new generation displays, high end software, large and high end computer servers and information services. The focus of the Plan was thus on creating competence in the area of software. The market and growth of ICT sector of China is at **Annexure I.**

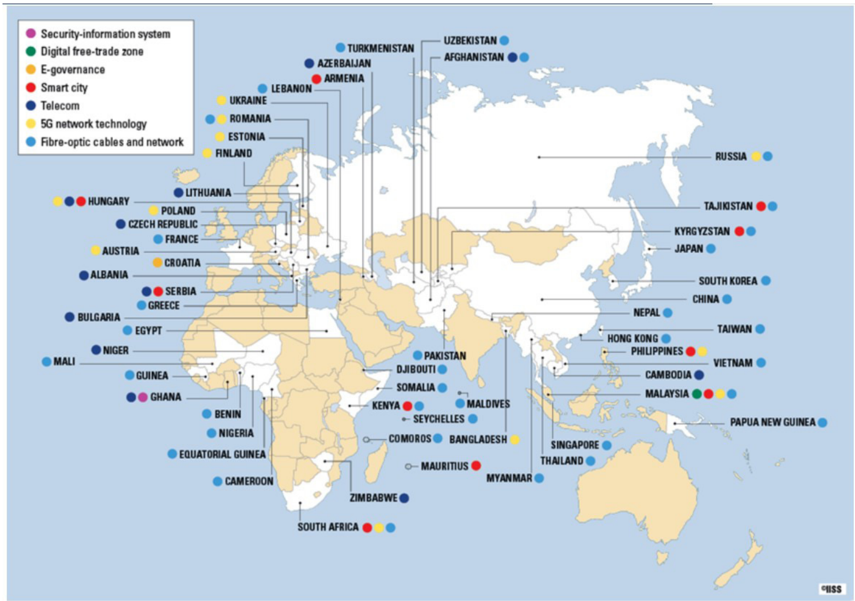
2.1 Made in China, 2025

China in 2015 (though announced in 2013), initiated a programme "Made in China 2025" aiming to transform China into global leader in manufacturing using industrial policy, indigenous innovations, smart manufacturing, local production, controllable standards, and domestic brands. The plan seeks to strengthen China's domestic companies by grant of incentives while increasing pressure on foreign companies to transfer technology for access in market in China. The programme is focussed on indigenising supply; sharpen China's ability to use interdependence as negotiating power so as to reduce risks of dependence on foreign resources. The programme is modelled on Germany's Industries 4.0. In the process, Huawei, ZTE, Baidu, Alibaba and Tencent, Byte dance have emerged as top technology companies of China and are playing geopolitical role worldwide dovetailing China's geopolitical objectives.

2.2 Digital Silk Road

China, announced in 2015, an initiative "Digital Silk Roads" (a digital subset of OBOR, One Belt One Road) to build China centric next generation of digital and telecommunications infrastructure around the world, from telecommunications and city projects throughout Asia and Africa. China had promised to spend about $1tn (BRI and Digital Silk Road) on building infrastructure in mainly developing countries around the world. The spending is much more than invested by any country internationally in a single programme any time. The entire programme has the potential for tremendous benefits to China for future exploitation. It will help China to create alternate and parallel Internet to be controlled by them and globalization of its technology through preferred standards to the benefits of its companies as well as building large repositories of data. The project envisages setting up digital free zones and developing advanced technologies envisaged as part of MCF.

The programme was initially planned to be financed almost all through its own financial institutions namely China Development bank and Export-Import Bank of China, the two State controlled Banks funding overseas investments. The programme, however, has attracted lot of criticism for its weakness including lending to low-income countries with shaky finance and lack of feasibility reports. There are studies and international reports of China silently pulling itself back from funding the project including entire BRI initiative.



China's Digital Silk Road: worldwide ICT infrastructure projects

Sources: IISS; unpublished data from Mercator Institute for China Studies, www.merics.org

2.3 Emerging Technologies

President Xi, in the year 2013, unveiled the ambitious plan to make China a world leader in emerging technologies. It is during this period that China started developing capability in the "next generation communications" by initiating development in 5G communications to be world leader in next generation communication technology. According to report published in Bloomberg, China is planning to ear mark funds to the extent of US$1.4 trillion till 2025 for technology development in the emerging areas ranging from wireless networks to artificial technologies, quantum technologies and great focus on semiconductors. China has already developed and conducted the first quantum secured intercontinental video communications conference. China already has 2000 km secure quantum communication ground line between Beijing and Shanghai and plan to expand the said line across the country. The plans are to have a satellite enabled, global Quantum encrypted communications capability operational by 2030. China is also reportedly building the world's largest quantum research facility slated to open in 2020. China private sector, led by Alibaba, Baidu, Byte Dance Tencent, Huawei and ZTE are driving the development of emerging technologies. These companies have set up innovation centres and funded start-ups across the world. Chinese leadership is currently engaged in laying their economic strategy for the next half decade, including efforts to make critical technologies in China. The programme relating to development of emerging technologies is regularly monitored by the President.

2.4 Artificial Intelligence

China unveiled new initiative in 2017 "New Generation Artificial Intelligence Development Plan" to make China world leader in AI by 2030.The National New Generation of Artificial Intelligence Governance Committee, in June 2019, released eight principles for AI development. These principles are similar to those released by the OECD in May. The major focus of the plan is to develop AI technologies tom support future military capabilities. Companies like Alibaba, Tencent, Baidu, Huawei, Hikvision, Megvii and Yitu, I flytek etc. have been designated as AI champions of China. The designation give these companies lead for setting national technical standards and enable extensive cooperation with the country's national security community. Start-ups like Sense Time, Megvii, Yitu and Deepglint have also raised billions of dollars from USA.

2.5 Semiconductor Development

As a part of "Made in China 2025 China initiated a big programme to be self-sufficient in design and fabrication of semiconductor devices. An amount of US$29.5 was earmarked towards semiconductor programme. A target was set to produce in China, 40 percent of integrated chips for mobile devices, 70 percent of industrial robots and 80 percent of renewable energy products. US- China trade issues, however, have adversely impacted the plan so far. They are able produce only 15 percent of semiconducting chips in China by the year 2019. Many of the high-end chips requiring 40/45nm or lesser technologies are designed in China but fabricated in Taiwan.

2.6 National Crypto Currency

China has proposed first nationally backed crypto currency in the form of a regional stable coin. Hong Kong is the favoured jurisdiction for setting such crypto currency node, given its interconnectedness with the financial system. China together with Russia is setting up a financial messaging system for inter country financial payment transactions to bypass SWIFT. It is proposed to link Russian financial messaging system (SPFS) with the Chinese cross border interbank payment system CIPS. The new system is proposed as a gateway for payment related messages. Russia began development of SPFS in 2014, amid threat from USA to disconnect the country from SWIFT.

2.7 World First Class University and Academic Discipline

The Chinese government, in 2017 had released the *World-Class 2.0* project, replacing the 211 and 985 projects, and aiming to become a global higher education centre to produce top-notch talent in education.

The programme divides the institutions into two streams: 42 universities have been selected to be developed as world-class universities (three more than the number of universities under 985 programme) while 95 universities (including 25 universities which were not under 211 programmes) will be developed as first-class disciplines. With this new strategy, the China Government is concentrating on investment on a smaller number of universities and the selected subjects. The state councils will fund rest of the institutions in the regions.

2.8 The 13th Five Year Plan

The 13th Five Year Plan period is coming to an end and China will be transitioning into its 14th Five Year Plan covering the years from 2021to 2025 and a 10-year long term roadmap through 2035. The 13th Five Year Plan has resulted in bolstering domestic semiconductor design and fab facility, next generation communications and artificial intelligence. This plan has enabled China to scale up their efforts set up efficient supply chain as global centre for OEM. However, US- China trade issues, disputes and sanctions have certainly impacted the plan in the last year of Plan. Meanwhile, digital transformation will enter version 2.0 powered by ubiquitous artificial intelligence and other technologies foundation of which were laid by CCP.

2.9 14th Five Year Plan and Long Term Roadmap Vision 2035

The 14th Five Year Plan approved on 30th October, 2020 by the Communist Party of China, acknowledges that the external environment will continue to be challenging. The Plan will focus on through supply chains, investments, and domestic self-sufficiency. Technological self reliance and competitiveness are at the centre of the new national development strategy. The Plan highlights private sector innovation, talent system reform and industrial modernisation as keys to China to become a global leader. China will also focus on making breakthrough in core technologies like home grown semiconductor technologies in the country including upgrading foundries for semiconductor fabrication strategically emerging technologies like engine technology, precision instruments, robotics and artificial intelligence biotechnology and new energy vehicles. The "technological self-reliance" is the goal of the Plan.

The government has proposed to enact a set of new policies to provide broad support for the so called third generation semiconductors for five years through 2025. The policies include to augment R&D, significant funding directed by state guided investment funds and acquiring companies worldwide etc., apart from other emerging area of technologies including tools and foundries.

2.10 The Long Term Roadmap National Plan called "Vision 2035"

The Vision 2035 has innovation at the heart of China's modernisation drive for achieving a big jump in China's economic, technological and comprehensive national strength. China aims to achieve 'socialist modernisation" by 2035, by which time it also hopes to become a "moderately developed" country, requiring it to triple from its current GDP per capita income of US$10000. China aims to realise critical technological innovation breakthrough by 2035.

2.11 Dual Circulation Policy

Together with 14th Five year Plan and Vision 2035, China, as announced in the meeting of politburo in May, 2020 has also started move to adopt policy called "Dual circulation". The policy places greater emphasis on China's domestic capability and market (internal circulation) and less on commerce with external world (external circulation). It is a structural shift and orientation in the policy in force and represents a change in

China's relation with external world. The objective is to consolidate, absorb and digest the investment already made in the overseas market in the past and some time in future and focus more resources and investment domestically particularly in the emerging technologies to realise the outcome of 14th Five year Plan and implement Vision 2035.

