CENTRE FOR LAND WARFARE STUDIES

ISSUE BRIEF

No. 289 May 2021

Safeguarding Critical Information Infrastructure in the Information Domain

Colonel Gaurav Gupta is currently a Senior Fellow at CLAWS. He is an alumnus of the National Defence Academy. He was commissioned into the Corps of Signals in Dec 1992. He has served in various appointments in the field of Telecomm and IT in all terrains of Indian Army. The officer also served at Army HQs in DGIS and at Army War College, Mhow, where he was responsible for management of IT and Cyber Security. His areas of interests are IT, Cyber Security and Information Warfare.

"If we can imagine it, we can achieve it"

—William Arthur Ward

Abstract

As we move towards a data driven economy, there is an exponential increase in critical information infrastructure(CII). The entire digital ecosystem of CII in India is imported and is vulnerable to backdoors, malwares and cyber attacks. Startup India, Make in India and Digital India are required to promote an indigenised ecosystem for all of our CII. In the interim, there are certain security steps that are required to be undertaken by all organisations to protect their CII.

Key Points

- As we march towards the digital era, there is a shift in the nature of warfare.
- CII created by various organisations are vulnerable to cyber attacks.
- Our adversaries are pushing Trojans and Malwares through cheap IT infrastructure into the CII of India.
- India needs to strike a balance between digital expansion and risk of likely attack on CII.
- India needs to organise and prepare multi-dimensional doctrines and include cyber attacks.
- India should enhance the scope of CII and take steps to mitigate trojans and malwares through thorough testing in the short term and indigenised IT infrastructure in the long term.

Introduction

The onset of information age has brought about a paradigm shift in the nature of warfare, which,

until now, was restricted to the traditional land, air, sea and space domains, has now been extended to the information domain also. Information warfare is the action taken during peace, crisis and conflict with an aim to achieve information dominance over the adversary by degrading its information infrastructure and protecting one's own. Warfare in information domain is a 'blue ocean' as international bodies are yet to identify the complete nature of threats that can possibly be posed by information warfare. While some countries have gained adequate expertise in this dimension of warfare, most of the nations are still groping in the dark about this 'unidentified ghost'. In the absence of a formalised framework, low cost and blurred boundaries, the countries are continuously fighting information warfare 24x7 and year round. This warfare is invisible to the outside world and the effects of the information warfare are often downplayed by both the attacker and the affected organisation.

The Dtrack malware attack on the CII of Kudankulam Nuclear Power Plant (KKNPP) in 2019 is one such example of information warfare. KKNPP officials initially denied the attack but later admitted to a breach in their administrative network. The malware entered the network as a user from KKNPP had connected malware infected computer. According to some agencies, the attack on the KKNPP originated in North Korea whereby the attackers managed to breach and manipulate the nuclear facility's heavily protected industrial controls.[1] VirusTotal, a virus scanning website owned by Google's parent company—Alphabet, had indicated that a large amount of data from KKNPP's administrative network was stolen. If this is true, then subsequent attacks on the nuclear power plant could target its CII more effectively. Most recently, cyber attacks on India's power infrastructure by RedEcho — an actor group with China links — was frequent especially during India-China Ladakh standoff and its intrusive infrastructure is still active even after military de-escalation in Ladakh's Pangong Tso area.[2] Power outage in Mumbai in October 2020 can be considered as a warning that, retaliatory action could be in other domains of warfare also. Targeting the Indian energy sector offers limited economic espionage opportunities to our adversaries, but at the same time, facilitates the gathering of future operational activities and pre-positioning of destructive malware as a warning/ show of strength to disturb the Indian population. Maharashtra cyber department submitted a provisional report to the Maharashtra Government on the massive grid failure which hit Mumbai and surrounding areas on October 12 last year.[3] The report confirmed the malware attack on the electric grid of Mumbai from an entity outside India and also highlighted that about

14 Trojan Horses and 8 GB of unaccounted data was found in the system, which as per investigation was installed in Maharashtra State Electricity Board (MSEB) systems by 'unverified sources'. India as a rising power is inching towards a data driven economy. Hence, it needs to protect its CII to prevent any breach of information or make the CII dysfunctional during peace or war, as per our need.

Critical Information Infrastructures

CII are information systems that are so vital to a nation that their incapacity or destruction would have a debilitating effect on national security, the economy, or public health and safety.[4] CII commonly comprises of infrastructure which are essential for the functioning, maintenance and resilience of vital societal functions that protect the safety, security, economic or social well-being of people, and the disruption or destruction of which would result in equally significant impact. As nations globally continue to develop and grow, critical services are becoming increasingly complex and interconnected, and posing consequential challenges to their security. Another term which loosely refers to critical infrastructure is 'strategic asset'. Strategic asset is a relatively new term that refers to the fast forward development of economic globalisation in the 20th century and also refers to a new wave of economic conflict or trade war that has been 'unleashed' by the change in economic power centres which facilitates the reorganisation of economic, political and strategic alliances connected with it. Strategic Assets can be defined as any tangible or intangible asset of substantial value in a given economy, state, or nation. Today, India is embroiled in a conflict with stateless/ proxy enemies who will resort to unprecedented tactics, both kinetic and non-kinetic (hybrid warfare), to disrupt the country's stability and eventually achieve their extreme goals.

