Vivekananda International Foundation

VIF BRIEF | JULY 2022

CHINA'S CYBER ESPIONAGE OPERATIONS

MAJ GEN PK MALLICK, VSM(RETD)

© Vivekananda International Foundation

Published in 2022 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

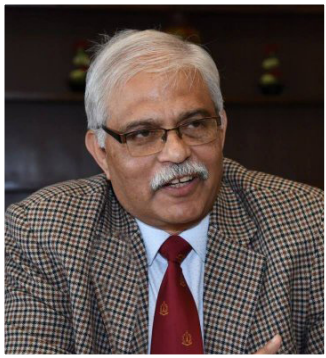
Follow us on

Twitter | @vifindia
Facebook | /vifindia

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 The author certifies that the article/paper is original in content, unpublished and it has not been submitted for publication/web upload elsewhere, and that the facts and figures quoted are duly referenced, as needed, and are believed to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

All Rights Reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form, or by any means electronic, mechanical, photocopying, recording or otherwise without the prior permission of the publisher.



An Electronics and Telecommunication Engineering graduate from BE College, Shibpore, M Tech from IIT, Kharagpur and M. Phil from Madras University Major General P K Mallick, VSM (Retd) was commissioned in the Corps of Signals of Indian Army. The officer has interest in Cyber Warfare, Electronic Warfare, SIGINT and Technology. His last posting before retirement was Senior Directing Staff (Army) at National Defence College, New Delhi. He runs a popular website on national security issues @ https://www.strategicstudyindia.com.

China's Cyber Espionage Operations

"There are two kinds of big companies in the United States; there are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese."

- Former FBI Director James Comey

Introduction

In the Annual Threat Assessment of the U.S. Intelligence Community published on February 7, 2022, it is stated that "We assess that China presents the broadest, most active and persistent cyber-espionage threat to U.S. Government and private sector networks. China's cyber-espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack or influence operations." *FBI Director Chris Wray stated on February 1, 2022 that there was no country that presents a broader threat than China*.

The Chinese government causes damage across a range of industries. Chinese hackers have stolen more personal and corporate data than every other nation

combined. Their toolbox contains everything from traditional intelligence officers targeting private industries' innovations and trade secrets, co- optees not in official pay rolls but tasked by Chinese government to help steal secrets, sophisticated cyber intrusions, shell game transactions, pressure on U.S companies operating in China, joint ventures and partnerships, etc. However, during a meeting with President Barak Obama, China's Chairman Xi Jinping stated, "China is strongly opposed to the theft of trade secrets and all type of cyber attacks."

At the other end, U.S.' hacking activities are well known. WikiLeaks published 9,000 documents in the Vault7 leaks in 2017 detailing many of the CIA's tools. A year earlier, the mysterious 'Shadow Brokers' hacking group leaked many exploits and new zero-days that others have used repeatedly in some of the most significant cyberattacks. Since the beginning of 2022, China has made a strategic change. Foreign Ministry and the country's cybersecurity firms have increasingly been calling out alleged U.S. cyberespionage. Some of them are:-

- Chinese security company Pangu Lab On February 23, published that the U.S. National Security Agency's elite Equation Group hackers used a backdoor, dubbed Bvp47, to monitor 45 countries.[1]

- The Global Times, on March 14, ran an exclusive story about anotherNSA tool, NOPEN, based on details from China's National Computer Virus Emergency Response Center.[2]

- Chinese cybersecurity firm Qihoo 360, a week later, allegedthat U.S. hackers had been attacking Chinese companies and organisations.[3]

- The Global Times, on April 19, reported about HIVE, a malware developed by the CIA.

Wang Wenbin, China's Foreign Ministry spokesperson said in April 2022, "China is gravely concerned over the irresponsible malicious cyber activities of the U.S. government. We urge the U.S. side to explain itself and immediately

stop such malicious activities."[4] He emphasised, "As we can see from exposed operations such as 'Dirtbox', 'PRISM', 'Irritant Horn' and 'Telescreen', the U.S. doesn't even spare its allies and partners in its global cyber-surveillance and attacks." Liu Pengyu, a spokesperson for the Chinese Embassy in the U.S. in a statement said, "We oppose and crackdown in accordance with law all forms of cyber espionage and attacks. Recently, there have been many reports of U.S. carrying out cybertheft and attacks on China and the whole world. The U.S. should reflect on itself and join others to jointly safeguard peace and security in cyberspace with a responsible attitude."[5]

Coming back to the Chinese, it carries out cyber warfare and cyber espionage for political reasons. They perform it not for money or religion but to cause havoc in important national services or try to steal information for intelligence. The aim is to find weaknesses to cripple their adversaries.

Why Cyber Espionage?

There has been a significant shift in China's approach to Computer Network Operations (CNO) since the early 2000s. It found CNO was extremely useful to bridge gaps in niche technology areas and quickly gain parity with advanced countries like the U.S. This would enable China to gain technology which would not be possible without years of research and development and spending billions of dollars. That CNO could also be used as a modernised extension of its economic espionage campaigns would change China's intelligence collection methods.