3. Cyber Governance System

China's cyber space operations are part of a complex, multipronged technology development, legal and regulations strategy which is governed by an extensive cyber governance framework. It is articulated on five basic principles namely sovereignty and security of cyber space with state-controlled governance of Internet, Social stability and National Security, system of international rules governing cyberspace, multi-stakeholder approach controlled by State and promote cooperation. The governance system is a complex matrix of interrelated strategies, laws, regulations, and standards. The Governance cover rules for data protection, export regulations, encryption, Media and Internet content, and growth of emerging technologies to emerge as economic and military power of the world. These laws and other measures are essential components of a comprehensive security architecture established by Chinese authorities, encompassing military, political and party propaganda. Many of the laws are in place and few are in the process of being introduced. In all these laws, the principle of double conformity has been followed. On one hand legal framework follow broad features of international practices and confirm to international standards. On the other hand, the Frameworks take in to account China's reality in terms of its development goals and state of its market. A list of rules, laws and principles is listed in the annexure.

Apart from US-China Cyber agreements and recently concluded China EU investment agreement, the four legislations of the complex framework namely National Security Law, Counter terrorism law, Intelligence Law, Cryptographic law, Cyber security law and Export Regulations have far reaching impacts both in the domestic and internationally arenas. China, nevertheless, continues to enact new laws and measures related to Cyber space.

3.1 The National Security Law

The National Security Law enacted in July 2015 requires citizens and organisations to provide national security authorities, public securities authorities, and military authorities with needed support and assistance. This law also declares cyberspace to be part of its national interests and requires "secure and controllable systems thereby providing capability to Chinese Government to control content and dominate discourse in cyberspace as integral to the security.

3.2 Counter Terrorism Law

Counter Terrorism Law enacted in December 2015 expands powers of military and police regarding the potential of the provisions of this law to be used to control religious and ethnic groups. It also allows for conflation of domestic protests and other dissenting activities with international terrorism operations. The law requires all work units and individuals to assist relevant departments in carrying out counter terrorism work and report of suspected terrorist activities or suspected terrorist to relevant organisations or departments efficiently. The law provides powers to PLA to intervene if China's civilian activities abroad are attacked, for example attack on BRI CPEC related work.

3.3 The Intelligence Law

The Intelligence Law enacted in June 2017, allows authorities to monitor and investigate foreign and domestic individuals and organisations to protect national security. Specifically, it allows authorities to use or seize communication devices, buildings and other assets to support intelligence collection efforts.

3.4 Cryptographic Law

Adopted in October 2019 and coming into effect in 2020 requires entities working on cryptography to have management systems in place to ensure sufficient security for their encryption and systems. The law encourages development of commercial encryption technology; however, its use should not harm national security and public good. The law provides for the State Cryptography Administration and its local agencies to have complete access to cryptography systems and data protected by such systems.

3.5 The Cyber Security Law

The Cyber Security Law enacted in June 2017 provides framework for regulating China's network on grounds of national security and for general supervision of the ICT and cyber sector. The law provides security obligations on Internet products and service providers, mandate rules for transmission and sharing of data, usage of Virtual Private Network (VPN), data localisation and cross border flow of Information and Data security. The law also has defined personal identifiable Information which is different than international practices. An important feature of this law is obligations on the part of Network operators to provide technical support and assistance to public security and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law.

3.6 Data Security Law

China has recently (2020) released draft of Data Security law. It is drafted in broad terms and imposes a range of obligations on individuals and entities using data. The law also has broader scope, both in relation to extraterritorial jurisdiction as well as types of data activities. It applies to data activities conducted within as well as outside the territory of China that may harm the national security or public interests of China or the legitimate rights of Chinese individuals or entities. The definition of data extends beyond data that is personal to individuals. Foreign data processing activities (even those that do not involve the data of individuals or entities in China) will be impacted if they could be perceived to harm China's national security or public interests. The law also appears to have broader scope than similar regulations in other jurisdictions, such as European General Data Protection Regulation (GDPR) and the draft of India's Privacy law.

This Law, after its enactment, together with the Network Security law will provide comprehensive legal framework for information and data security in China.

3.7 Multi-level Protection Scheme version 2.0 (MLPS) and Cyber Security Classified Protection Regulations

The law seeks to protect information network from being attacked or damaged. Products which have embedded emerging technologies like Internet of Things. Big data, Cloud computing AI etc are classified into different levels in terms of the criticality to the social order, national security and economic interest of the country. Eight levels have been so far provided but list could be expanded to have more levels. The higher levels represent more criticality in terms usage. Adoption and usage of indigenously designed technologies and products are must for projects above level 3. Mandatory certifications are required to use the products and access Chinese market. The rules also require results of tests so conducted to be verified by the Government through its agencies. The verification by the government will focus on assessing the possibility of risk which may be caused by the cyber products and services, mainly considering the risk of controlling key infrastructure by usage of such product and services. It would include theft, leakage and damage of important data and destruction on the services provided by the critical information infrastructure. The companies would be required to submit requirement documents, purchase agreements and a potential impact of deal on the national security. The new rules affect foreign vendors selling technologies and critical products to Chinese operator. The rules have also been set for Cloud service providers for compliance for providing services to Government and critical information service providers in the country. The rigorous testing is must for such products deployed in critical sectors and operations. The foreign companies are required to take license to sell such products in the country.

3.8 Preferential Market Access

The laws governing public procurement activities, namely Government Procurement Law and Bidding Law have been amended with respect to procurement and bidding of projects and related goods and services in China by the Government funded organisations. The amendments stipulate strict number of requirements to promote the indigenous products and innovation. Incentives have been provided for usage of indigenous product, in general. Trademarks of all new products developed in the country are required to be registered in China.

3.9 Export Control Law

The existing export legal framework and systems have been amended empowering the govt. to effectively safeguard interests related to national security, industrial and economic development. The new list contains large number of items including those of nature of dual use, military, nuclear and other categories. The export of such items license would be allowed after considering trade, industrial competitiveness, international market supply and technological development. The new law empowers the Chinese government to impose embargo by prohibiting export of certain controlled items or prohibiting them from reaching specific destinations, to specific individuals, entities or organisation. The organisations importing items from China will be subject to extra territorial export licensing provisions and controls in relation to the export, re-export of such items exported outside China and re-export of foreign made items that contains Chinese controlled item where latter value exceeds certain percentage of total cost of the finished item. The new law also empowers the government to maintain a blacklist of importers and users who are found violating the rules and regulations governing the export. On 28th August 2020 China updated its export control list by adding 23 items covering artificial intelligence technologies, personalized information services based on data analysis, drones, voice recognition software, handwriting scanning software including other software algorithms and high end technological items. The new rule is not explicitly targeted at any deal; however, it is expected that it may have impact on deals which are in pipeline on account of recent directives of US President. The rules are likely to impact wide range of companies (which include Zoom, Microsoft etc. and those Chinese companies having significant overseas business) across different business sectors. The companies with R&D centres in China may face difficult options. It may be mentioned that companies like Microsoft and Zoom have their

R&D centres in China. Microsoft centre is engaged in the development of AI technologies.

3.10 Anti Trust Law and Anti Monopoly Guidelines

Anti Trust Law and Anti Monopoly Guidelines for the platform economy—China has notified issued rules and guidelines under the Antitrust law, 2008 to stop anti competitive practices in the Internet Sector and Platform economy. The guidelines and rules are aimed at protecting fair competition in the market and safe guarding consumer interest. All the Tech companies like Alibaba, Tencent, Byte Dance, Pinduoduo, Tmall, JD.com etc. acquire lot of companies' world over. All these companies will get cover the antitrust law. The guidelines are said to be part of over plan of Made in China 2025 and Vision 2035.

The guidelines prohibit agreement of the nature of:

- Monopoly
- Hub and spoke
- Abuse of dominant market position and,
- Concentration of Undertakings which include merger, control by acquiring assets and shares and obtaining control or a decisive influence over another company and undertaking by signing contracts or via other means.

The guidelines together with Anti Trust law provide a set of rules for increased scrutiny on internet platforms and flow of foreign capital. Notably, the law has already produced effects on the market. Ant group suspended its planned large public offering and listing on the stock market.

4. Active Cyber Defence and Cyber Warfare

China had, since 1949, as a general principle, adopted policy of "Active Defence". This policy has been tailored, over period of time, in its specifics with changes in geopolitical, technological, and economic scenarios. It is a strategically defensive but operationally offensive. It is rooted in a commitment not to initiate armed conflict, but to respond robustly if an adversary challenges China's national unity, territorial sovereignty, or interests. The policy also applies to defend external interests. According to this concept, China may conduct defensive counterattacks by responding to an attack or striking pre-emptively to disrupt an adversary's preparations to attack. It includes "blinding", "paralysing" and "chaos" methods of defence cum deterrence. As part of this strategy, China use tactics short of armed conflicts to pursue its strategic objectives. Activities are calculated to fall below the threshold of provoking an armed conflict. The PLA interprets active defence to include both de-escalation and seizing the initiative. Active defence is enshrined in the 2015 National Security Law and is included in the PLA's major strategy documents. Time in again this policy has been reaffirmed at all levels be it political and military

The 6 important elements of the said "Active Defence" policy include:

i. Adhere to a position of self-defence and stay ready with counter strike,

ii. Combined strategic defence with operational and tactical defence,

iii. Operational initiative

iv. Explore and try for best possibilities

v. The dialectical unity of restraining war and winning war

vi. Soldiers and people are the source of victory

4.1 Cyber Strategy – "Active Defence"

China characterizes its Cyber Strategy as one of "Active Defence". The concept has been strictly followed while investing in building comprehensive cyber capability both for defensive and offensive striking capability. Active Defence encompasses elements like cyber space situation awareness, cyber defence, support for the endeavours of the country in cyberspace, defending critical information infrastructure and national network, robust internal internet infrastructure, averting any cyber crises and participation in international cyber cooperation.

