CENTRE FOR LAND WARFARE STUDIES

ISSUE BRIEF

No. 337 April 2022

India's Options against China's Developing Cyber Capabilities

Major General PK Mallick, VSM (Retd) held the Chief of Army Staff Chair of Excellence at CLAWS. The General is an Electronics and Telecommunication Engineering graduate from BE College, Shibpore, MSc (Defence Studies) from Madras University, M.Tech from IIT, Kharagpur, MMS from Osmania University and M. Phil from Madras University. He was commissioned in the Corps of Signals of Indian Army. The Officer has interest in Cyber Warfare, Electronic Warfare, SIGINT, Technology and Strategic Affairs. His last posting before retirement was Senior Directing Staff (Army) at National Defence College, New Delhi.

Introduction

If countries go to war, cyber-attacks will be a part of it. Cyber operations are a new way to exercise national power. How countries will use cyber operations is determined by their existing strategies, larger interests, risk tolerance, experience and institutions.

China is increasingly using cyber capabilities including cyber espionage, attack and influence to seek political, economic and military advantage over its adversaries. Like the internet, cyberspace and the digitised information environment are in their relative infancy as are the strategic, operational, and doctrinal concepts governing military operations in this relative unknown territory.

Key Points

- China is using cyber capabilities to seek political, economic and military advantage over its adversaries.
- In cyber domain, China has advanced far ahead of India.
- IISS Report on Cyber Capabilities and National Power has interesting observations on India.
- India should take some action in Mission Mode.
- At the Chief of Defence Staff (CDS) level, certain actions are recommended.
- India should develop Deterrence Capability.

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with national security and conceptual aspects of land warfare, including conventional & sub-conventional conflict and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.
Website: www.claws.in **Contact us: landwarfare@gmail.com**

In cyber and space domains, China has advanced far ahead of India. With India's software development capabilities and human resources, it should have taken the lead in these areas. However, it should now catch up fast.

India has taken some baby steps by establishing the Defence Cyber Agency, a precursor to the Cyber Command. Indian Armed Forces could have leapfrogged from the present state to cyber command, keeping in view the fast changes in the cyber domain. They have taken the evolutionary approach. Knowing how bureaucracy, including military bureaucracy, works this may not be a bad idea.

IISS Report on Cyber Capabilities and National Power

The recent International Institute for Strategic Studies (IISS) Report on Cyber Capabilities and National Power has interesting observations on India. These are:[1]

- India has made only ‘moderate progress’ in developing its policy and doctrine for cyberspace security.
- India's approach towards institutional reform of cyber governance has been ‘slow and incremental’.
- The ‘private sector’ has moved more quickly than the government in promoting national cyber security.
- India is ‘visible and active’ in cyber diplomacy. However, it cannot be counted among the leaders on global norms. India prefers to engage with leading states to make productive and practical arrangements.
- India’s offensive cyber capability is ‘Pakistan focused’ and regionally effective. It is not focused on China.
- India's best chance of advancing to the second tier is by ‘harnessing’ its great digital industrial potential and adopting a whole-of-society approach to upgrade its cyber security.
- Since the early 2000s, India's cyber command-and-control structure has been under development but remains ‘decentralised’.

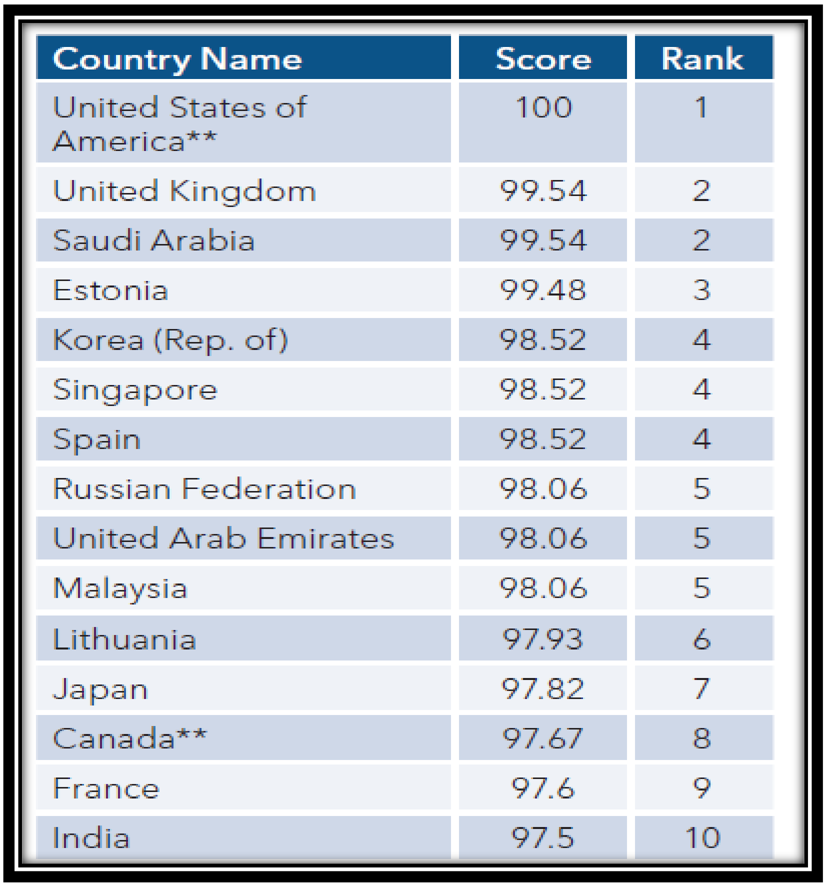
- Cyber security powers are spread across various agencies, with reports of ‘overlapping competencies’ and ‘bureaucratic turf wars’.
- The Intelligence Bureau (IB), Research and Analysis Wing (R&AW) and Defence Intelligence Agency (DIA) each represent a part of India’s cyber intelligence capability. They are all ‘heavily reliant’, for core capability, on the technical intelligence agency— the National Technical Research Organisation (NTRO). Various parts of the Ministry of Home Affairs, including the Cyber Crime Wing and Central Forensic Science Laboratory, are also important sources of cyber intelligence.
- India’s cyber intelligence reach is weak. It relies on partnerships with U.S, U.K. and France for a higher level of cyber situational awareness.
- The infrastructure is mainly built from imported equipment at the heart of India’s digital economy.
- Almost all the country’s most popular mobile applications were designed abroad. One exception is Aarogya Setu, the Indian government’s COVID-19 contact-tracing app.
- India has been the victim of cyber attacks frequently, including on its critical infrastructure— a significant proportion of them has been attributed to China or Pakistan. CERT-In reported that there were more than 394,499 incidents in 2019, and 2020 saw an upswing in attacks from China.[2]
- The majority of cyber incidents flagged by CERT-In, appear to have been espionage attempts. However, they could have resulted in severe damage to the integrity of Indian networks and platforms.
- India had the second-highest number of Ransomware attacks in the world in 2020.
- Because of stringent guidelines from the Reserve Bank of India (RBI), the financial sector is more secure than other areas of the Indian economy.