For a long time, Chinese espionage activities are targeted at defence capabilities, diplomatic, economic and defence industrial base sectors that support U.S. national defence programs and other national security secrets and economic espionage activities. China is particularly interested in space, infrastructure, energy, nuclear power, technology firms, clean energy, biotechnology and healthcare.[6] China's foreign science and technology collection efforts against the U.S. and most western countries correlate closely to the priority

technologies identified in government strategic planning documents: 'Made in China 2025', 'Space Science and Technology in China', the 'National Key Technologies R&D Program', 'A Roadmap to 2050' and the '13th Five Year Plan'. These cyber-espionage operations are part of a sophisticated, long-term campaign to get inside targeted networks. Once intruders are inside the network, they can exfiltrate information, manipulate data, and implant stay-behind devices or software for future generations' action.

Not only Chinese hackers have been carrying out traditional state espionage, they were also busy stealing intellectual property from every major company in the Fortune 500 American research laboratories and think tanks. Chinese hackers have also been stealing trade secrets from innovators, mainly from the U.S. By some estimates, they were passing trillions of dollars worth of American research and development to China's state-owned enterprises. Chinese hackers had taken everything from the designs of the next F-35 fighter jet to the Google code, the U.S. smart grid, and Coca-Cola and Benjamin Moore paint formulas.

Espionage Targets, Objectives and Agencies

Primary targets of China's foreign intelligence collection are the Western and Japanese commercial and military technologies, and trade secrets. The main targets for China's espionage efforts are commercial businesses, research institutes and universities.

The Economic and Technical Domain

One of Chinese espionage activities aims to strengthen China's economic effectiveness and strategic position. China is assessed to be responsible for 50 to 80 per cent of cross-border intellectual property theft worldwide and over 90 per cent of cyber-enabled economic espionage in the U.S. The U.S.-China Economic and Security Review Commission has concluded that Chinese

espionage "comprises the single greatest threat to U.S. technology." Espionage helps China save on research and development expenses while catching up in several critical industries. China does this to "erode the United States' long-term position as a world leader in science and technology innovation and competitiveness." China is reverse engineering many of the U.S. military's technical and industrial advantages.

China has concentrated cyber industrial espionage at high-technology and advanced manufacturing companies in the United States, Europe, Japan and Southeast Asia. Hackers have targeted the firms' negotiation strategies and financial information in the energy, banking, law and pharmaceutical sectors.

In the Five Year Plan for 2011-15, China identified seven priority industries to develop. These industries are:

- New Energy (nuclear, wind, solar power, Turbines, Hybrid/electric cars).
- Energy Conservation and Environmental Protection (energy reduction targets).
- Biotechnology (drugs and medical devices, Biomanufacturing, Biopharmaceuticals, Genetically modified organisms, Infectious disease treatment, Cutting-edge vaccines and drugs).
- New Materials (rare earths and high-end semiconductors).
- New Information Technologies (I.T) - broadband networks, Internet security infrastructure, network convergence.
- High-End Equipment Manufacturing (aerospace and telecom equipment, Chemical Manufacturing, Advanced robotics, High-performance composite materials, Integrated circuit manufacturing equipment and assembly technology).

- Defence (Aerospace & Aeronautical Systems, Armaments, Marine Systems, Radar, Optics, Space infrastructure and Exploration Technology).

Not surprisingly, the U.S. has been an innovator and leader in these very industries. Most of China's industrial espionage involves these industries.

China's Collection Objectives

Clean Energy	Biotech	Aerospace & Ocean Engg	Information Technology	Manufacture
Clean Coal Tech	Agriculture Tech	Deep Sea Explo-ration	Artificial Intelli-gence	Robotics
Low Carbon Tech Production	Brain Science	Space Navigation Tech	Cloud Tech	Additive Manu-facturing
Energy Storage Systems	Genomics	Next Generation Aviation Equip-ment	Information Security	Advanced (nano) Manufacturing
Hydro Turbine Tech	Precision Med-icine	Satellite Technology	IoT Infrastructure	New Materials
New Energy Vehicle	Genetically Modified Seeds	Proximity Ops Tech	Semi-conductor Tech	Smart (A.I.) Manufact-uring
Nuclear Tech	Regenera -tive Medicine	Arctic Tech	Quantum Com-puting	Green Manu-fac-turing
Smart Grid Tech	Synthetic Biology	Precision Optics	Telecoms	
Power Tech	Pharma Tech	Heavy Launch Vehicle Tech	5G Technology	

At the end of the day, foreign technology is converted into products and weapons in China at 'Pioneering Parks for Overseas Chinese Scholars', 'Innovation Service Centers', 'National Technology Model Transfer Organizations', and an unknown number of 'technology business incubators'. These large, sophisticated facilities are located strategically to ensure wide distribution of the foreign technologies obtained informally.