The strategy, however, encompasses far more areas than the civil and intelligence gathering but envisages comprehensive capability of a country. It includes `militarisation of cyber space, information dominance & campaigns, control content and dominate discourse in cyber space, technological research and development, innovation capabilities, information technology industry, internet infrastructure, security and influence of internet websites, and foreign policy and diplomacy on cyber related matters. China also has often taken a position "Will not attack in cyberspace unless we are attacked; but we will surely counterattack". This important aspect was stated in the "China Military Strategy" in the approach outlined in 2015 by Ministry of National Defence.

5. Stake Holders in Cyber warfare

President Xi Jinping is directly shaping China's cyber policies, but there are also number of stakeholder institutions who are participating and influencing Country's approach to digital economy and cyber warfare at strategy, policy, implementation, and operational level. These are:

i. Politburo Standing Committee (PBSC),

ii. Politburo,

iii. State Councils

iv. Central National Security Commission (CNSC)

v. Central Military Commission (CMC)

vi. Cyber Space Administration of China (CAC)

vii. Ministry of Public Security (MPS)

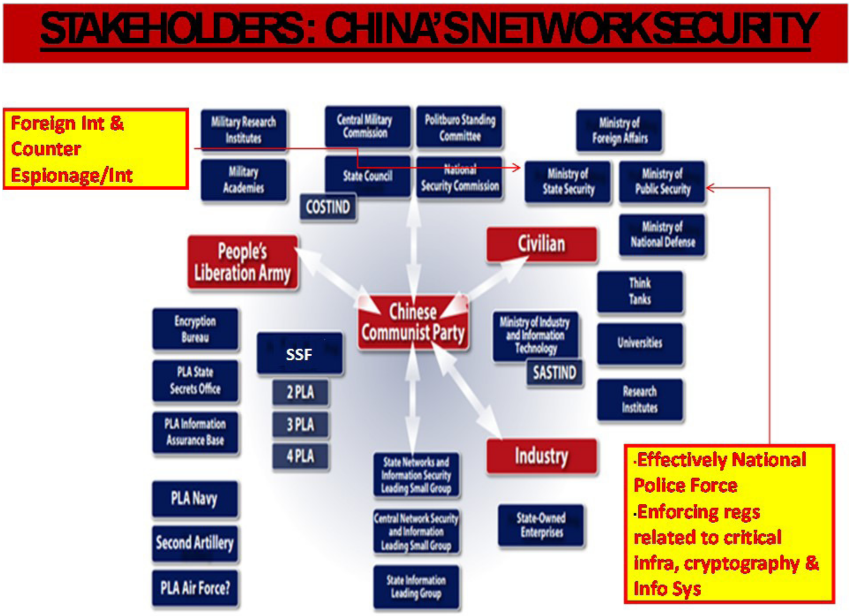
viii. Ministry of State Security (MSS)

ix. People Liberation Army (PLA) and Strategic Support Force (SSF) of PLA

x. Ministry of Industry and Information Technology

xi. Ministry of National Defence and Cyber Space Strategic Intelligence Research Centre

All these stakeholders have different roles which overlap in certain aspects. The three-stake holder namely MSS, CAC and PLA SSF play vital roles at tactical and operational levels in Cyber Operations in China. The operational roles of these organisations are discussed in the following sections.


STAKEHOLDERS: CHINA'S NETWORK SECURITY
Foreign Int & Counter Espionage/Int
Military Research Institutes
Military Academies
Central Military Commission
State Council
COSTIND
Politburo Standing Committee
National Security Commission
Ministry of Foreign Affairs
Ministry of State Security
Ministry of Public Security
Ministry of National Defense
People's Liberation Army
Civilian
Chinese Communist Party
Think Tanks
Universities
Research Institutes
Ministry of Industry and Information Technology
SASTIND
Encryption Bureau
PLA State Secrets Office
PLA Information Assurance Base
SSF
2 PLA
3 PLA
4 PLA
PLA Navy
Second Artillery
PLA Air Force?
State Networks and Information Security Leading Small Group
Central Network Security and Information Leading Small Group
State Information Leading Group
Industry
State-Owned Enterprises
·Effectively National Police Force
·Enforcing regs related to critical infra, cryptography & Info Sys

5.1 Cyber Space Administration of China (CAC)

CAC was set up in 2014 and report to central cyberspace Affairs commission headed by the Communist Party general secretary Xi Jinping. It is also known as the office of the Cyber Space Affair Commissions. It is the Central Internet Regulator and is involved in the formulation and implementation of a policy on variety of issues related to Internet in China. It exercises oversight and censors' content and information, undertakes propaganda relating to ideology on the Internet and gives directive to media companies in China. It also regulates domain usernames on the Chinese internet, virtual private network, Domain Name Servers (DNS), content of internet portals and many more such activities. CAC works with other Regulators in China to formulate a catalogue of key network equipment and specialised network security products for certification. It is also engaged in reviewing the requirement of network products and services for national security consideration as well as security of devices made by the foreign companies in and out of China but for use in China. **Data stored outside of China by Chinese company is also required to undergo approval of CAC**. The organisation has also been reported to be assisting other Chinese agencies and, on its own in many ways, launches cyber-attacks on websites and visitors accessing the Chinese websites.

5.2 Ministry of State Security (MSS)

Ministry of State security is a key operational player in the overall scheme of Cyber warfare. The missions of MSS include; to protect the national security, secure political and social stability; implement state security law and related laws and regulations; protect state secrets; conduct counter intelligence; and investigate organisations or people inside China who carry out or direct, support or aid other people perceived to harm national security. MSS is the key player in the military civil fusion programme of China. They coordinate with military research institutes, military academics and such civilian institutions, industries and think tanks both within and outside the country. It is engaged in economic intelligence, counter intelligence and economic espionage activities in China and internationally to protect economic interests of China. MSS is engaged in acquisition of foreign companies, merger and acquisitions (M&A), economic espionage, conceptualisation and execution of information propaganda and campaign through national and international media either by themselves but mostly covert operations through networks of shell companies both Chinese and non-Chinese located in the respective countries. These shell companies collect data; process and analyse the same in the name of Big Data and IT services in the respective countries. The modus operandi is to outsource the task of data collection, processing, and analysis as export of IT services. The analysis along with certain raw data is passed to Chinese agencies. The overall supervision is performed by MSS with the help of different non state actors, state actors and Chinese companies. It coordinates with companies for acquisition and development of Cyber tools for the purpose of gathering intelligence and surveillance. Over a period, MSS has gained expertise and operates with greater sophistication in its tactics, techniques and procedures and extends their operations covering entire globe. Several of Advance Persistent Groups (APT) like APT 3, APT 10, APT15, APT 20 and APT 27 etc are associated with MSS and operations cover entire globe. MSS has emerged as highly capable institution in cyberspace, demonstrating increasing sophistication and operational security while undertaking a global campaign of cyber espionage for economic, political, and strategic purposes.

5.3 Strategic Support Force (SSF)

The PLA Strategic Support Force (SSF) is a theatre command level organisation established in December 2015 and centralises PLA strategic, space, cyber, electronic, and psychological warfare missions, and capabilities. The SSF was formed from organisations formerly subordinate to PLA services and the General Staff Department (GSD). SSF reports directly to Central Military Commission (CMC) headed by supreme Military Commander & President Xi Jinping and support the entire PLA. It provides other Theatre Commands training and information derived from data collected from their space and cyber operations activities. On a broader architecture, SSF overseas two sub theatre command level departments namely, the Space Systems Department responsible for military space operations, and the Network System Department responsible for information and cyber operations which include electronic warfare, cyber warfare, exploitation and hacking of networks and psychological operations.

They provide intelligence support obtained through their operations to all other Theatre Commands. The creation of SSF highlights the very high priority placed by the PLA, on being able to fight and win future conflicts both in cyber space and outer space domain. SSF has consolidated most of the China's military, space and information warfare capabilities to move towards realising integrated information operations and integrated strategic deterrent. It is still a force in transition and changes may happen to its organisational structure composition and operational thinking.

5.4 Structure of SSF Dedicated to Cyber Operations and Warfare

The Network System Department, SSF have four Technical Reconnaissance Bureau (TRBs) namely, 56th, 57th, 58th and 61th Research Institutes from the former third department generally known as 3PLA of the GSD (now merged with Joint Staff Department) as well as quite large elements of 4PLA (fourth Department) which like 3PLA was earlier entirely with GSD. 4PLA is responsible for electronic countermeasures like jamming and spoofing signals and some type of offensive cyber operations while the 3PLA is primarily responsible for cyber espionage and signal intelligence and cyber operations. It is reported that 61 research Institutes have more than 20 bureaus (these bureaus are also known as units like 2nd (unit 61398), 4th (unit 61419), 8th unit, 12th bureau (unit 61486) etc. These units launch cyber-attacks and monitor communications both within and outside the country. Two more units have come up recently and are known as 61786 and 78020. All these units are stated to be based in Shanghai area. The units are further characterised and grouped by the nature of Advance Persistent Threats (APT) carried out by the group. Each of the group also called, APT Groups, has certain dedicated mission and targeted sector and country. Securities companies worldwide also classify these APT groups such as "Panda", Comment Crew etc. in accordance with nature and signature of their intrusion and backward resolution. Much of the efforts of SSF involve intercepting phone calls, monitoring communications, hacking devices, ex filtrating target data, launching DDOS (distributed denial of service attacks) and ransom ware attacks. SSF have developed capabilities to launch DDOS attacks as high as terabits per seconds. The Research Institutes have developed specialised skill in spear phishing, creating software scripts for exploitation of interfaces and launching zero-day attacks. China today has largest detected zero groups actors (20 groups) in the world. A massive database has been created for different versions of malwares and their variants. All attacks and cyber operations are launched while masking identities. The estimates available in the market indicate that about one lakh trained and skilled professionals in different domains of IT and computers are engaged in cyber operations in SSF. Another important unit of SSF called "The Psychological Warfare Mission" engages in shaping international public narratives, weaken the enemies will, and shape diplomatic and political narratives and advance interests of China through all phases of conflict.