Cyber Security

Everything is not bad in the cyber domain in India. As per the Global Cyber security Index (GCI), an initiative of the International Telecommunication Union (ITU), India was ranked 47th out of 175 countries in the International Telecommunication Union's 2018 GCI, well behind its geopolitical rival— China (27th).[3]

However, in the latest 2020 GCI, India is ranked 10th while China is ranked 33rd.[4]

Figure 1: GCI results: Global score and rank



Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10

Source: https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/

India can learn from the Israeli theoretical and practical approaches to cyber security experience. These are:[5]

- A National Concept of Operation to Deal with Cyber-attacks and Attackers as part of an overall National Cyber Strategy
- An operational Central Cyber Agency for National Cyber Defence
- Enhancing National Robustness
- Establishing a Cyber Eco-System of Industry, Academia and Human Capital
- Cyber Commando. Assembling Small Elite Teams to Tackle Tough Techno-Operational Problems
- Dealing with Attackers, not only Attacks.

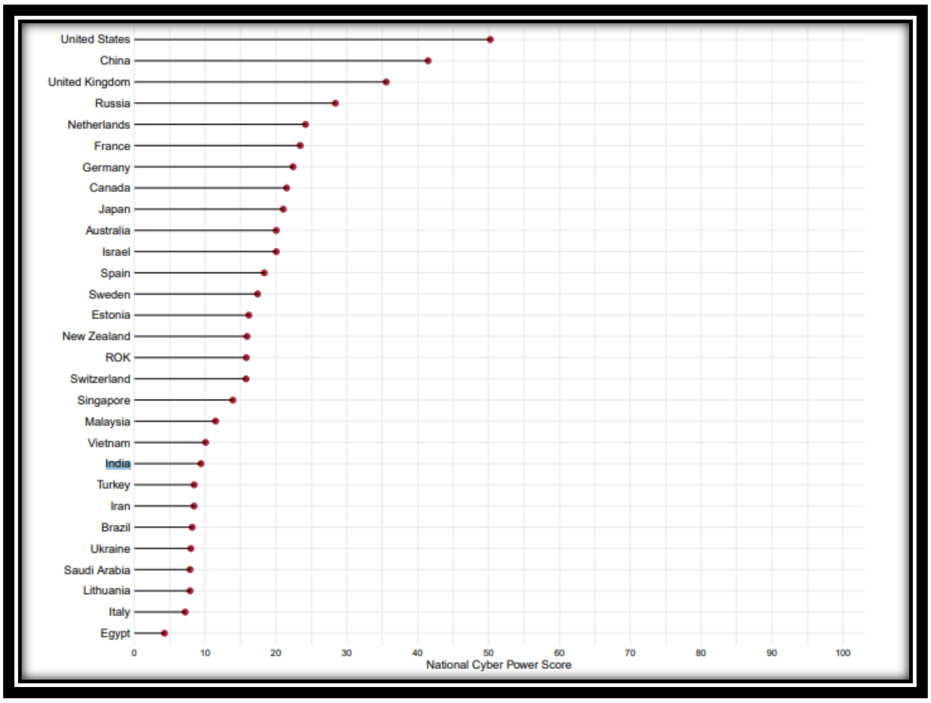
The following is recommended for the defence of our networks:[6]

- Removes Barriers to threat information sharing between Government and the private sector.
- Modernise and implement stronger cyber security standards in the Government.
- Improve software supply chain security.
- Establish a cyber safety review board to analyse following a significant cyber incident and make concrete recommendations for improving cyber security.
- Create a standardised procedure for responding to cyber security vulnerabilities and incidents.
- Improve investigative and remediation capabilities.

Cyber Warfare

In a report published by Belfer Center for Science and International Affairs Harvard Kennedy School, China is ranked second in the National Cyber Power Index, behind only the US. In contrast, India is ranked 21st of the 30 countries analysed.[7]