China's Cyber Espionage in Military Domain

PLA cyber forces want to build an operational picture of U.S. defence networks, military disposition, logistics and associated military capabilities that could be used before or during a conflict to deter, delay, disrupt and degrade U.S. operations. The skill sets and accesses required for these intrusions are similar to those necessary to conduct cyber operations. Chinese hackers have pilfered information from more than two dozen U.S. Defence Department programs, including the the F-35 and MIM-104 Patriot surface-to-air missile system. They have targeted more than 24 universities in the United States, Canada and Southeast Asia to pinch research about maritime technologies being developed for military use.[7]

As per their military doctrine, China wants to prevent the U.S's ability to mobilise for war. Chinese hackers broke through a large number of the civilian organisations and contractors who work for the U.S. military's Transportation Command, which is responsible for the movements of men and materials in position for battle. Chinese hackers want to know about the technology of the U.S. armed forces and its operational plans. Hacking efforts were concentrated against Pacific Command, which would be directly involved in any war with China.

For PLA, Command-and-control targets are principally attractive. A RAND Corporation report concludes, "Perhaps no U.S. military vulnerability is as important, in Chinese eyes, as its heavy reliance on its information network. Successfully attacking that system will affect U.S. combat capabilities much more profoundly than would directly targeting combat platforms. Chinese strategists also believe that the U.S. military information network is not just vulnerable but also fragile. Thus, the foundation of the U.S. military's success can also be its undoing."[8]

The Washington Post reported that Chinese hackers pilfered critical missile defence information, including "the advanced Patriot missile system, … an Army system for shooting down ballistic missiles, … and the Navy's Aegis

ballistic missile defense system." The hackers also gathered information on planes, helicopters and ships, including "the F/A-18 fighter jet, the V-22 Osprey, the Black Hawk helicopter and the Navy's new Littoral Combat Ship, which is designed to patrol waters close to shore." These were the very weapons on which the U.S would depend in a conflict with China. China can now study the vulnerabilities of these types of equipment.[9]

Activities of Su Bin, a businessman from Canada, can be an interesting case study of Chinese espionage activities. Su Bin's task was to track American military aerospace developments. He used his industry, aviation, and English knowledge to channel the Chinese hackers toward the most critical targets. One of his targets was Boeing's giant cargo plane, C-17, which the U.S. Air Force uses extensively in different missions. John Carlin, the senior Justice Department official, wrote that "thanks to Su Bin, the Chinese were able to develop, build, and deploy their own copy, in barely a third of the time it had taken the United States to design, test, and build the original C-17." At an air show in November 2014, PLAAF kept its C-17 clone, the Xi'an Y-20, right next to the original U.S. It was a spectacular visual symbol of what hacking can do.

Su Bin and his hacker colleagues also targeted other advanced aircrafts in the U.S arsenal like the F-22, a fighter jet optimised for air-to-air dogfighting and the F-35, the Joint Strike Fighter that was the most expensive aeroplane project in history. China was closing the technological gap. The total cost of the team's effort was only one million dollars compared to the multibillion-dollar price tags of these systems.

China's Demonstrated Cyber Espionage Activities

China has targeted foreign ministries, embassies and important government offices in India, Taiwan, Germany, Indonesia, Romania, South Korea and other countries. Journalists and Tibetan and Uighur activists are tracked. Chinese hackers broke into telecommunications operators in Turkey,

Kazakhstan, India, Thailand, and Malaysia to follow Uighurs travelling in Central and Southeast Asia.[10]

The Center for Strategic and International Studies (CSIS), In July 2021, published a report on the patterns of operation and espionage methods of Chinese intelligence in the U.S. This report refers to about 160 espionage incidents between 2000 and 2021, whose details were made public. The report highlights a significant rise in espionage activity example of which are listed below.

2005-2010. CNE campaigns increase exponentially in ShadyRat, GhostNet, HiddenLynx, Aurora, etc.

GhostNet. China has been conducting cyber espionage operations against India for a long time. One of the earlier examples was the GhostNet episode. The Information Warfare Monitor, between June 2008 and March 2009, conducted an investigation focused on allegations of Chinese cyber espionage against the Tibetan community. GhostNet penetrated computer systems containing sensitive and secret information at the private offices of the Dalai Lama and other Tibetan targets. GhostNet infected 1,295 computers in 103 countries.

Titan Rain. Chinese cyber-enabled espionage gained prominence with the Titan Rain series of cyber incidents, beginning in the early 2000s. Chinese actors accessed unclassified information across many organisations, including DoD, Department of State, NASA, DHS, Department of Energy, Department of Commerce, Army Information Engineering Command, Defense Information Systems Agency, U.S. Army Space and Strategic Command, Army Aviation and Missile Command, and defence contractors, as well as the United Kingdom's Ministry of Defence, Foreign Office, and House of Commons. The full scale of Titan Rain has not been disclosed. However, in 2006, Air Force Maj Gen William Lord acknowledged that 10 to 20 terabytes of data were stolen from DoD's Non classified Internet Protocol Router Network (NIPRNet). The actors appeared to be interested in learning

more about U.S. military strategy and doctrine. China denied responsibility, calling the private accusations "totally groundless, irresponsible and unworthy of refute."