6. Layers of Cyber Operation

The Chinese cyber operations and cyber warfare operates broadly in three tiers which further have several layers. The first tier consists of 3PLA, State-sponsored APT groups and cyber professionals hired from universities, companies, and other non-state actors within and outside China to conduct offensive and defensive cyber operation. The second tier consists of specialists in civilian organisations such as the Ministry of State Security or Ministry of Public Security/ CAC, who are authorised by the military to conduct cyber operations. The third tier consists of external group that are hired or mobilised to conduct cyber operation. These include cyber criminals 'mercenaries' groups and software script writers or sellers on malwares and other infrastructure like ToR (The onion Router) servers and hosting platforms, who, in the need, also work with other tiers. Beneath all the tiers and levels are an estimated five lakhs (5 lakhs) propaganda proponents and other internet users who are members of the Chinese Communist Party and promote their interests on the social and online media in variety of ways and engage in criticising country's enemies. The PLA or SSF does not always fully cover the operating expenses. The cyber criminals are hired who partially funded and are encouraged to earn money from criminal activities relating to theft, Ransomware, financially motivated attacks and selling of data relating to employees directory, intellectual property, marketing strategy, bank accounts, tax ID numbers etc, to government agencies, businesses and companies.

7. Nature and Modes of Cyber Operation

China's cyber operations are undertaken using distinct modus operandi and complex techniques. These include:

i. Scanning and mapping the networks, systems, and supply chain of the organizations by pinging and collecting versions of software's and other details of the configuration and vulnerabilities of the systems are assessed,

ii. Designing implants in the form of software scripts called "Malware" for exploitation of desktops and network devices, industrial control systems and mobile device etc. and collecting credentials and identities of users,

iii. The software scripts could be general purpose, at the initial stage. Based on the information gathered the malware is and customized to the mapped configuration of desktop, network devices etc.

iv. Installing malware in the networks as man in the middle

v. Installing malware as agent to initiate attack

vi. The vulnerabilities in the network and communication systems are exploited and communications are intercepted

vii. Bypassing Crypt Systems by using malware

Techniques used are like social engineering by posting links on social media, spear phishing mails, water holing, use of proxy servers, hosting of web sites to act as a pivot, hiding the malware as back door in computer devices, peripherals like printers USB drives and other computer devices like modems and open source software's and poisoning of Domain Name System (DNS) for diverting the communication traffic, evidences of hosting rogue digital certificates. The appropriate techniques and modus operandi are used depending on the target. Hiding of identity, origin of cyber operations is strictly followed by using VPNs and ToR servers of other countries for deniability.

8. Evolution and Sophistication of Cyber Operations

Pre 2004, Chinese cyber operations were unsophisticated (by today's standards), easy to detect and variety of industries and organizations were used to be randomly targeted. The software scripts were simple and mostly Microsoft products-based applications were used to be targeted. It may be mentioned that China was among the first few countries that signed agreement with Microsoft for sharing of source codes of their software products. The skill initially was largely in creating simple malware like APT1 to exploit Microsoft products. The operations were by and large confined on Government organizations. These malware tools and attacks could be tracked back to organizations sponsoring such operations or even origin of individual actors. The operations were undertaken by both military and civilian organizations. Private companies and students were also used. There were significant overlaps in operational activities among the actors. During the next decade, so called Version2, the operations were gradually expanded to the defense related organizations, M&A entities both within and outside China. The unit 61398 was launched.

Post 2015, after the formation of Strategic Security Force (SSF), the Chinese operations are being conducted in coordinated centralized manner, have become complex and refined with the modified protocols and procedures. The cyber-attacks are now focussed on high priority targets, more professionals and difficult to detect. Over just the last four years the Chinese cyber hackers have gone from relatively solitary players to adopting the same tactics as adopted by the professional cyber hackers. The Chinese non state actors are no longer low skilled hackers trying to penetrate the systems. They have transformed from small local network targeting mostly small businesses and citizens to large well organised groups hacking international organisations the Chinese cyber hacking activity is large and expanding quickly to dark web. Skills have been significantly upgraded in almost all areas of cyber, be it networks, operating software, semiconductors, and communications etc. Massive investment has been made in skilling the manpower at reputed universities in understanding different emerging technological domains to exploit the vulnerabilities. Several APT groups have emerged from among Chinese who have studies abroad. The software codes now are complex. More use is being made of Root Kits. Sophisticated techniques like spear phishing, water holing, installation of web shells (complex software scripts), backdoors, key loggers, man in the middle, bypassing crypto codes and for DNS poisoning and hi-jacking IP traffic have been developed and deployed. The techniques include data ex-filtration via customised encryption algorithms and using several hop points. The use is made of specialised systems known as "trusted window binaries", stolen credential etc. Continuous use of dynamic DNS domains as first level command and control servers is generally made. The first level command and control servers are generally hosted on another Virtual Private Servers (VPS) identified in the respective country of target. Open source tools and other technological protocols called TTPs, are used for intrusion. Home grown Malware are used for intrusion and comprising high value and specific targets. Some of such home grown software tools are listed below: -

i. *PLUGX AKA KORE PLUG (It is shared software tool among the Chinese State sponsored groups)*

ii. *Redleaves, Quasar RAT [apt10]*

iii. *SHIMRAT, HYPERBRO*

iv. *TAIDOOR, GHOST RAT, TIDELPOOL*

v. *BADSIGN, FINDLOCK, PHOTO, SCANBOX, WIDENTON (These are close group software tools used among Chinese threat actor group)*

vi. *BACKBEND, BACKSPACE, CREAMSICLE, FLASHFLOOD, GEMCUTTER, MILKMAID, NETEAGLE, ORANGEADE, SHIPSHAPE and SPACESHIP [APT30]*

vii. *BLACKCOFEE, DEPUTYDOG, HIKIT,*

viii. *Zero day vulnerabilities in Browsers like Internet Explorer (IE), Chrome, Mozilla, Firefox and Microsoft office, Flash Players etc.*

More focus has been on exploitation of systems and networks for collecting strategic intelligence and geopolitical developments which would help China in their program "Made in China 2025". The individual actors were regrouped and assigned to known units in SSF and MSS. Massive use of publicly available malwares have been made after suitable modifications w.r.t targeted entity, sector, and country. Each of the APT tools focuses on such aspects. Different strains of publicly malware have been developed and used. Several Command and control servers, commonly called C2 servers have been set up in different parts of the world.

9. Expansion Depth of Cyber Operations

The potency, depth, and overwhelming expansion of cyber operations of China have outpaced their indigenous development of cyber technologies. The cyber operations are said to be penetrating, wide, complex and deep in different countries across the world. Large numbers of actors are focusing on different aspects and sectors of economy and military. China has consistently expanded their scope of targets as well as range of software tools. The operations are enlarged from simple intrusions to state-sponsored targeted intrusions that often align with country strategic objectives and other initiatives like "Made in China, 2025" and 13th Five Year Plan. China has the largest group of threat actors (detected 70 actors) having capabilities, potential impact and more so with expertise in exploiting zero-day (22 actors) vulnerabilities. Zero days are vulnerabilities, bugs or flaws in software code that can give access to hackers to or access over systems but which have not yet been discovered and fixed by software companies. Zero-day exploits formed a key part of the "Stuxnet" cyber weapon. The Chinese threat actors are known to be using broad range of custom-made tools/non-Public tools and techniques and numerous publicly available remote accesses Trojan in their operations. These tools and malware are basically public and open source malware compiled from GITHUB and deeply and heavily customised for different variants w.r.t sectors and disciplines. Open source and public tools are used generally for exploiting vulnerabilities in public facing Web systems, proxy systems, clouds, content delivery networks etc as such tools are considered to be best for exploiting the vulnerabilities in the open interfaces. The design of home-grown malwares and tools are complex and use mix of assembly and other high level languages, built in FTP and email transmission server, customised encryption, AI and feature for remote control. These malwares are used for special and high-stake targets.

It may be mentioned that the evidences have indicated that by and large Chinese intrusion activities including those related to DDOS (Denial of Service) and ransomware attacks fall under the passive activities like exploiting ICT systems, networks for scanning, data collection, data deletion, stealing or theft of data, espionage, or surveillance. The Chinese has the capabilities to launch precise and simultaneous DDOS attacks in the range of terabits. All the cyber attacks are precise and controlled remotely. The foot prints and evidence are deleted.

Under the UN definition such types of attacks does not qualify as Cyber weapon. A cyber weapon is something that is "deliberately designed to cause damage or destruction". Stuxnet was a cyber weapon which was designed and used for destructive purpose. However, the cyber operations being carried out by China are prelude to the Cyber warfare. It provides them strategic and important information to design and customise the cyber weapon which may be used to cause damage and destruction in military systems and critical information infrastructure. The cyber operations of China are clearly military focussed. China has, thus emerged as power on the world stage and possesses cyber, economic, and military capabilities that augment its overall national power.