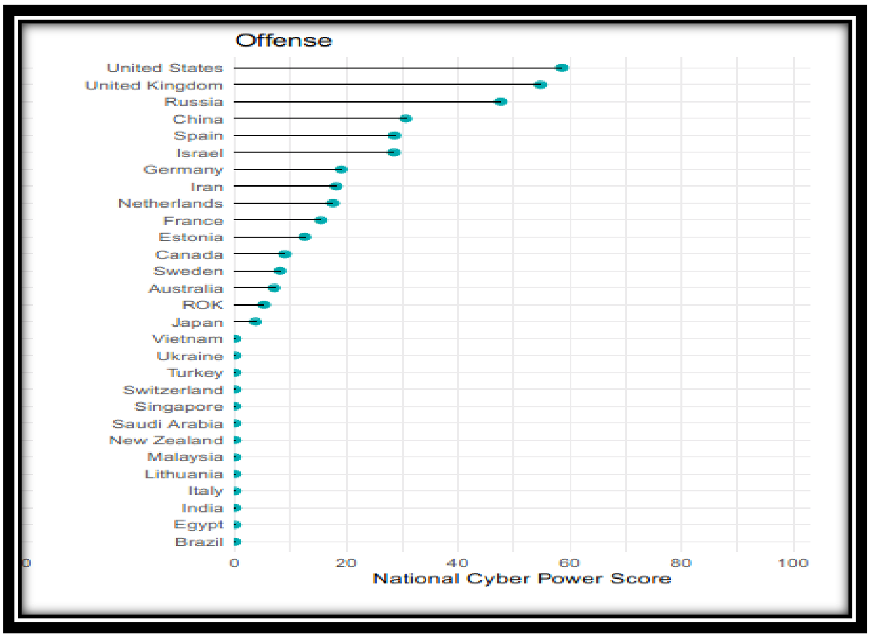
Figure 2: NCPI 2020: Most Comprehensive Cyber Powers



Source: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

India’s offensive cyber capabilities have been shown as under.

Figure 3: India's Offensive Capability Position



Source: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

India has been placed under the category of Lower Capability & Lower Intent. Countries that fall into this category either are not actively developing the capability and intent to project power in cyberspace or have not published sufficient information on their cyber strategy, cyber attacks attributed to them, or capabilities.

China is an acknowledged master in cyber espionage activities. In addition to traditional state espionage, Chinese hackers are said to be stealing intellectual property from every significant Fortune 500 company, American research laboratories and think tanks worth trillions of dollars. According to FBI Director Christopher Wray, there are more than 2,000 open espionage cases currently directed by Beijing to support economic and technology goals.[8]

Chinese hackers have taken everything, from the designs of the next F-35 fighter jet to the Google code, the US smart grid and the formulas for Coca-Cola, Benjamin Moore paint and Microsoft Exchange Server.[9]

In the recent report of The US intelligence community (IC) on Annual Threat Assessment, the report raises concerns about China's ability to disrupt the United States' critical infrastructure; warning that "China almost certainly is capable of launching cyber attacks that would disrupt critical infrastructure services within the United States, including against oil and gas pipelines and rail systems.[10]" If China can break through the reasonably good cyber network defences of these organisations, then it can be logically assumed that Chinese malware are present in most of India's critical information infrastructures.[11]

It is true that China has not shown its hand in carrying out offensive cyber operations against India. But, the only distinction between computer network exploitation and attack is the attacker's intent, as the malware is already inside your network. The skill sets required to penetrate a network for intelligence collection purposes and offensive action are the same.

Several measures have been initiated to improve the cyber defence of important infrastructures. However, some reality checks are worrisome. The September 2019 cyber exploitation by North Korean cyber criminals in India's largest civil nuclear facility— the Kudankulam Nuclear Power Plant in Tamil Nadu, highlighted the vulnerabilities of Indian nuclear power plants. These nuclear installations do not fall under the National Critical Information Infrastructure Protection Centre and have not been audited by them.[12] If a cybercrime team from North Korea can penetrate India's largest nuclear facility, surely state-backed cyber attacks can cause much more damage.

Many of India's extremely sensitive and critical networks are not audited by any agency but are self-audited, including the intelligence agencies, armed forces, Defence Research and Development Organisation (DRDO), defence public sector undertakings and the Ordnance Factory Board units. There is an urgent need to put these organisations under some cyber audit mechanism.

Indian Cyber Players. Indian cyber exploitation actions have come under increasing attention. The Daily Swig, a website that gives the latest cyber security news from around the world, has provided the following information about Indian hacker groups:[13]

- Indian cyber espionage differs from other top state-sponsored threats, like those of Russia and China, in their attacks' less ambitious geographic scope.

- India has less mature cyber warfare tools and capability than the 'Big Six' – China, North Korea, Russia, Israel, UK and US At this stage, they cannot call on a cache of zero-day exploits to utilise. They use reasonably practical techniques such as decoy documents containing weaponised macros. It may change over time since their capability is growing.
- The level of sophistication of these groups affiliated with India can vary. Few have shown a high level of sophistication in using advanced custom-built tools or advanced exploits.
- The level of sophistication is not always linked with the group's operation or goals' success rate. At times, simple social engineering attacks delivering a known commodity malware can be enough to get the threat actors what they want.
- There is no shortage of people with advanced technical skills in India.