Operation Aurora. The spear-phishing and drive-by download effort, Operation Aurora, became public in 2010. Operation Aurora targeted thirty-four major companies, including Google, Microsoft, Juniper and other firms. The hackers had the following objectives for Operation Aurora:-

- Spy on Chinese dissidents. Google wrote that "we have evidence to suggest that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists."

- Undermine the home-field advantage that hugely benefited the U.S. They wanted to find out which targets in China the United States was observing through Google's systems. With access to the legal-discovery system, the Chinese could see a list that former top Justice Department official John Carlin described as a "who's who" of the spies, hackers, and criminals known to the United States. China could see if the U.S. was using American technology companies to watch the activities of alleged Chinese intelligence officers.

- Access to those companies' secrets, beginning with their source code, is a valuable form of intellectual property. It is easier to find software vulnerabilities and write software exploits to take advantage of them. Discovering and exploiting software vulnerabilities is critical for cyber operations.

- Obtain signing certificates which are cryptographically complex markers that authenticate that a particular piece of code came from a known source like Google and can be trusted.

In 2013, Mandiant, a U.S. cyber security company, published a detailed report pinpointing a Chinese military unit's cyber-espionage involvement.[11]

Theft of Personel Data. In the Office of Personnel Management (OPM) data breach https://www.tandfonline.com/eprint/97VQ9GTNYRM3HCBXGUMK%20/full?target=10.1080%2F01402390.2020.1732354&%3E in 2014, Chinese hackers stole almost 22 million records of government employees. Stolen data included names, places of birth, dates, security background checks, data on intelligence and military personnel and 5.6 million employees' fingerprint data. The hackers accessed Standard Form 86, which includes records of drug use, alcohol addiction and financial problems. This data could be combined with medical data stolen from Anthem Insurance, travels documents from United Airlines and hotel reservation data from Marriott International to create a complete picture of U.S. personnel and their movement.[12] Michael Hayden, former CIA Director, stated that the exfiltrated OPM data remain "a treasure trove of information that is available to the Chinese until the people represented by the information age off. There's no fixing it. I don't blame the Chinese for this at all. If I [as head of the NSA] could have done it, I would have done it in a heartbeat. Former National Intelligence Director James Clapper "expressed grudging admiration for the OPM hack, saying U.S. spy agencies would do the same against other governments."

Theft of Private Data. In 2017, people from the PLA's 54th Research Institute hacked into the protected computers of Equifax and took the names, birth dates and social security numbers of approximately 145 million American citizens. The hackers obtained credit card numbers and other personally identifiable information belonging to about 200,000 American consumers. The PLA obtained sensitive identifying information for nearly half of all American citizensin a single breach.

Microsoft Exchange. On March 3, 2021, Microsoft's email and calendar service "Exchange" was hacked. The perpetrators were identified as the hacker group "Hafnium", with known Chinese government connections. It gave the perpetrators access to millions of emails. Over 60,000 organisations were affected.

Espionage Operations against Other Countries

United States, England, France, Taiwan, etc., have all been targets of cyber-attacks by China.

France. China penetrated France's external intelligence service, the French General Directorate for External Security (French: Directoire Générale de la Sécurité Extérieure, DGSE). In 2020, two former DGSE officers (and the spouse of one) were convicted in Paris for providing intelligence to China for more than ten years. They would have provided China with access to some DGSE intelligence from partner countries.

Taiwan. On August 19, 2020, it was found that Chinese hacking groups had infiltrated several of Taiwan's government agencies and tech companies. They had stolen emails from over 6,000 people. It was committed by the group "Blacktech" and used the malware 'Taidoor', both of which are connected to the Chinese government. China has used Taiwan as a testbed for information and cyber attacks.

Cyber Espionage Against Russia During the ongoing Ukraine War. Espionage is a dirty game. The close relations between China and Russia have not prevented China from carrying out espionage operations against Russia. Recently, Check Point Research (CPR) observed that a campaign, part of an extensive Chinese espionage operation, has been continuing against Russian-related entities for several months.