10. Strategic Cyber-Attack Actors/ Groups

The Chinese cyber operation groups/actors are identified based on nature of targets, type of operations e.g. nature of espionage, nature of data that need to be stolen from different sectors of economy / education / defence etc. There are, however, many more Chinese sponsored groups that remain undiscovered. Security companies like Fire eye classify these groups by the name of Advance Persistent Threat (APTs) groups while other companies e.g. Crowd Strike designate them “Panda”. Similarly, Kaspersky and MacAfee name the actors by different name. About 70 Chinese cyber groups are detected to be active worldwide. Out of which about 22 groups are specialising on exploiting zero day vulnerabilities in software and hardware. Majority of the cyber groups are in Shanghai, Wuhan and Tianjin. These are mixed up in military, universities and in civilian sectors. A list of lethal Chinese cyber-attack groups is listed under: -

TG 8223/ APT1/ Comment Panda	APT 26/ Hippo Team APT27/ Lucky House
TG 6952/ APT2/ Putter Panda Gh0st RAT	APT40/ Leviathan 2017 APT41
APT3/Gothic panda APT4 APT5, APT6, APT7, APT7, APT8, APT9	Axiom/ Winnti Group TEMP.Trident, TEMP.Overboard TEMP.Trident, TEMP.Hex
APT10/ Net Panda/ Cloud Hopper	Hurricane Panda
APT12/ Numbered Panda	NetTraveler/ Netfile
APT 15/ Vixen Panda/ Mirage	Hellsingh
APT 17	Stone Panda
APT19 / Deep Panda)	Night shade Panda
APT20/ Periscope,	Anchor Panda
APT21, APT22, APT23, APT24, APT25	Overt Spy Hidden Lynn Backdoors likeTrojan Moudoor/Naid Red Echo

Source:1. Reports of Fire Eye, Crowdstrike, Kaspersky and Symante

2. Red colour APTs are deeply active in India

11. Collaboration of Chinese Threat Actors with other Threat Actors worldwide

The securities companies worldwide have detected that Chinese actors are collaborating with non state actors worldwide. The DDOS attacks are launched together and with active collaboration with such non state actors. The evidences, based on the signatures and artifact of malwares and techniques of cyber attacks indicate close contacts and collaborations between actors, both State and Non state, of Pakistan, North Korea, Iran and Russia. New evidence is emerging indicating association of adverse groups from central Africa with non state actors of China. Among all, China, North Korea and Pakistan have been detected to have far more stronger and closer collaboration especially, in advancing regional interest of China. Most of the malwares, at the binary level, and techniques used by Pakistan bears Chinese signatures. The malwares used by North Korea for committing financial frauds and hacking of banks in the South East Asia (India, Bangladesh, Bhutan and Myanmar) and stealing information from sensitive targets are of Chinese origin. The Digital Silk Route and BRI are expected to be fully exploited by China in forging stronger collaboration with adversaries and actors in countries which are part of such projects and initiatives.

12. Future Direction of China's Cyber Warfare and Operations (version 3)

The year 2020 is turning point for technological / global digital transformation, cyber security, and geopolitics in the world. The technological innovations are driving Fourth Industrial revolution towards seamless connectivity and digitization. The next generation communication networks will significantly enhance access to Internet for devices and people. There will be explosion in use of connected devices, ubiquitous and edge computing to virtual augmented reality, artificial intelligence and IoTs. The environment will be more virtual and heterogeneous in almost every aspect of use and development of technology. The role of interfaces will become important. Accessing applications through "APP" will be order of the day. The vulnerabilities of the systems and software will increase significantly. Communication and technology will become weaponries. Geopolitical issues of technology and data are thus bound to assume greater importance. Tech companies will play important role in the emerging geopolitical scenario. With the ongoing geopolitical tensions and trade wars and sanctions as well as failure of significant international or UN level response and repercussions, the cyber operation activities of China will continue to expand and become more complex and aggressive.

All available evidences indicate that China has been preparing itself and is engaged in implementing integrated plan not only to defend them but exploiting vulnerabilities of the new order. The cyber operations of China will embed convergence of technologies like artificial intelligence, machine learning, big data, quantum technologies, crypto, VPN (Virtual Private Network) and ToR (Layered routing) networks for providing a significant edge to their operations. The cyber actors will engage in developing super complex tools to intrude into networks and digital systems while hiding their identities and leaving no trace of the origin. With the usage of emerging technologies, the protocols and procedures followed and used in their operation will also undergo significant revision. The actors will combine existing proven tactics with new techniques to exfiltrate IP (Intellectual property) and data of strategic importance. Use of dark net and dark web will significantly increase. Focus would be more on infiltrating the sensors, IoT devices and IoT networks and diversion of Internet traffic. A new breed of file less malware and vapour worms are emerging and will emerge with worm like properties that allow it to self-propagate through vulnerable systems and avoid detection. There will be higher storage and preprocessing of data, may be at locations outside China. It may be mentioned that in this regard several ICT projects have been initiated by China in no. of third countries in the world. BRI infra will be potential tool in China operations. It will drive Cyber Espionage Activities in the region. China will further strengthen alliances and synergy with state and non-state actors of Iran, Pakistan, North Korea, Russia, and some other countries which are part of BRI. There is likely hood of emergence of new groups along the BRI route.

Several international reports and trend of intrusions suggest that eight sectors will be of major focus by the Chinese actors. These include: i) New energy vehicles; ii) Next generation ICT; iii) Biotechnology; iv) New Materials; v) Aerospace; vi) Robotics; vii) Power equipment and Pharmaceuticals.

13. Strength and Depth of China's Cyber Capabilities

China has consistently expressed that it has a mission to become major cyber, economic, and military power on the world stage. To achieve this ambition, China, over the last two decades, has comprehensively planned and implemented strategies, legal framework, regulations, and policies to promote digital technology as an integral component in all its economic and military activities. At least three Five Year Plans and the one in pipeline have had focussed on achieving capabilities to be leader and self-sufficient in the digital arena. China, for almost decade, focussed on specific programmes and after laying good foundation of infrastructure, policies frameworks and linkages between different organs and agencies of the government, have had initiated integrated programme like "Made in China 2025", "National Artificial Intelligence Plan, 2017", "Semiconductor self-sufficiency", "Thousand talent", "Project World Class education 2.0" and restructuring of Military Commands by setting up Strategic Support Group. These are under different stages of implementation. China has moved rapidly to construct an integrated and comprehensive policy and regulatory framework to address and meet their goals of self-sufficiency, social stability, and national security. These frameworks are more integrated than that of any other country. Most of the frameworks are developed on international pattern but heavily customised to china's need and coordinated by the Communist Party either at the level of Central or State Councils. As a result, China's capabilities have been quickly developed and grown comprehensively in all the disciplines of research and development, manufacturing, skill up gradation and attracting foreign direct investment (FDI). Several Chinese technical giants are operating globally and driving the development of emerging technologies such as 5G communication, AI, quantum computing etc. They have set up innovation centres and funding start-up's worldwide. Chinese companies have expanded into overseas markets offering their products and solutions. It has resulted in increased access to foreign talents, technology, and data. China has invested in or outright purchase of foreign companies that have technologies, facilities and people working in key technology areas. The use of various incentives and strategies has been made to attract foreign experts to work on and manage strategic programmes and fill technology gaps. Overall a good, broader and deep base of infrastructure for research and development, design, manufacturing has been established and developed.

China is able to enhance resiliency of their systems w.r.t cyber-attacks largely by adopting and installing appropriate and layered network architecture, filtering and monitoring IPs accessing web sites and ICT systems in China from overseas. Most of the websites of Ministries, sensitive organisations and critical infrastructure in China are not allowed to be accessed without proper authentication and authorisations at the Internet gateways. The sensitive and strategic organisations and institutions in China use Virtual Private Circuits which are developed indigenously and customised. This is one country which largely useS version 6 of Internet Protocol (IPv6). The CERT and other agencies under Ministry of State Security, Public Security and SSF work closely and in integrated manner.

14. Gaps, Vulnerabilities and Challenges of Technologies

14.1 Digital Silk Road and BRI

A report published by the Boston University in December 2020, indicates that the biggest development programme is drifting in its original funding plan and has the potential to become China's first overseas debt crises. The research study shows that lending by the Chinese financial institutions that drives BRI and Digital Silk Road; along with Bilateral support to Governments has fallen considerably. The lending by the two banks has been reduced from $75bn in 2016 to $4bn in 2019. The two banks fall under the direct control of China's State Council. China is in negotiations with host of countries on the funding aspect of the project. At the same time reference of BRI and Digital Silk Road in the domestic media has come down a lot. The significant reduction in overseas funding and reduced lending by the two key institutions of China is being interpreted as "rethink" by China towards BRI and Digital Silk Road initiative and will have geopolitical issues and will be exploited by the countries having difference of views on this project. It is reported by Media that reduced funding may have resulted in renegotiation of several infrastructural projects, the indication of which is reflected in some of the projects under implementation in Pakistan.

14.2 Semiconductor Technology:

China has acquired technology via imports and transfers from foreign companies. All the ICT and Cyber products have import content ranging between 65 to 82 percent. The estimates available in the market indicate that China may achieve only about 30% of target of having 70% domestic requirement of semiconductors from Chinese sources. China annually imports semiconductors worth over US$ 300 billion. China has only recently started fabricating semiconductor memory circuits and lacks non-memory semiconductor chip fabricating facilities. Different groups and agencies estimate that China will take several years (at least 5 years) to become competitive in the non-memory semiconductor circuits. China has not stabilised and proven capability to fabricate semiconductor wafers and circuits lower than 28NM technology. It is reported that they have set up plant to fabricate semiconductor chips with 40 NM technologies. The pilot production of chip of 40 NM is underway, however, it is yet to be proven and the capacity is limited. Most of the world's leading semiconductor circuits are made by US companies such as Intel, APPLE, AMD, QUALCOMM and Nvidia are of better technology. The semiconductor technology below 10 NM is commonly in use in rest of the world. Given the extremely small and undeveloped base of Chinese semiconductor production and weak technological capabilities, and with increasing difficulty to procure high-end semiconductor equipment and design tools, it will be extremely difficult for China to make strides in becoming self-sufficient for its need of semiconductor circuits within next 5 years, probably not even within next 10 years, if same conditions relating to export restrictions from USA and Western countries prevail as are today. The US export control restrictions have been made applicable on products both hardware and software and tools which are made using US technologies. The impact is now visible on Huawei and ZTE and such companies. The present stock of semiconductors with the leading Chinese equipment companies may last only for the next few months. TSMC, the leading semiconductor manufacturer of Taiwan has already stated that they will not be able to supply semiconductors and semiconductors' wafers to Chinese companies. The research programmes relating development of high end technologies have also been adversely impacted**.**