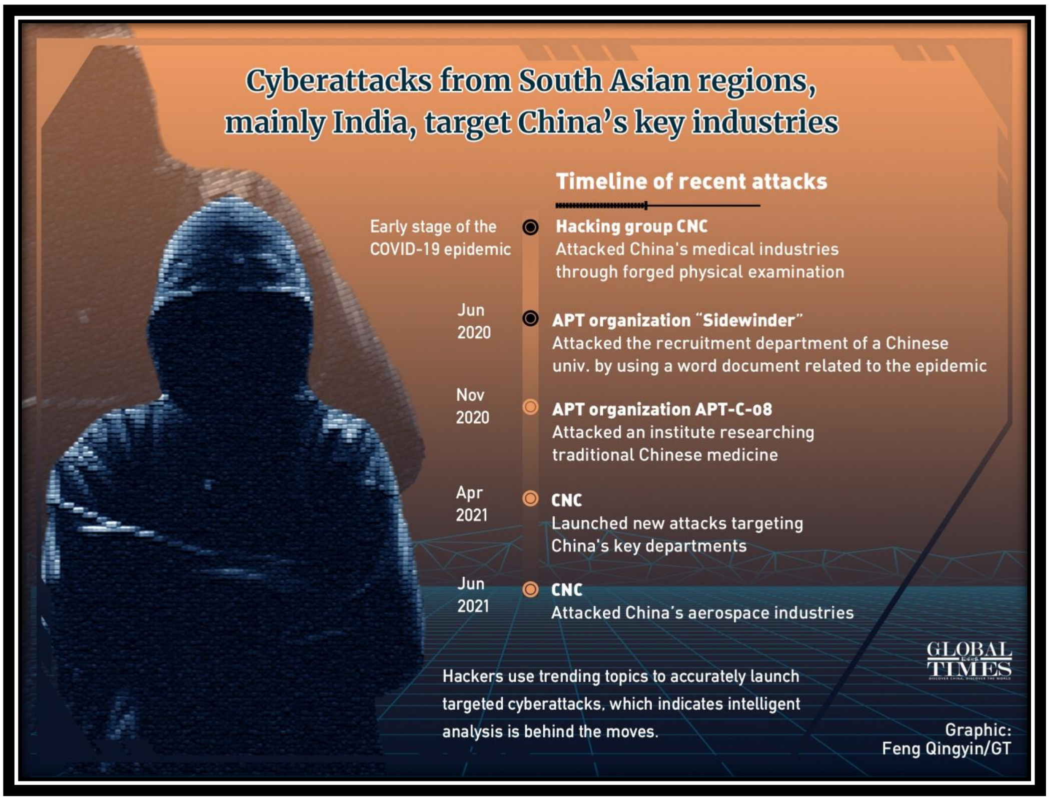
Recent Attacks by Indian Hacker Groups. The cyber espionage entity known as Side Winder has been highly active since 2012. A report by AT&T Alien Labs shows that most of Side Winder's activity is heavily focused on South Asia and East Asia, likely to be supporting Indian interests.

Recorded Future observed that suspected Side Winder targeted Chinese military and government entities in 2020. Side Winder APT group used the ‘Binder Exploit’ to attack mobile devices and used lure files related to Covid-19.[14]

Cyber security company Trend Micro stated, "While tracking the activities of the Side Winder group, which has become infamous for targeting the South Asia region and its surrounding countries, we identified a server used to deliver a malicious LNK file and host multiple credential phishing pages. We learned that these pages were copied from their victims’ webmail login pages and subsequently modified for phishing. We believe further activities are propagated via spear-phishing attacks”.[15]

In an interesting development, China has accused India of hacking China’s defence and military units and state-owned enterprises.

Figure 4: Cyber Attacks from SA Regions targeting China



Cyberattacks from South Asian regions, mainly India, target China's key industries

Timeline of recent attacks

Early stage of the COVID-19 epidemic — **Hacking group CNC**
Attacked China's medical industries through forged physical examination

Jun 2020 — **APT organization "Sidewinder"**
Attacked the recruitment department of a Chinese univ. by using a word document related to the epidemic

Nov 2020 — **APT organization APT-C-08**
Attacked an institute researching traditional Chinese medicine

Apr 2021 — **CNC**
Launched new attacks targeting China's key departments

Jun 2021 — **CNC**
Attacked China's aerospace industries

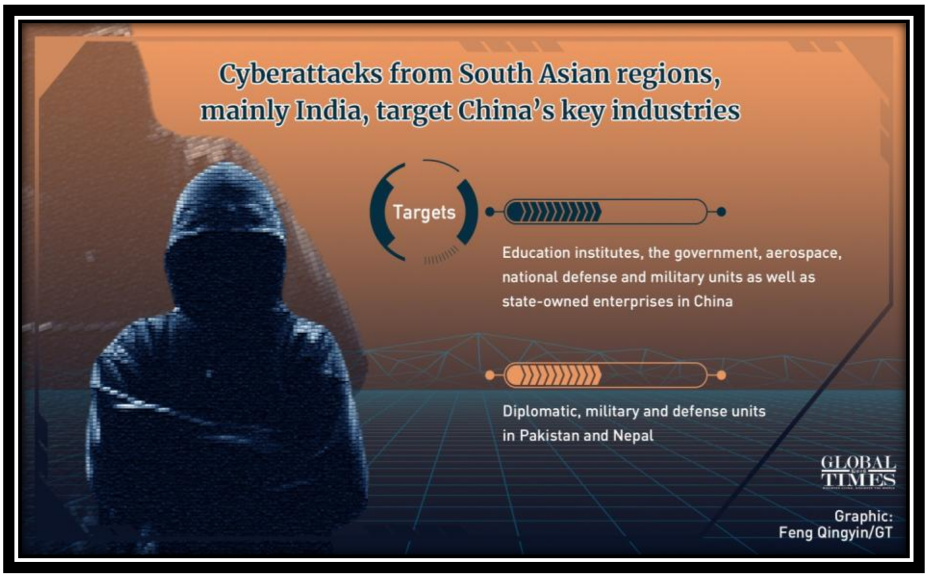
Hackers use trending topics to accurately launch targeted cyberattacks, which indicates intelligent analysis is behind the moves.

Graphic: Feng Qingyin/GT

Source: https://www.globaltimes.cn/page/202111/1238218.shtml

One of China's well-known cyber security companies— Antiy Labsin, in a statement to the *Global Times* stated "Since March, we have detected several phishing activities targeting government, defence and military units, as well as state-owned enterprises in China, Pakistan, and Nepal. The organisation behind the attacks is from India, and its activities can be traced back to as early as April 2019. So far, more than 100 phishing fake websites created by the organisation have been detected by Antiy Labs[16]".