Civilian sectors attacked	Companies and targets attacked
Technology Industries	Motorola, EMC, Google, Yahoo, Sun Microsystems, SiRF 3D-
Energy	GEO, Exxon Mobil
Automotive and paint industry	Ford, Dupont, General Motors, Metaldyne, Vaispar
Academia and Research Institutes	MIT, University of California, Oak Ridge National Laboratory
Aviation	United Airlines, Civil Reserve Air Fleet, GE Aviation
Medicine and health	NIH, GlaxoSmithKline, Ventria Bioscience, G.E. Healthcare

Civilian sectors attacked	Companies and targets attacked
Software and communications	T-Mobile, Lucent, L3, Avago Technologies, Analog Devices
Cyber	RSA Security
Journalism	WSI, WP, NYT
Capital	Moody's Analytics
Food	Coca Cola
Tourism	Mariott
Agriculture	Orbit Irrigation, Dow AgroScience
Public figures	Office of Sen. Bill Nelson, Sen. Dianne Feinstein

The key findings are:- [13]

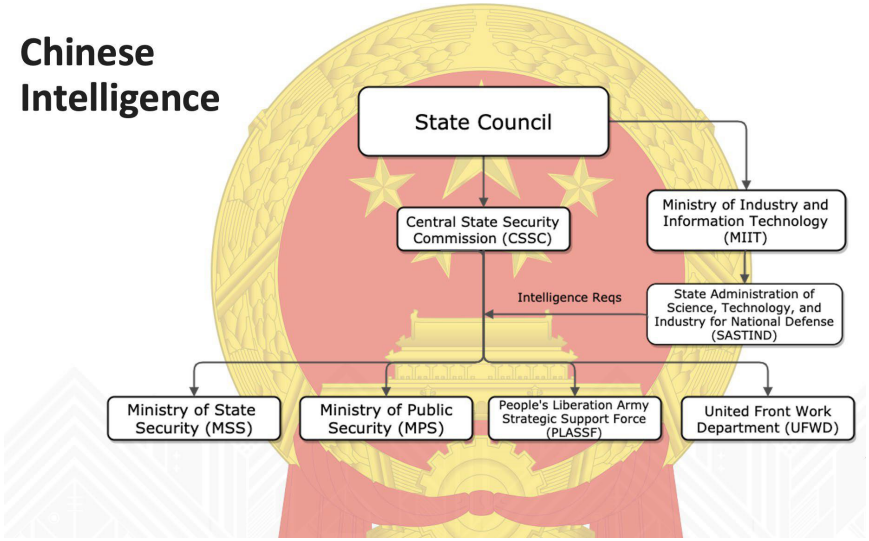
- A targeted campaign against at least two Russian research institutes which is part of the Rostec corporation, a state-owned defence conglomerate.
- This campaign is a continuation of a long-running espionage operation against Russian-related entities since at least July 2021. The most recent activity was observed in April 2022.
- This activity was attributed to a sophisticated and experienced Chinese threat actor, with possible connections to Stone Panda and Mustang Panda, another proficient China-based cyberespionage group.
- The hackers use new tools, which have not been observed in the past.

China's Organisations for Cyber Espionage

Ministry of State Security (MSS).

China's Ministry of State Security (MSS) is the preeminent civilian intelligence agency. The MSS came into being in June 1983 by combining the espionage,

counterintelligence, and security functions of the Ministry of Public Security and the Investigations Department of the Chinese Communist Party Central Committee.



(Source: Adam Kozy, Testimony before the U.S.-China Economic and Security Review Commission Hearing on "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States", February 17, 2022)

In 1983, a new MSS came into being. The MSS combined the external collection functions with the counterintelligence and counterespionage functions of the Ministry of Public Security (MPS), which became public order and police organisation. The MSS served as both an internal security service and a foreign collection organisation. But its primary focus is on gathering foreign intelligence. The overall organisation chart showing where the MSS derives its authority and intelligence requirements from is given below.[14]

The MSS draws its authority from the CCP's State Council and legislation in 2014 and 2015, including China's National Intelligence Law which made it clear that all Chinese citizens and companies operating in China or Chinese companies abroad must collaborate with the MSS in gathering intelligence. All Chinese government departments are obliged to support their intelligence

operations when required. This enables the MSS to leverage foreign affairs departments, government-sponsored overseas educational programs, military liaison programs, universities, think tanks, etc., for operational cover and use them as recruitment platforms. This policy also grants the MSS access to many foreign government officials, academics, scientists and students.

State Administration for Science, Technology and Industry for National Defense (SASTIND)

Other government elements that collect intelligence and technology include the PLA Political Department Liaison Office, United Front Work Department (UFWD) and many universities under the State Administration for Science, Technology and Industry for National Defense (SASTIND). There are two departments under SASTIND responsible for developing and tasking technology-related intelligence requirements and for collecting intelligence against those requirements:-

- **Comprehensive Planning Department** tasks collection to the MSS and the PLA Joint Intelligence Bureau.
- **International Cooperation Department** has its own independent collection capability. Members of this department travel with Chinese scientists to collect information against particular requirements.

SASTIND has direct control over seven universities and contracts for defence research with 55 additional universities. The seven universities are called the Seven Sons of National Defence, and several of them have been identified in U.S. court for actively conducting espionage. Most of these universities have high-security research facilities to support classified technology development for the PLA. These seven universities are:-

- Beijing Institute of Technology.
- Beijing University of Aeronautics and Astronautics.

- Harbin Engineering University.
- Harbin Institute of Technology.
- Northwestern Polytechnical University.
- Nanjing Aeronautics and Astronautics University.
- Nanjing University of Science and Technology.