14.3 Artificial Intelligence

China wants to lead the world when it comes to artificial intelligence. The quality of their Artificial Intelligence algorithms has improved significantly. There are several factors that can dampen the nation's plan to lead in the area of Artificial Intelligence. China is far behind in developing and shaping core technological tools of AI. As of today, it does not have platforms, like the one built by US universities and companies, to design, build and train the sets of algorithms that enable computers to function more like a human brain. It severely lacks fundamentals in development of tools to test and develop AI algorithms. All the virtual systems and operating systems designed worldwide, today, embed AI. China is far behind in making fundamental breakthrough in this direction. It also lacks behind in AI hardware even tools both w.r.t designing and productions that can support advance AI systems. Most of the world's leading AI enabled chips and systems are designed by US companies in USA. It may, however, be mentioned that China has created certain level of skill in designing semiconductor chips of technology better than 22 NM for their 5G communication equipment. Even there, many of the sensitive subsystems like radios and modems are designed and produced by companies like Nokia and Qualcomm. The three core tech companies of China, namely Tencent, Baidu and Alibaba, no doubt, have become big global leaders in the area of AI. Nevertheless, they are still not in the same tier as US companies such as Google, Microsoft, and Apple. Chinese companies are fast coming under scrutiny due to their domestic laws on surveillance. The Chinese companies would also find a challenge particularly in the wake of evolving geo political situation and international practices and regulations, e.g. European General Data Protection Regulations empower the users the right to ask for transparency and disclosure of AI algorithms particularly when such algorithms relate to their lives. It will be very difficult for China to showcase their algorithms. AI technologies promises advances in health care, communications, and smart manufacturing. These technologies coupled with AI enabled semiconductor chips are critical technologies for growth in economy, industry, and national security. The nation that makes fundamental breakthrough in these technologies is likely to shape its future direction and reap the most benefits. Fundamental foundation of such technologies will be essential for China to meet its long-term objective with respect to their ambition of becoming world superpower.

14.4 Security

The National Cyber Power Index published by Belfer Centre of Harvard Kennedy School, USA has ranked five most powerful countries in cyberspace, namely, USA, China, United Kingdom, Russia and Netherlands (in particular order). The National Cyber Power Index is stated to be composite index of two broad factors: capacity and intentions. These factors are further based on several sub parameters –defence, offence, surveillance, control, intelligence, commercial and norms. The report clearly states that the said top five most powerful countries have laid out clearly their objectives and intentions of building comprehensive cyber capabilities to be super cyber power. The global cyber security index, 2018 published by International telecom union (ITU) ranked China at number 27. The cyber security ranking published by a UK-based firm analysed and compared cyber security posture of 76 countries ranking them on a scale of 1to 76. The said report ranked China at 18th position in 2020. It may be mentioned that higher a country's ranking, better is their cyber security posture. China's Internet is also one of the most regularly attacked. China has been witnessing increased cases of cyber incidents, cyber warfare and cyber-attacks, malware/ virus attacks of variety of nature and Denial of Service attacks. The report published by security companies mentioned that China suffered the highest rate of distributed denial of service attacks in the world in 2019. Majority of cyber attacks are of the nature of scanning of the ICT systems, installation of backdoors, and injection of malware through remote log in and telnet software, protocols, ransom ware, denial of service, intrusion to networks using malware and more particularly injection of malware in the financial systems. It is also reported that more than 12 percent of total mobile phones and devices in China are infected with one or the other malware. More than 65% of the attacks were launched by systems located in China itself. However, complex, and sophisticated cyber-attacks from overseas and outside China have shown an increasing trend. Among all the attacks originating from outside China, those that targeted government and financial websites outnumber those on other targets. The nature of cyber incidents reported by the security companies' world over indicates that that China has fairly large number of systems and infrastructure. The other factor of large number of attacks and intrusions from within China is also said to be a part of country's strategy to test various software tools and malware which are made by the Chinese cyber actors for surveillance of their citizens and undertaking cyber operations in other countries. The security companies, world over have also reported that the versions of software and interfaces used in the ICT systems are old and vulnerable. This is true mostly with the professional ICT equipment's. Though China deploys lot of proprietary interfaces, customisation of software from US and Western sources in Chinese language and large numbers of open systems have enhanced weakness and vulnerabilities in the cyber systems, the percentage of which is consistently increasing. China has disadvantages in self-sufficiency in design and production of indigenous cyber security equipment like firewall, intrusion prevention system, web firewalls, operating system software and such other essential security systems. Weakness is also reflected in good Anti-virus and Anti-Bot software both for detection and prevention of cyber attacks and intrusions. China has serious limitations in design of software based cyber security-based systems. Their capabilities are far away in developing and customising AI and Machine learning based software engines used and deployed in perimeter security equipment which secure the ICT and ICT based systems.

15. China's Position on Cyber Security in International Institutions

China's cyber related foreign policy is driven primarily by the domestic political imperatives that protect the country's interest. At the same time China also convey its signal of openness and responsible actor on technology and policy issues by engaging with the international community and participate in all the important bodies in the world namely WTO, UN, International Telecommunications Union (ITU), WHO etc. It also participates and attempts to dominate in the standard making process in bodies like 3GPP, ISO and has started participating in CCRA, a body handling cyber security testing standards. China has started dominating in all such institutions. For example, China played and is playing a very active and dominant role in framing the standard relating to 5G communication and next generation communications, AI norms, e-commerce policies and norms of Behaviour in Cyber Space etc. However, it is apparent that China espouses laws, norms, standards, and policies that allow for sufficient flexibility of interpretation to serve their domestic and strategic interests. Similar example of their approach in meetings of UNGGE is relating to norms of behaviour in cyber space. China has expressed willingness to conform to some norms of behaviour in cyberspace while maintaining their stand of commitment to state sovereignty over ICT related activities and more so on issues related to cyber security. China has now been advocating for adoption of international law in cyberspace revising their earlier stand that the laws of conflicts including armed conflicts do not apply to the cyber realm. China's stand with respect to Article 51 of UN Charter is much different than western countries and US. China is also agreeable to the norms that state must meet the international obligation regarding internationally wrongful acts attributable to them. However, it is generally the view that China's willingness to conform to some norms of behaviour in Cyber Space and not all, are only at face value to avoid further scrutiny by the international organisations and countries. Similar examples are reflected in majority of issues debated in WTO and ITU. Parallel examples of China's behaviour could be seen in other areas of Chinese foreign policies.

16. Global Rules on Data Security

China in an attempt to play lead and aggressive role in data governance unveiled new "Global initiative on Data Security". The stated objective is to safeguard global data and supply chain security, promoting development of the digital economy, and providing a basis for international rules-making in their area.

The initiative involves eight points:

1. First approach data security with an objective and rational attitude, and maintain an open, secure and stable global supply chain.

2. Second, oppose using ICT activities to impair other States' critical infrastructure or steal important data.

3. Third, take actions to prevent and put an end to activities that infringe upon personal information, oppose abusing ICT to conduct mass surveillance against other States or engage in unauthorized collection of personal information of other States.

4. Fourth, ask companies to respect the laws of host countries, desist from coercing domestic companies into storing data generated and obtained overseas in one's own territory.

5. Fifth, respect the sovereignty, jurisdiction and governance of data of other States; avoid taking companies or individuals to provide data located in other States without the latter's permission.

6. Sixth, meet law enforcement needs for overseas data through judicial assistance or other appropriate channels.

7. Seventh, ICT products and services providers should not install backdoors in their products and services to illegally obtain user data.

8. Eighth, ICT companies should not seek illegitimate interests by taking advantage of users' dependence on their products.

9. China has been pushing and taking for these positions at all international talks, but now is formally attempting to aggressively get them into global rules for data security. The most important aspect is cross border retrieval of data for law enforcement.

17. Concerns and Actions for India

It is apparent that ambitions of China are closely linked with their domestic, political, social order, economic growth and military modernisation that help them to emerge as a superpower in the world. China is already attempting to establish its hegemony as regional power. China's cyber operations, accordingly, reflect its priorities and an approach to cyberspace that is much different to the Indian approach. Not only China but also many other countries are observed to be targeting and launching cyber operations that are more aggressive than in the past. India is already facing significant number of cyber-attacks on its critical infrastructure, sensitive organisations, government institutions and diplomatic missions abroad. Several high value target attacks have been launched on the Indian entities not only by China but also in association with countries like Pakistan and North Korea. Large numbers of Chinese Cyber threat actors are active in Indian cyber space, some of which have been mentioned in this report. Significant part of the cyber infrastructure of India has been mapped by Chinese actors and agencies. It is imperative that India must formulate a robust strategy that both significantly prevent and check China and other country's pursuit of deceptive cyber activities to impact India's economic, military, and national security. The Indian strategy must have a dual objective which protects its cyber infrastructure and also to conduct full spectrum military cyber operations in order to enable actions in all domains while ensuring domestic and international business at all times. In any case, India must review and map in detail the Chinese cyber capabilities vis a vis weakness in the Indian systems and preparations so as to understand its cyber infrastructure, drivers, and perspectives which would help to predict the behaviour and actions of Chinese agencies and get ready for it. May be India needs revisiting its cyber apparatus and structures. An integrated approach and blue print are in escapable requirements.

18. Conclusions

China has been planning since 1990, in an integrated and finely crafted manner to emerge as economic, military, and cyber superpower. Each of the policy, programme, and five-year plan, legal frame work and foreign policies had been very carefully planned and implemented to make China a self-sufficient and cyber super power and to protect national security and social stability. The attempt is clearly to establish the country as a global leader in military and technological domain. Integrated efforts are being made to narrow the gap, as much as possible, in all sectors and disciplines including military and cyber including cyber operations and cyber warfare with USA. China's thrust and active focus on use and development of emerging technologies including AI, Big Data and Robotics would drive and reshape technological landscape in China. Much, however, depends on the emerging geopolitical scenario and trade disputes with USA and other countries in Europe and Japan. The landscape would certainly expose the country to much vulnerability which could be exploited. China will use its economic, cyber, and military power to support its political and geopolitical interests. China's will also continue to conduct strategic cyber operations worldwide keeping a high degree of deniability. With such a strategic objective, Chinese are occupying significant positions in all UN agencies. Having succeeded in developing good capabilities in almost every discipline, China has been taking aggressive positions geopolitically more particularly w.r.t USA. Last four years are of significant importance. China's trajectory as super power will have serious implications on the security and stability of all its neighbouring countries more predominantly India.