Figure 5: Cyber Attacks on China's Key Industries


Cyberattacks from South Asian regions, mainly India, target China's key industries
Targets
Education institutes, the government, aerospace, national defense and military units as well as state-owned enterprises in China
Diplomatic, military and defense units in Pakistan and Nepal
GLOBAL TIMES
Graphic: Feng Qingyin/GT

Source: https://www.globaltimes.cn/page/202111/1238218.shtml

360 Security Technology, one of China's tech giants, told the Global Times, "hackers from India have been actively launching cyber attacks targeting multiple organizations and individuals in China in the past two years. In 2020, the company monitored and captured more than 100 initial payloads mostly from India and they induced users to execute malicious payloads through harpoon emails in various fields." [17]

Their attacks were largely on the rise in the first half of 2021, targeting education, government, aerospace and defence industries in many fields. The company said that those attacks were especially aimed at organisations or individuals mentioned in online trending topics—politics and economy, the pandemic situation and industrial activities. Cyber security analysts from the company believed that an intelligence organisation is likely behind such accurate hacks".[18]

What should India do in Mission Mode

- ***War Gaming of Probable Events.*** Probable scenarios in a realistic environment should be 'wargamed' to determine the vulnerabilities in our systems and take appropriate remedial measures. For instance, consider this scenario. Just before a conflict in India's North East, the power grid and railway communications network failed, adversely impacting the large-scale movement of men and material of the armed forces. War Gaming scenarios like these will help identify and plug weaknesses.

- ***Mismatch in Cyber Security Measures.*** Though, there has been improvements in the cyber defence of power networks, the efficacy varies. For example, the NTPC, other public sector undertakings and private sector may be well off in cyber protection, but can the same be said about the arrangement in a state-owned hydroelectric plant that is also connected to the national power grid? A hacker could quickly get into the national power grid through this poorly protected power plant and create mayhem at their choosing. What can India do to prevent this incident?
- ***Development of Crypt Analysis Capability.*** India does not have any high-grade crypt analysis capability. The introduction of 128 or 256 bits keys has made code-breaking extremely difficult. However, US National Security Agency (NSA) and U.K. Government Communications Headquarters (GCHQ) already possess this capability, as also perhaps Russia and China. India, therefore, should start the process of developing this capability. Crypt analysts and mathematicians with the power of supercomputers must come together to develop this capability. Collaboration with countries like Ukraine, Belarus, South Africa, Iran and Russia can be explored. There is a difference between cryptography and cryptanalysis. Cryptography is largely theoretical. Indian Army must invest in developing cryptanalysis capabilities and should not fritter away scarce resources.
- ***Forensic Labs for Embedded Hardware and Software.*** India is the world's biggest importer of military equipment, comprising plenty of electronic hardware and software components. No country shares its codes. There is always a chance of embedded hardware and software in such weapon platforms. What is the mechanism to check whether or not there is any malware in the increasingly sophisticated technology areas? What is the mechanism in the procurement of equipment procedure and supply chain management system to ensure that bugs are not present? While procuring, some legal and business clauses can be incorporated. India should develop its own testing facilities. Such testing facilities are extremely niche technology and expensive. [19]

- ***Command and Control Set-Up.*** There should be no ambiguity concerning the responsibility of organisations for cyber security. In the US NSA and Cyber Command come under the Department of Defense. In the UK, the GCHQ falls under the Foreign Ministry. In Israel, the National Cyber Bureau, directly under the Prime Minister, regulates activity in cyberspace. In India, the NTRO has been entrusted with this responsibility, which does not come under any Ministry and operates directly under the Prime Minister's Office. The interplay between the Ministry of Defence, the Armed Forces, the Ministry of Home Affairs, the Ministry of External Affairs and Intelligence Agencies (internal and external) needs to be clearly demarcated. Who will carry out offensive cyber operations in a conflict scenario? Can an intelligence agency do it, bearing in mind the rules of engagement or the laws of armed conflict?
- ***Collaboration with Friendly Countries.*** India should actively collaborate and exchange information with friendly countries like Japan, Taiwan, Vietnam and Australia. For developing niche technology, counties like Israel, Belarus, Romania and South Africa can be approached.

Psychological Operations

Information operations doctrine acknowledges the important role that cyberspace operations play in information operations. Whereas, cyberspace operations doctrine generally ignores this relationship and the human element.

In the Indian Armed Forces who is responsible for carrying out Psychological Operations? It requires a broad and deep integration of cultural and regional knowledge in concert with technical skills, knowledge, abilities and attributes. In the U.S Special Operations Command (USSOCOM) does the Psychological Operations.

Currently, the Indian armed forces and strategic community blindly follow US jargon. In today's world, if you want to influence the mind of the people and the leaders of the adversary, then what terminology should be used? Is it information operation, psychological operation, strategic communications, influence operations, perception management, public information operations, public field diplomacy, or similar terms? These terms are being used interchangeably, but they are not synonyms. The Indian Armed Forces must coin their own common phrase and take appropriate actions to develop concepts, tactics, techniques and procedures.

Take, for instance, information warfare. The various stakeholders are the Ministry of Home Affairs and the Intelligence Agencies, Ministry of Defence, Ministry of External Affairs, Ministry of Information and Broadcasting, Ministry of Electronics and Information Technology, Ministry of Communications and Ministry of Education, Ministry of Law & Justice among others. Close coordination between these Ministries will be required to carry out information warfare against an adversary. As of now, there is no central agency to coordinate and lead such a task. The integration for the use of information operations within the armed forces is minimal as well.

The National Security Council Secretariat is the appropriate agency to be made responsible for information operations, given India's notoriously stove-piped bureaucracy.

Actions Recommended to be Taken at the Chief of Defence Staff (CDS) Level

The role of the armed forces for the protection of critical information infrastructure, including the private sectors, should be clearly defined. What happens when the armed forces are called in to provide aid to the civil authority in case of some cyber calamity?

The following actions are recommended:

- Should extensively use cyber training ranges. Preferably Indian Army should take the lead.
- Should develop and implement professional development courses to build leaders and elite forces in the cyber branches of all services.
- The MoD and the Army should leverage appropriate expertise outside the military, that is from academia, industry and individuals to augment their cyberspace planning, operation and capability development.
- Should establish a Centre of Excellence (CoE) dedicated to the cyber domain. The Indian Army can be the lead agency as it has already a CoE at the Military College of Telecommunication Engineering (MCTE), Mhow.
- Coordinate with the services and integrate cyber operations and related activities.