Some of the organisations actively involved in cyber espionage operations are given below.

Industry Names (CrowdStrike, Mandiant, Microsoft, Other)	**Affiliation**	**Unit/Location**
COMMENT PANDA APT1 FLUORINE	Former 3PLA 1st Bureau	Unit 61398 - Shanghai
PUTTER PANDA APT2 SULFUR	Former 3PLA 12th Bureau	Unit 61486 - Shanghai
OVERRIDE PANDA APT30 Naikon	Former PLA Chengdu 2nd TRB	Unit 78020 - Kunming
GOTHIC PANDA APT3 BORON UPS, Buckeye	MSS Contractors (Boyusec)	Guangzhou, Guangdong
TURBINE PANDA APT 26 TECHNETIUM Bronze Express	MSS Contractors	Nanjing, Jiangsu
STONE PANDA APT10 POTASSIUM CloudHopper, MenuPass	MSS Contractors (Huaying Haitai, Laoying Baichen)	Tianjin
AURORA PANDA APT17 HELIUM HiddenLynx, Sportsfan, DeputyDog	MSS Contractors (Real SOI, etc.)	Jinan, Shandong
KRYPTONITE PANDA APT40 GADOLINIUM Bronze Mohawk	MSS Contractors (Hainan Xiandun Technology)	Haikou, Hainan
WICKED PANDA APT41 BARIUM	MSS Contractors (Chengdu 404)	Chengdu, Sichuan

(Source: Adam Kozy, Testimony before the U.S.-China Economic and Security Review Commission Hearing on "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States", February 17, 2022.)

PLA's Cyber Espionage

The PLA collaborates with various institutions within China's civilian sector and has raised several 'cyber militias' that are called upon to perform cyber-espionage activities. These organisations are made from academic institutions, telecommunications companies, municipal governments and volunteers within China. China's telecommunications firms play a major role in strengthening China's activities in this domain. These are not technically part of the Chinese governmental apparatus or State-Owned Enterprises. Nevertheless, major Chinese telecommunications firms like Huawei act as de facto proxies for China. As per the Federal Bureau of Investigation (FBI) estimation, China has more than 30,000 military cyber spies, plus an additional 150,000 private sector cyber experts, "whose mission is to steal American military and technological secrets", according to the former head of U.S. counterintelligence, Michelle Van Cleave.[15]

MSS and PLA: Competition vs. Collaboration

The Ministry of State Security (MSS) and PLA are primarily responsible for cyber operations, including espionage and offensive action. PLA's Strategic Support Force (SSF), raised in 2015, has integrated both Computer Network Exploitation (CNE) capabilities for espionage and Computer Network Attack (CNA) capabilities which can prepare potential targets for destructive attacks in a wartime scenario. It is believed that MSS and PLA's SSF operations were somewhat in competition for resources and value collections on identified targets. There was a lack of coordination. However, the coordination is improving with time and greater control of the PLASSF's cyber actions due to reorganisation.

MSS activity can be differentiated from that of the PLASSF based on geographic scope and alignment of operations and victims to each organisation's mission mandate. Threat groups affiliated with PLA Theater Commands focus operations on regions within the areas of responsibility of

their respective Theater Commands. MSS-affiliated groups, demonstrate a much broader geographic scope. Responsibilities are now clearly demarcated. This reflects MSS responsibilities to conduct domestic counter-intelligence, non-military foreign intelligence and support aspects of political security.[16] PLA concentrates on military intelligence and warfighting. There has been a marked increase in cyber espionage activity conducted by the MSS and its contractors over the past several years, signifying the MSS model is more favourable for cyber espionage.