Annexure I

1. Size of ICT Market

The growth of the digital economy has become integral part of overall economic growth of the country. The size of the digital economy of China is growing at the rate of about 18 percent and is estimated to be around US$ 5 trn and could grow to a level of US$ 16 trn by 2035. It contributes about 35 percent to the national GDP. It is currently ranked as second largest digital economy in the world. As per estimates available from IDC sources, the Chinese ICT market grew around 8 percent in 2019 and is around US$ 3 trillion. The sector contributed about 11.8 percent in the National GDP in 2019. The average growth of the ICT sector during the last year is more than 12%. The ICT market is expected to register a compound annual growth rate of more than 8 percent from 2016 to 2021. China estimate that by 2025, ICT and cyber market will represent around 50 percent of China's GDP. According to IDC report, the growth is faster than that predicted for the global ICT market. The three Chinese digital companies namely Alibaba, Tencent and Baidu have combined annual revenues of more than US$100 billion.

2. Vibrant Start-up system

China has set up vibrant start up eco system. Their share of Unicorns companies in the world, though much smaller than USA, has registered 100 percent increase in 2019. Estimates suggest that China (their digital and Tech companies) participates in more than 15 percent of all venture capital deals world over. US have highest Chinese investment of US$ 174 billion (more than 16 percent of total Chinese foreign investment, followed by Australia, UK, Switzerland and Canada). The focus of all deals is to acquire emerging technologies. The investment in Start-up in India in 2019 was to tune of US$ 4.6 billion. 50 percent of Unicorn start-up companies in India have significant investment from China. More than 20 Chinese companies are actively engaged in investing in India. The focus of venture investment in India is largely in the Fintech sector and to get into technological means to gather citizen data and high-end FINTECH.

IDC has also predicted that the ICT investment market in China would be reaching US $191 billion by 2023. Among 176 countries, China ranked 80th in the ICT development index, while Canada ranked 29th. The consumer readiness of China w.r.t ICT is more than 67 percent. Almost all consumer and citizen related services are available online on mobile phones. More than 60 percent of transfer of money is carried through mobile devices. China has more than 1.60 billion mobile phones. 84% of the mobile phones based on android and 15% are IOS based Apple mobile phones. The Web traffic accordingly is dominated by the android-based applications and is growing consistently. The overall mobile index of the country is 74.3%. China has 885 million internet users and expected to reach billion numbers by 2025. The e-commerce market in China is estimated to be around US dollar 900 billion and has become world's largest e commerce market. Around 80% of the Chinese people have bank accounts. WeChat accounts for more than 75% of the messenger traffic followed by Baidu and Tencent. The share of Skype is consistently reducing and was around 12 percent of total messenger traffic in 2019. Several Japanese companies like Toshiba, NEC and Taiwanese companies have made significant investment in IT hardware in China. The quality of ICT products and services has improved considerably. The provision of carrier services in the Telecommunication industry is by and large dominated by four state run companies including China Telecom, China Mobile, China Unicorn and China DBSAT. The Telecom hardware market is largely dominated by Huawei, ZTE, Datang and players like CISCO, Nokia, and Alcatel.

3. Growth in Demand

The digital transformation in China is entering into 2.0 version fuelled by ubiquitous artificial intelligence, integration of cloud and edge computing, Automatic cars and applications like big data birth and virtual reality. This version of digital transformation will witness four main pillars, namely, customers, skill, critical infrastructure and industry eco system. Market sources estimate that domestic demand would be sustained by liberalization and growth of service sectors like health, education, and smart cities. China estimates that by 2025, more than half of the China's top 500 enterprises will be software producers and more than 90% applications will be cloud native. 50% of the enterprise software codes used in China will be sourced from external sources and there will be 1.5 times as many developers as today. At least 80% of enterprises applications in China will be based on artificial intelligence. More than 50% of the user interface interaction will employ AI enabled speech, natural language processing and AR/VR. China estimates that by 2025, 40% of the China's new enterprise infrastructure deployed will be at the edge rather than corporate data centres. The number of applications at the edge will increase by 700 percent vis a vis 2019. All estimates available in the market reflects that China's and consumer market will have a structural change by the year 2025.

4. Weakness of ICT and Cyber Market

The penetration rates of business hardware, software and IT services are still comparatively low. It is increasingly facing challenges and coming under intense nature of variety of domestic and external pressures. The companies have attained maturity and competition is growing. There is oversupply of items in some sub sectors like electronic panels, printed circuit boards and lithium and other nature of batteries. Surging labour costs have also weakened cost advantage enjoyed by China. According to the World Bank, China's labour costs are twice as high as Vietnam, Philippines, Indonesia, and Thailand. ICT companies are being exposed to high risks due to their narrow range of products portfolio. The capacity to innovate original and independently design IT products is still low proportionate to growth of market and innovations elsewhere in the world.

The ICT market in China is characterized by high reliance on imports of components. More than 85 percent of China imports are of electronic components and sophisticated capital goods needed for surface mounted components. Currently, China's imports of semiconductor devices are to the tune of US$ 300 billion. China currently represents almost 50 percent global semiconductor market. The ongoing trade tensions between US and China will severely affect the ICT growth in China. Additional import tariffs on all Chinese telecom products including displays and printed circuit boards would slow down growth of the ICT sector. Long sanction period will adversely impact maintenance of capital goods deployed in the production lines. Several ICT companies have started shifting and planning to shift their manufacturing activities out of China. The US sanctions, if continued would have a negative impact on the growth of ICT and Cyber technologies in China. Apart from such emerging obstacles, high level of piracy, cyber security and regulatory uncertainty is expected to severely affect growth.

Big opportunities in the area of ICT and cyber are posing real challenges for the foreign companies. The rapidly maturing domestic competition may diminish share of foreign companies in many ICT sub sectors. Moreover, policies are regulated to ensure security also will impact on participation of foreign companies, particularly in the high-end market. Much of the growth of Cyber and ICT sector now depend on policies and plan which are envisaged in the 14th Five Year Plan.

Annexure II

Important Cooperation Programmes of China in the area of Cyber

UN Processes

- The Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (2004, 2009, 2012/2013, 2014/2015, 2016/2017, 2019/2021)

- The Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security

U.S.-China Cyber Bilateral Dialogue

- US China cyber agreement, 2015

- U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues

- U.S.-China Law Enforcement and Cyber security Dialogue

- U.S.-China cooperation in cyber security and cybercrimes.

Australia-China Cyber Agreement

- Australia-China Cyber Policy Dialogue

China-U.K. High-Level Security Dialogue

EU - China Investment Agreement 2020

- EU and China have in principle agreed to enter in to Comprehensive Agreement on Investment. The agreement, inter alia will include investment in the area of cyber, telecom and all aspects of Technology.

- The agreement is pending ratification by the European parliament.

Trilateral Cyber Policy Consultation, Japan, China, South Korea

Russia-China Cooperation in ensuring International Information Security (Sino-Russia Cyber Security Agreement 2015). This is under the umbrella of BRICS

Memorandum of Understanding, China-Laos

China-Japan-Korea CSIRT Annual Meeting for Cyber Security Incident Response (Fifth)

Korea-China Cyber Security Forum

Annexure III

Top Universities for the Engineering and Technology subject area in China

Based on the QS World University Rankings by Subject 2020

China Ranking	**World Ranking**	**Institution**	**Location**
1	9	Tsinghua University	Beijing
2	22	Peking University	Beijing
3	26	Shanghai Jiao Tong University	Shanghai
4	32	Zhejiang University	Hangzhou
5	50	Fudan University	Shanghai
6	67	University of Science and Technology of China	Hefei
7	93	Xi’an Jiaotong University	Xi’an
8	100	Huazhong University of Science and Technology	Wuhan
9	117	Nanjing University	Nanjing
10	119	Harbin Institute of *Technology*	Harbin
11	123	Wuhan University	Wuhan

Annexure IV

US Universities with Significant Chinese Students

1. Cornell University – Ithaca, NY
2. Massachusetts Institute of Technology (MIT)- Cambridge, M
3. University of California- Berkeley
4. Columbia University
5. University of Southern California
6. University of Michigan – Ann Arbor
7. Purdue University
8. University of California- Los Angeles
9. University of Illinois – Urbana – Champaign
10. Princeton University
11. New York University (NYU)
12. John Hopkins University
13. Ohio state University
14. Yale University – New Haven
15. Harvard University
16. University of Notre Dame
17. New York University
18. University of Pennsylvania
19. Vanderbilt University

Annexure V

Significantly Serious Large Scale Chinese Cyber Attacks during 2020

A summary of serious incidents launched by Chinese actors on Government agencies worldwide is listed below. It is only a representative list which is compiled from much exhaustive list published by the Centre of Strategic and International Studies (CSIS), Washington.

October 2020. U.S. government officials revealed that suspected Chinese hackers were behind a series of attacks on entities in Russia, India, Ukraine, Kazakhstan, Kyrgyzstan, and Malaysia.

October 2020. A Chinese group targeted diplomatic entities and NGOs in Africa, Asia, and Europe using advanced malware adapted from code leaked by the Italian hacking tool vendor Hacking Team.

October 2020. A Chinese cyber group targeted government officials and private organizations in South Asia and the Middle East using a combination of methods including zero-day exploits.

October 2020. A previously unknown Chinese cyber espionage group was found to have been stealing documents from government agencies and corporations in Eastern Europe and the Balkans since 2011.

October 2020. The UN shipping agency the International Maritime Organization (IMO) reported that its website and networks had been disrupted by a sophisticated cyber attack from China.

September 2020. American healthcare firm Universal Health Systems sustained a ransom ware attack from China that caused affected hospitals to revert to manual backups, divert ambulances, and Reschedule surgeries.