- Should develop theories and concepts of cyber operations at strategic, operational and tactical levels.
- Should encourage open discussion regarding the future evolution of military cyberspace in terms of tasks, authorities and organisational structures.
- Should consider raising an organisation like the Defense Information Systems Agency (DISA) under the US Department of Defense which provides, operates and assures command & control and information sharing capabilities in direct support to war fighters and national level leaders across the full spectrum of military operations.
- Should create a mechanism to ensure that bugs are not present in the procurement of equipment and supply chain management system.
- Should define Rules of Engagement for armed conflicts.
- Should lay down human resource development policies for the Armed Forces in the cyber domain. It will require drastic changes to attract and keep talents in such niche technology areas. The Chiefs of the Army, Navy and the Air Force should direct their military secretary branch and its equivalents to treat the cyber career field as a national security priority, where promotion boards must understand the cyber mission as a priority and facilitate recruitment, retention and career-long professional development in cyber expertise.
- Create a red team for performing operations on MoD critical systems and critical infrastructure.
- The Defence Minister of India should be regularly updated on identified challenges, plans and progress.
- Direct DCA to develop cyber capabilities/effects focused on adversary military targets, which would include:
    - Development of infrastructure and tools to support his Forces.
    - Ensure operational experience and an appropriately skilled workforce.
    - Create agility to respond to dynamic situations/opportunities.
- Develop a deliberate plan and acquisition strategy that leverages existing infrastructure and identify where new infrastructure and tools are required.

- Develop a plan for joint training, exercises and ultimately operations with and alongside other national cyber organisations operating as joint teams.
- Ask DCA to establish and enlarge professional military education opportunities at all levels, allowing military personnel to work in cyber-related private sector positions. Should encourage greater commercial exchange opportunities to improve skills and operational understanding.
- Create a mechanism to coordinate national cyber priorities and private-public collaboration across the spectrum of peace, no war no peace, and war. DCA should play a key and unique role in this.
- The Office of Net Assessment in HQ IDS should institute a continuous strategic net assessment process to support its operations. This process should leverage the Intelligence Community, industry & academia and integrate red team assessment activity for measuring our effectiveness in cyberspace.
- Should coordinate with MHA and the Ministry of Law and Intelligence Agencies to review existing laws governing action in cyberspace. Should update or draft replacement language to protect own people and promote national interests in cyberspace.
- The incident of the compromise of widely used enterprise IT systems (SolarWinds), reportedly by Russian intelligence and Russian cyberattacks against Ukraine's critical infrastructure, are well known. In case of such happening in India, what should be our action? What offensive cyber capabilities should we develop? Should war game all these likely eventualities and take action accordingly.
- The responsibilities should be made clear. For example, who should take action against ransomware crime groups, terrorist operations online or state actors like China or Pakistan?

Development of Deterrence Capability[20]

Though this is a highly classified domain, the armed forces and intelligence agencies must develop these capabilities in close cooperation. These should be tested in peacetime to be employed in the event of war. Projects that can be undertaken as part of capability development could include:

- How to penetrate the adversary’s classified military networks?
- How to isolate a built-up area electronically and in the cyber domain before carrying out any kinetic operation?
- The kind of tasking to be given to Special Forces operating deep inside enemy territory. For instance, can they puncture the enemy's optical fibre cable networks and obtain data?
- Develop malware in pen drives to be inserted into the enemy's classified network with the help of intelligence agencies so that information is sent back undetected at appropriate times.
- Develop cyber exploits to be planted in the enemy's key military infrastructure like telephone exchanges, main servers of classified networks or radar installations to explode electronically at an appropriate time to make them non-functional.
- How to influence the minds of opposing operational, strategic commanders and leaders, especially of our northern neighbours?
- The security of the tactical data link of India's extremely costly airborne early warning and control system related to other flying aircrafts or bases. India must develop its own solutions for such highly classified links and not rely on foreign technology.
- How to overcome electronic and cyberattacks by a swarm of drones? How to develop a malware that can be flown into an adversary’s dense radar coverage, homed onto the radar beam and inserted to make the Air Defence Command and Control Systems malfunction, like in Operation ORCHARD?[21]

Removal of Chinese Network Equipments. Earlier, there was no national policy on the use of Chinese network equipments and hardware. The audit authorities have no concern for national security and insist on the least price. Chinese companies always have the advantage of low prices. In the L-1 syndrome, Chinese telecom equipments get inducted into many sensitive and classified network of the Indian Armed Forces. Although commanders at every level have the authority to overrule audit observation on the grounds of security and procure equipment, this option is generally not undertaken for valid reasons. In the changed scenario, efforts should be made now to remove the Chinese equipments from these networks.

Cyber Capabilities at Operational and Tactical Levels. What is our policy to provide cyber capabilities at the operational and tactical level? Due to the characteristic of target equipments and terrain features in operational and tactical battlefields, proximity to the target is essential. In the US, to carry out sophisticated cyber operations in operational and tactical battlefields, the most elite and niche technology cyber warfare experts from the NSA's Tailored Access Operations are included at appropriate levels in the battlefield. They carry out the tasks and report back to the headquarters. The Indian Army should also have similar arrangements with NTRO. The procedures should be rehearsed well in advance and glitches sorted out.

There are no boundaries in the cyber domain. Any offensive cyber operation at the lowest level can quickly go out of control and become global. Stuxnet did not remain within the confines of Iranian Nuclear Installations. Russia carried out NotPetya cyber-attack against Ukraine in June 2017. It quickly spread worldwide and caused damage of more than $10 billion.