Devolpments in China's Cyber Espionage

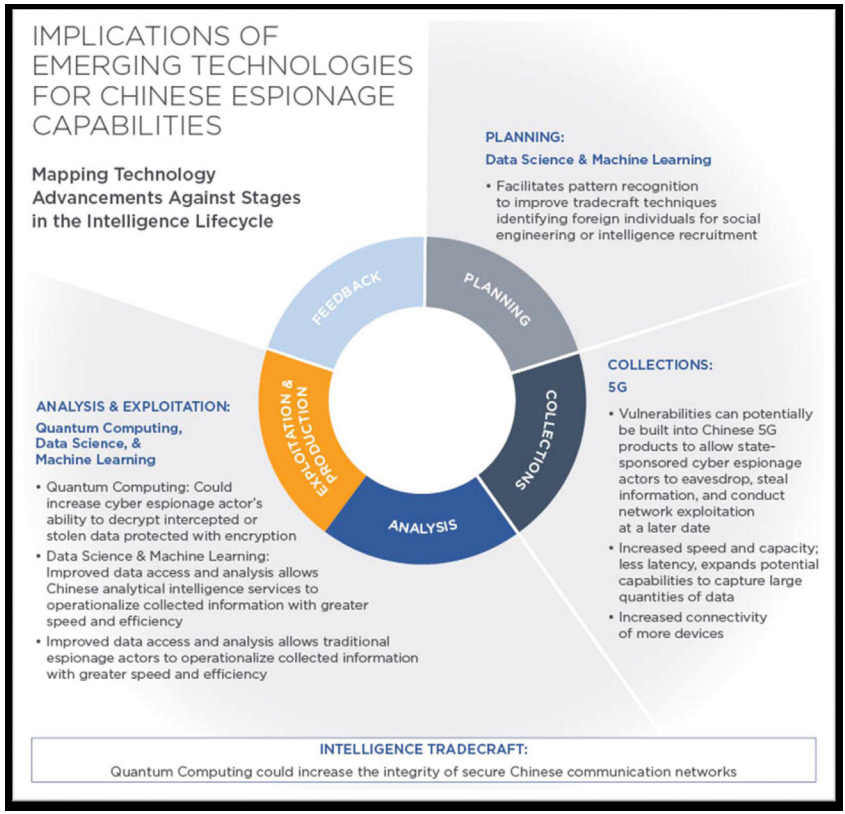
Chinese threat actors use a complete range of tactics, techniques, and procedures (TTPs). The most common methods used are spear-phishing, watering hole attacks and strategic web compromise operations, compromising shared services and operating supply chain compromises. In recent years the threat actors have become more focused and targeted, moving away from the high volume, unfocused older attacks.

Frederick Plan, senior analyst of cyber-espionage at Mandiant Intelligence feels, "Ten years ago, Chinese espionage operators were not as specific about their desired targets and would compromise the websites of major news sites and high-profile industry-focused organisations in an attempt to distribute malware to all visitors to these pages. More recently, however, Chinese groups are generally more nuanced and more choosey with their targets so they will rely on white listing or spear-phishing of specific individuals in a targeted organisation. The use of software security vulnerabilities is also popular with Chinese Advanced Persistent Threats (APT)."[17]

Natalie Page, threat intelligence analyst at Talion, said, "In October 2020, the National Security Agency published a report detailing 25 publicly known high severity vulnerabilities being utilised by Chinese state-sponsored hackers, way after patches had been made publicly available." "For initial infiltration, highly targeted spear-phishing is seemingly the current favoured

tactic amongst these groups," Page added.

Paul Prudhomme, head of threat intelligence advisory at IntSights, told The Daily Swig, "Chinese cyber-espionage groups are among the most sophisticated in the world, but are not as sophisticated as their Russian counterparts. Advanced features of Chinese cyber-espionage attacks have included the exploitation of zero-day vulnerabilities, the execution of supply chain and third-party attacks, and the use of proprietary or custom malware and other tools. Chinese cyber-attacks have nonetheless often had weaknesses in their operational security that have enabled security researchers to attribute them to Chinese actors. "[18]



Source: Kelli Vanderlee, Testimony Before the U.S.-China Economic and Seecurity Review Commission, February 17. 2022

Chief security advisor at Sentinel One and a former U.S. State Department special advisor, Morgan Wright, told The Daily Swig that China was far more deliberate than Russia in executing cyber-attacks. He said, "Russia has moved from being more covert to more overt in the last few years. China, on the other hand, takes time to evaluate progress, identify follow-up tasks, and even develop specific modules depending on the type of machine being attacked. "[19]

How Emerging Technologies Support Chinese Espionage. Innovative emerging technologies such as 5G, quantum computing, artificial intelligence (AI) and machine learning will provide new and better means for Chinese intelligence organisations to capture, transfer, decrypt, and process data.[20]

Comparison with Russia. As of mid-2021, Chinese Advanced Persistent Threats (APT) were not as sophisticated as Russian APTs' nor do the threat intelligence firms link Chinese APTs to cyberattacks such as NotPetya.

The Indian Context

Cyber Security Company Kaspersky predicted a rise in cyber espionage against India in 2022. Based on its data and advanced cyber-intelligence through various reports on cybersecurity, Kaspersky has found India making to the top five nations among targets for cyberattacks, with attention to cyber espionage. The type of attacks that are expected to increase is APT cyberattacks to collect valuable geopolitical, business and military intelligence.

Indian businesses having close tie-ups with entities in Singapore need to take note as Kaspersky identifies Singapore as among the significant hotspot for cyberattacks. Experts believe, "India continues to be on the hit list of some very sophisticated cybercriminals and groups of attackers worldwide. Its bustling economy and expected growth are among the key reasons for the elevated level of threat it faces. The only correct response is prevention is better than cure – to invest in infrastructure and capabilities aimed at improving cyber intelligence by improving prediction capabilities."

If China can breach the cyber security of Microsoft in the Microsoft Exchange attack, it can be reasonably assumed that it can penetrate India's cyber systems. Post Galwan, China would be expected to be active in cyber espionage activities against Indian security forces, the ISRO, DRDO, BARC, critical information infrastructure etc. Indian cyber establishments should be extremely vigilant against these operations and take mitigating actions.