September 2020. The U.S. Department of Justice indicted five Chinese hackers with ties to Chinese intelligence services for attacks on more than 100 organizations across government, IT, social media, academia, and more.

September 2020. French shipping company CMA CGM SA saw two of its subsidiaries in Asia hit with a ransomware attack from Chinese group that caused significant disruptions to IT networks, though did not affect the moving of cargo.

September 2020. One government organization in the Middle East and one in North Africa were targeted by Chinese agencies with wiper malware that leveraged a ransomware-as-a-service offering that has recently become popular on cybercrime markets.

September 2020. Georgian officials announce that COVID-19 research files at a biomedical research facility in Tiblisi were targeted as part of a cyber espionage campaign from China.

August 2020. A North Korean and Chinese hacking group together targeted 28 UN officials in a spear-phishing campaign, including at least 11 individuals representing six members of the UN Security Council.

August 2020. Hackers for hire suspected of operating on behalf of the Iranian government and Chinese agencies were found to have been working to gain access to sensitive information held by North American and Israeli entities across a range of sectors, including technology, government, defense, and healthcare.

August 2020. New Zealand's stock exchange faced several days of disruptions after a severe distributed denial of service attack was launched by Chinese actors.

August 2020. Taiwan accused Chinese hackers of infiltrating the information systems of at least ten government agencies and 6,000 email accounts to gain access to citizens' personal data and government information.

August 2020. A Chinese cyber espionage group targeted military and financial organizations across Eastern Europe.

August 2020. The Israeli defense ministry announced that it had successfully defended against a cyber attack on Israeli defense manufacturers launched by suspected North Korean and Chinese hacking groups.

August 2020. Seven semiconductor vendors in Taiwan were the victim of a two-year espionage campaign by suspected Chinese state hackers targeting firms' source code, software development kits, and chip designs.

July 2020. Chinese state-sponsored hackers broke into the networks of the Vatican to conduct espionage in the lead-up to negotiations about control over the appointment of bishops and the status of churches in China.

July 2020. Canada, the UK, and the U.S. announced that hackers associated with Russian and Chinese intelligence had attempted to steal information related to COVID-19 vaccine development.

July 2020. The UK announced that it believed Russia and China had attempted to interfere in its 2019 general election by stealing and leaking documents related to the UK-US Free Trade Agreement.

July 2020. Media reports say a 2018 Presidential finding authorized the CIA to conduct cyber operations against Iran, North Korea, Russia, and China. The operations included disruption and public leaking of information.

July 2020. President Trump confirmed that he directly authorized a 2019 operation by US Cyber Command taking the Russian Internet Research Agency offline.

June 2020. Uyghur and Tibetan mobile users were targeted by a mobile malware campaign originating in China that had been ongoing since 2013.

June 2020. A hacking group affiliated with an unknown government was found to have targeted a range of Kurdish individuals in Turkey and Syria at the same time as Turkey launched its offensive into northeastern Syria.

June 2020. The most popular of the tax reporting software platforms China requires foreign companies to download to operate in the country was discovered to contain a backdoor that could allow malicious actors to conduct network reconnaissance or attempt to take remote control of company systems.

June 2020. The Australian Prime Minister announced that an unnamed state actor had been targeting businesses and government agencies in Australia as part of a large-scale cyber attack.

June 2020. In the midst of escalating tensions between China and India over a border dispute in the Galwan Valley, Indian government agencies and banks reported being targeted by DDoS attacks reportedly originating in China.

June 2020. Suspected North Korean and Chinese hackers compromised at least two defence firms in Central Europe by sending false job offers to their employees while posing as representatives from major U.S. defense contractors.

May 2020. Chinese hackers accessed the travel records of nine million customers of UK airline group Easy Jet.

May 2020. Two days before Taiwanese President Tsai Ing-wen was sworn in for her second term in office, the president's office was hacked, and files were leaked to local media outlets purporting to show infighting within the administration. The president's office claimed the leaked documents had been doctored.

May 2020. U.S. officials accused hackers linked to the Chinese government of attempting to steal U.S. research into a corona virus vaccine.

May 2020. Suspected Chinese hackers conducted a phishing campaign to compromise Vietnamese government officials involved in ongoing territorial disputes with China in the South China Sea.

May 2020. Japan's Defense Ministry announced it was investigating a large-scale cyber attack against Mitsubishi Electric that could have compromised details of new state-of-the-art missile designs.

May 2020. A suspected PLA hacking group targeted government-owned companies, foreign affairs ministries, and science and technology ministries across Australia, Indonesia, the Philippines, Vietnam, Thailand, Myanmar, and Brunei.

May 2020. Operations at two Taiwanese petrochemical companies were disrupted by malware attacks. Taiwanese officials speculated that the attacks could have been linked to the upcoming inauguration of Taiwanese President Tsai Ing-wen's second term.

April 2020. U.S. officials reported seeing a surge of attacks by Chinese hackers against healthcare providers, pharmaceutical manufacturers, and the U.S. Department of Health and Human services amidst the COVID-19 pandemic.

April 2020. U.S. officials reported seeing a surge of attacks by Chinese hackers against healthcare providers, pharmaceutical manufacturers, and the U.S. Department of Health and Human services amidst the COVID-19 pandemic.

Annexure VI

What is APT?

APT stands for advanced persistent threat. It became famous following a New York Times exposé detailing a month's long attack campaign in which a Chinese military unit now known as "APT 1" thoroughly penetrated the media organization's networks with a series of spear-phishing emails and a deluge of customized malware samples.

APT is defined in two ways: On the one hand, an advanced persistent threat (APT) refers to a highly precise sort of cyber attack, on the other hand, advanced persistent threat (APT) can also refer to the groups, often state sponsored or well-funded in other ways, that are responsible for launching such precision cyber attacks.

Truly advanced persistent threats are a bit counter-intuitive. When one thinks about most cyber criminals and other spreaders of malware, one thinks that their goal is to infect as many computers / ICT/Internet connected devices as possible with their credential pilfering, botnet building, or other malicious software. The wider the net, the more opportunity for stealing money, computing resources, or whatever it is they're after. APT actors on the other hand are interested in infecting the machines of particular people.

The end-goal of an APT-style attack is to compromise a machine on which there is some sort of valuable information. It would be an obvious success if an attacker managed to load a key logger or install a backdoor onto the machine of the chief executive or information officer of a prominent company, but you've got to wake up pretty early in the morning to trick one of these guys or gals. They're smart. They have security teams and tools looking out for them. In other words, it may just be too hard to hack these enterprising individuals.

So instead of targeting the CEO, APT groups often choose to target some lesser employee, like a copy-writer or graphic designer, who may not have particularly valuable information on his or her machine but is on the same network as machines with valuable data and could potentially be used as a stepping stone toward infecting valuable machines.

In other words, compromise a device of an employee and use his or her email address to spear-phish the CEO.

Even this tactic often proves too difficult as companies continue investing more money on corporate security products and employee education. APT hackers now resort to choosing increasingly obscure targets in an attempt to daisy chain a complicated sequence of infections that eventually yields valuable data. For example, maybe your great uncle is a bigwig at Boeing or you work as an engineer at a highly specialized design firm that develops a certain exhaust component that Boeing uses in one if it's jetliners. APT groups might target you as a starting point that could eventually lead to the compromise that yields secrets. Nearly anyone with an internet connection is a potential target.

References

1. China's Espionage Dynasty by James Scott – Senior Fellow ICIT and Drew Spaniel – Researcher ICIT, Institute for Critical Infrastructure Technology

2. https://www.symantec.com/securityresponse

3. http://threatpost.com

4. http://www.trendmicro.com

5. https://www.fireeye.com

6. http://thehackernews.com

7. http://thediplomat.com

8. http://securelist.com

9. http://go.crowdstrikes.com

10. http://www.darkreading.com

11. Understanding the Chinese Communist's Approach to Cyber-Enabled Economic Warfare, Zack Cooper

12. Wikipedia page of Cyberspace Administration of China

13. Wikipedia page on EU –China investment agreement

14. Annual report of Department of Defence, US Government Military and Security Developments involving the Peoples Republic of China, 2020

15. Market Monitor, Focus of ICT performance and outlook, 2019

16. Report: ICT Markets in China, 2020

17. Reports published on “www.ft.com’

18. http://www.nature

19. IDC release, 2020, China ICT market predictions

20. China’s Cyber Warfare Capabilities- Brigadier Saurabh Tiwari

21. Chapter Five - China’s Cyber Power in a New Era

22. China’s National Defence in New Era, 2019

23. China’s Emerging Cyber Governance System, Centre for Strategic and International Studies

24. Cyber Policy Portal, UNIDIR

25. China’s Cyber security strategy -Amy Chang forwarded by Joseph S. Nye

About the VIVEKANANDA INTERNATIONAL FOUNDATION

The Vivekananda International Foundation is an independent non-partisan institution that conducts research and analysis on domestic and international issues, and offers a platform for dialogue and conflict resolution. Some of India's leading practitioners from the fields of security, military, diplomacy, government, academia and media have come together to generate ideas and stimulate action on national security issues.

The defining feature of VIF lies in its provision of core institutional support which enables the organisation to be flexible in its approach and proactive in changing circumstances, with a long-term focus on India's strategic, developmental and civilisational interests. The VIF aims to channelise fresh insights and decades of experience harnessed from its faculty into fostering actionable ideas for the nation's stakeholders.

Since its inception, VIF has pursued quality research and scholarship and made efforts to highlight issues in governance, and strengthen national security. This is being actualised through numerous activities like seminars, round tables, interactive dialogues, Vimarsh (public discourse), conferences and briefings. The publications of VIF form lasting deliverables of VIF's aspiration to impact on the prevailing discourse on issues concerning India's national interest.

VIVEKANANDA INTERNATIONAL FOUNDATION
3, San Martin Marg, Chanakyapuri, New Delhi – 110021
Phone: +91-11-24121764, 24106698
Email: info@vifindia.org,
Website: https://www.vifindia.org
Follow us on twitter@vifindia