We need specifically trained senior officers who have the technical and strategic education to carry out offensive cyber operations by the armed forces. The current focus is on developing technically skilled people in the junior ranks. The General Cadre strategic leadership of Indian Army comes from National Defence Academy. Most of them are from Sainik Schools. A large number of them are arts graduate from the Jawaharlal Nehru University(JNU). The existing Professional Military Education (PME) does not educate and prepare Indian Army's strategic leadership to operate in extremely high-tech niche technology areas[22]. Without adequate knowledge and expertise, it will not be proper to give responsibility to the Indian Army's strategic leadership for offensive cyber operations. It may have catastrophic consequences.

It is strongly recommended that no offensive cyber operations be carried out at the army's tactical, operational, and strategic levels.

Cyber operations capabilities in the tactical battle area could include the following:[23]

- Collect intelligence by rapidly exploiting captured digital media.
- Counter and exploit adversaries' unmanned aerial systems by exploiting data feeds.
- Protect friendly unmanned aerial systems functioning in the area of operations.
- Gaining access to closed networks in or near the area of operations, including extracting and injecting data.
- Using electronic warfare systems as "delivery platforms for precision cyber effects".
- Exploiting new devices emerging from latest trends and opportunities.
- Conducting cyberspace intelligence, surveillance and reconnaissance operations.
- Engaging in offensive social media operations.

Bug Bounty Program. The US Army conducts 'Bug Bounty Program' to incentivise security research and reporting of real-world security vulnerabilities in exchange for monetary rewards. This helps in resolving the vulnerabilities before the adversaries exploit them. The last Program was held from 06 January to 17 February 2021.

Bug Bounty Programs are an effective force multiplier for securing critical Army networks, systems and data. By crowdsourcing solutions with the help of military and civilian ethical hackers, the existing security measures are complemented.

The participants had identified 238 vulnerabilities, including 102 rated high or critical and designated for immediate remediation. More than $150,000 was awarded to eligible civilian hackers in bounties during "Hack the Army 3.0".[24] In China the Chinese hackers compete to find new cyber vulnerabilities in Tianfu Cup. The competition has shown the noteworthy technical talent of participating Chinese individuals[25].Indian Army should also organise such 'Bug Bounty Programs' to identify vulnerabilities in their network and take remedial measures.

HRD Policy. The Human Resource Development (HRD) Policies for the armed forces will require drastic changes to attract and retain talent in the niche technology areas. The present policies for talent management are inadequate.

Conclusion

India has been a target of cyber espionage by several states. India understands that its defensive capabilities are comparatively weak. India has increased its diplomatic efforts to bring cyberspace governance within the rules-based international order. For dealing with states carrying out cyber operations against India, it maintains a realistic approach. At least in the public domain, it is unknown whether India will use the options of retaliatory measures for acts that fall below the thresholds of a 'threat or use of force' or 'armed attack' under international law.

India's bilateral cyber partnership with the US is well developed. India pursues bilateral cyber dialogues with several states, including the European Union, the UK and Russia. The cyber partnership with UK is particularly well developed.[26] Information from the open domain indicates that India has developed relatively advanced offensive cyber capabilities focused on Pakistan. It is believed that the focus may have been shifted more to countering China.[27]

No cyber defence can be full-proof. Every piece of hardware, software, code, connectivity, privilege and access at all times cannot be protected. Attacks will come, and defences will be breached. If the Chinese hackers can breach the Pentagon, it can happen in India also. Points to be considered are: when do we realise that breach has happened, does it have the capacity to damage the system, what is the resilience of the system, how much time it takes to plug the gap etc. The September 2019 cyber exploitation by North Korean cyber criminals in India's largest civil nuclear facility— the Kudankulam Nuclear Power Plant in Tamil Nadu, was undoubtedly a wake-up call. If a cybercrime team from North Korea can penetrate India's largest nuclear power plant, surely state-backed cyber attacks can cause much more damage. The shortcomings detected in that incidence should have been corrected by now. Who could imagine that nuclear power plants were not part of the responsibilities of NCIIPC?[28] Was the malware detected by in house expertise of CERT- In or NCIIPC, or did they get the information provided by Recorded Future? How come all these major breaches in recent cyber exploitation activities in critical information infrastructures have been reported by foreign cyber security companies and not detected by us? Typically cyber exploitation activities for industrial espionage are carried out by The Ministry of State Security (MSS) of the Chinese government and not by PLA. The affiliation of Red Echo to PLA should raise heckles as it would indicate the intention of a cyber attack by PLA in an opportune time.

There are question marks on Indian cyber security companies. Some of the experts may be earning big bucks in US IT companies' Bug Bounty Programs. It is time now for them to show their expertise in detecting breaches in Indian critical information infrastructure. How do we get them to work for the Indian system? Bureaucratic hurdles have to be overcome. The Nation must be assured of the resilience of India's critical information infrastructure. It is given that breaches will take place. The issue is what we do after the breach has happened. Can we hack the hackers? What are our deterrence capabilities against an adversary like China?

It seems India has miles to go in the cyber domain.

End Notes

[1] "Cyber Capabilities and National Power: A Net Assessment", *IISS*, 28 June 2021. Available at https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power. Accessed on 31 March 2021.

[2] "Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology", *CERT-In Annual Report*, 2019. Available at https://www.cert-in.org.in/Downloader?p ageid=22&type=2&fileName=ANUAL-2020-0001.pdf. Accessed on 31 March 2022.

[3] "Global Cyber security Index (GCI) 2018", *International Telecommunication Union*, 2019, p. 58. Available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf. Accessed on 31 March 2022.

[4] Ibid.

[5] Eviatar Matania and Lior Yoffe, "Some Things the Giant Could Learn from the Small: Unlearned Cyber Lessons for the US from Israel", *The Cyber Defense Review*, Winter 2022. Available at https://cyberdefensereview.army.mil/Portals/6/Documents/2022_winter/11_Matania_Yoffie_CDR_V7N1_WINTER_2022.pdf?ver=Y-_Ofzd37FWrxaZmICkkFQ%3D%3D. Accessed on 31 March 2022.