Conclusion

The 'Made in China 2025' plan defines objectives for China to become a major technological and economic power. It identifies ten sectors in which it must become a world leader: information technology, robotics, 5G networks, new materials, electric vehicles, aviation, green energy and medical and agricultural equipment. China employs covert methods for information gathering and combines civilian partnerships with different intelligence and espionage activities of its intelligence agencies. In that, it extensively uses governmental, business, party and academic bodies and private individuals. This systematic and long-term effort meets China's strategic objectives to achieve technological superiority, strengthen its military power, and create dependence as well as influence among foreign countries and elites.[21]

Endnotes

1. Bvp47 - the top backdoor of the US NSA formula group, Feb 23, 2022 available at: https://www.pangulab.cn/post/the_bvp47_a_top-tier_backdoor_of_us_nsa_equation_group/
2. China captures powerful US NSA cyberspy tool, Global Times, Mar 14, 2022 available at: https://www.globaltimes.cn/page/202203/1254856.shtml
3. China cybersecurity firm alleges US National Security Agency is behind hacking group that has stolen a mass of critical data, South China Morning Post, March 23, 2022 available at: https://finance.yahoo.com/news/china-cybersecurity-firm-alleges-us-093000291.html
4. Foreign Ministry Spokesperson Wang Wenbin's Regular Press Conference on April 20, 2022 available at: http://us.china-embassy.gov.cn/eng/fyrth/202204/t20220420_10670511.htm
5. The Mystery of China's Sudden Warnings About US Hackers, Wired, MAY 26, 2022 available at: https://www.wired.com/story/china-us-hacking-accusations/?bxid=5be9d4c53f92a40469e37a53&cndid=49798532&esrc=desktopInterstitial&mbid=mbid%3DCRMWIR012019%0A%0A&source=EDT_WIR_NEWSLETTER_0_DAILY_ZZ&utm_brand=wired&utm_campaign=aud-dev&utm_content=WIR_Daily_052622&utm_mailing=WIR_Daily_052622&utm_medium=email&utm_source=nl&utm_term=P3
6. http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/HuaweiZTE%20 Investigative%20Report%20%28FINAL%29.pdf
7. The Future of Cybersecurity across the Asia-Pacific available at: https://www.nbr.org/wp-content/uploads/pdfs/publications/ap15-2_cyber-rt_apr2020.pdf
8. Roger Cliff, Evan Medeiros, and Keith Crane, "Keeping the Pacific: An American Response to China's Growing Military Might," RAND Corporation, Spring 2007 available at: https://www.rand.org/pubs/periodicals/rand-review/issues/spring2007/ pacific .html
9. Ben Buchanan, The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics, Harvard University Press, Feb 2020
10. Jack Stubbs, "China Hacked Asian Telcos to Spy on Uighur Travelers," Reuters, September 5, 2019 available at: https://www.reuters.com/arti-

cle/us-china-cyber-uighurs-idUSKCN1VQ1A5
11. "APT 1: Exposing one of China's Espionage Units," Mandiant, available at: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.
12. Richard J. Harknett & Max Smeets (2020) Cyber campaigns and strategic outcomes, Journal of Strategic Studies, DOI: 10.1080/01402390.2020.1732354
13. Check Point Research unveils a Chinese APT espionage campaign against Russian state-owned defense institutes available at: https://blog.checkpoint.com/2022/05/19/twisted-panda-check-point-research-unveils-a-chinese-apt-espionage-campaign-against-russian-state-owned-defense-institutes/
14. Adam Kozy, Testimony before the U.S.-China Economic and Security Review Commission Hearing on "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States", February 17, 2022
15. Michelle Van Cleave, "Chinese Intelligence Operations and Implications for U.S. National Security," Testimony before the U.S.-China Economic and Security Review Commission, June 9, 2016, page 5. available at: https://www.uscc.gov/sites/default/files/Michelle%20Van%20Cleave_ Written%20 Testimony 060916.pdf
16. China's Intelligence Services and Espionage Operations," Hearing Before the U.S.-China Economic And Security Review Commission, June 9, 2016 available at: https://www.uscc.gov/sites/default/files/transcripts/June%2009%2C%202016%20Hearing%20Transcript.pdf
17. Behind the Great Firewall: Chinese cyber-espionage adapts to post-Covid available at: https://portswigger.net/daily-swig/behind-the-great-firewall-chinese-cyber-espionage-adapts-to-post-covid-world-with-stealthier-attacks
18. Behind the Great Firewall: Chinese cyber-espionage adapts to post-Covid available at: https://portswigger.net/daily-swig/behind-the-great-firewall-chinese-cyber-espionage-adapts-to-post-covid-world-with-stealthier-attacks
19. *Ibid*
20. Kelli Vanderlee, Testimony Before the U.S.-China Economic and Seecurity Review Commission, February 17. 2022.
21. Nir Ben Moshe, Chinese Espionage Operations in the United States: And in Israel? No. 1560, February 20, 2022.

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