[6] Drew Spaniel, "Playing to Win: Using Strategy to Create Your Cybersecurity Battleplan",*Institute for Critical Infrastructure Technology*, March 2022. Avialable at https://icitech.org/category/latest-posts/. Accessed on 31 March 2022.

[7] Julia Voo et al, "National Cyber Power Index 2020", *Belfer Center for Science and International Affairs Harvard Kennedy School*, September 2020. Available at https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf. Accessed on 01 April 2022.

[8] Pete Willams, "FBI Director Wray Says Scale of Chinese Spying in the US Blew Me Away", 01 February 2022. Available at https://www.nbcnews.com/politics/politics-news/fbi-director-wray-says-scale-chinese-spying-us-blew-away-rcna14369. Accessed on 01 April 2022.

[9] "China's Microsoft Hack May Have Had A Bigger Purpose Than Just Spying", *NPR*, 26 August 2021. Available at https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying. Accessed on 01 April 2022.

[10]"Annual Threat Assessment of the US Intelligence Community", *Office of the Director of National Intelligence*, 09 April 2021. Available at https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf. Accessed on 01 April 2022.

[11] "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China", *US Department of Defense*, 15 May 2017, p.72. Available at https://www.defense.gov/Portals/1/Documents/pubs/2017ChinaMilitaryPowerReport.PDF. Accessed on 02 April 2022.

[12] PK Mallick, "Cyber Attack on Kudankulam Nuclear Power Plant: A Wake Up Call", *Vivekananda International Foundation*, December 2019. Available at https://www.vifindia.org/paper/2019/december/18/cyber-attack-on-kudankulam-nuclear-power-plant. Accessed on 02 April 2022.

[13] John Leyden, "Indian cyber espionage activity rising amid growing rivalry with China-Pakistan, *Port Swigger*, 25 February 2021. Available at https://portswigger.net/daily-swig/indian-cyber-espionage-activity-rising-amid-growingrivalry-with-china-pakistan. Accessed on 02 April 2022.

[14] "Study suggests Chinese cyber campaign targeted India's power grid after Galwan Valley clash", *Deccan Herald*, 01 March 2021. Available at https://www.deccanherald.com/national/study-suggests-chinese-cybercampaign-targeted-indias-power-grid-after-galwan-valley-clash-956614.html. Accessed on 03 April 2022.

[15] Joseph C Chen, Jaromir Horejsi, Ecular Xu, "Side Winder Uses South Asian Issues for Spear Phishing, Mobile Attacks", *Trend Micro*, 09 December 2020. Available at https://www.trendmicro.com/en_us/research/20/l/sidewinderleverages-south-asian-territorial-issues-for-spear-ph.html. Accessed on 05 April 2022.

[16] "GT investigates: Hacking China's medical institutes at COVID-19 outbreak, targeting aerospace firms during China's space missions – Cyberat tacks from India disclosed", *Global Times*, 05 November 2021. Available at https://www.globaltimes.cn/page/202111/1238218.shtml. Accessed on 05 April 2022.

[18] Ibid.

[19]PK Mallick, "Research and Development in Cyber Domain and Indian Perspective", *Vivekananda International Foundation*, September 2019. Available at https://www.vifindia.org/paper/2019/september/05/research-and-development-in-cyber-domain-and-indian-perspective . Accessed on 06 April 2022.

[20] AK Singh and Balraj Nagal (eds), Military Strategy for India in the 21st Century, New Delhi: KW Publishers, 2019. ISBN 978-9387324817, Ch-8.

[21] Caren Kaplan, "Air power's visual legacy: Operation Orchard and Aerial Reconnaissance Imagery as Ruses de Guerre", *Critical Military Studies*, 05 November 2014, Available at https://www.tandfonline.com/doi/full/10.1080/23337486.2014.974949. Accessed on 05 April 2022.

[22] PK Mallick, "Professional Military Education: An Indian Experience", *Vivekananda International Foundation*, 22 November 2017. Available at https://www.vifindia.org/occasionalpaper/2017/november/22/professional-military-education-an-indian-experience.Accessed on 05 April 2022.

[23] PK Mallick, "Cyber Security in India Present Status", *Vivekananda International Foundation*, October 2017. Available at https://www.vifindia.org/issuebrief/2017/octobe/30/cyber-security-in-india-present-status. Accessed on 05 April 2022.

[24] Bill Roche, "Latest Hack the Army bug bounty wraps up, increasing network security", 10 June 2021. Available athttps://www.army.mil/article/247381/latest_hack_the_army_bug_bounty_wraps_up_increasing_network_security. Accessed on 05 April 2022.

[25] JD Work, "China Flaunts Its Offensive Cyber Power", *War on the Rocks*, 22 October 2021, https://warontherocks.com/2021/10/china-flaunts-its-offensive-cyber-power/. Accessed on 05 April 2022.

[26] N.1.

[27] Aditi Agrawal, "India's Cybersecurity Strategy Policy in 2020: Says National Cybersecurity Coordinator Rajesh Pant", *Medianama*, 22 June 2019. Available at https://www.medianama.com/2019/06/223-indias-cybersecurity-strategy-policy-in-2020-says-national-cybersecurity-coordinator-rajesh-pant. Accessed on 05 April 2022.

[28] PK Mallick, "Cyber Attack on Kudankulam Nuclear Power Plant – A Wake Up Call", *Vivekananda International Foundation*, December 2019, Available at https://www.vifindia.org/paper/2019/december/18/cyber-attack-on-kudankulam-nuclear-power-plant. Accessed on 05 April 2022.

The views expressed and suggestions made in the article are solely of the author in his personal capacity and do not have any official endorsement. Attributability of the contents lies purely with author.

CENTRE FOR LAND WARFARE STUDIES (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Tel.: +91-11-25691308, Fax: +91-11-25692347, CLAWS Army No. 33098; Email: landwarfare@gmail.com
Website: www.claws.in