Threats to CII

The most common threats posed to CII is by means of cyber attacks by using malicious codes to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cyber crimes, such as information and identity theft. The computer programs are designed to identify equipment vulnerabilities, which could be inadvertent or deliberate. These vulnerabilities can exist at the operating system (OS) or at application software level or could also be at the chip level on firmware. Examples of cyber attacks, aimed at CII facility includes malicious computer programs called Flame and Stuxnet, which were reportedly created by the US and Israel for cyber espionage and sabotage of critical nuclear industrial facilities in Iran. Such special vulnerabilities make CII easy targets for cyber attacks, followed by 'Zero-

-day exploits' that secretly insert malicious codes into CII for espionage and cyber sabotage. Thereafter, hackers and cyber experts may knowingly or unknowingly sell these 'zero-day exploits' and malicious codes to extremists or terrorist groups. Governments and businesses may also use the stealth features of 'zero-day exploit' code to insert malicious cyber codes into CII of 'suspicious' businesses or nations that may later be activated for cyber sabotage or be used as a pre-emptive cyber strike to enforce unilateral policy decisions and weaken the adversary's CII.[5]

The extensive integration of Information and Communication Technology (ICT) for a Nation's defence, has introduced new vulnerabilities and created new categories of risks in the CII landscape. The outbreak of the Covid-19 pandemic has further intensified the exposure to cyber risks as there is an unparalleled increase in the usage of internet. A recent assessment revealed that, the ongoing Covid-19 pandemic has seen not only a general increase in malicious activities but also a shift of attacks from small businesses to critical infrastructure and government networks. As we move forward to the wide adoption of this new paradigm, ICTs are bound to become even more integral for increasing the supply and reach of critical services. The usage of IoT devices, together with 5G technology, is becoming pervasive in many verticals with an estimated 41.6 billion connected devices around the world by 2025. Cloud solutions have also become critical to operations with 94% of businesses worldwide relying on them. Artificial Intelligence, given the growing availability and preponderance of data, will find unprecedented applications in several domains including critical sectors for national security, well-being, and economy. According to the World Economic Forum, we are now entering a new era referred to as 'Globalisation 4.0', with digital assets and services constituting the backbone of the economy.

It is important to understand that, although it is not easy to compromise the critical systems electronically from outside, but the possibility of physical human access to the portable devices are always high and equally threatening. As per Nuclear Threat Initiative, targeted attacks go beyond network connections and generally leverages 'witting or unwitting humans, or a long and difficult-to-defend supply chain, to deliver the attack'.

Cyber Attacks on CII: Around the World

The very first known cyber attack on a nuclear plant was reported in 1992 when rogue programmer Oleg Savchuk deliberately infected the computer system of a plant in Lithuania with a virus.[6] Savchuk was later arrested and became a precautionary

footnote in the history of nuclear security. In March 2007, engineers at the Idaho National Lab showed how 21 lines of computer code could cripple a huge generator. It was through this jaw-dropping experiment, known as '*Aurora'*,that some energy industry officials accepted that digital tools are capable of physical destruction. Two years later, the destructive potential shown in '*Aurora'* became a reality.

The much talked about '*Stuxnet'* attack in 2009 - a formidable computer worm - was installed into Iran's Natanz enrichment facility, destroying about 1,000 centrifuges. Another playground for hackers was the Ukrainian power grid. In December 2015, a cyber attack on Ukrainian power grid plunged 2,25,000 people in darkness. The head of US Cyber Command, in March 2021 testified that the organisation had conducted more than two dozen operations to confront foreign threats ahead of the 2020 US elections, including eleven forward hunt operations in nine different countries.

In the same month, a group of Chinese hackers used Facebook to send malicious links to Uyghur activists, journalists, and dissidents located abroad. The Indian Computer Emergency Response Team (CERT-In) found evidence of Chinese hackers conducting a cyber espionage campaign against the Indian transportation sector. Similarly, Polish security services announced that suspected Russian hackers briefly took over the websites of Poland's National Atomic Energy Agency and Health Ministry to spread false alerts of a non-existent radioactive threat. Both Russian and Chinese intelligence services targeted the European Medicines Agency in 2020, in unrelated campaigns, and stole documents related to Covid-19 vaccines and medicines.[7] In March 2021, Ukraine's State Security Service announced that, it has prevented a large-scale attack by Russian Federal Security Service hackers attempting to gain access to classified government data. Lithuania's State Security Department declared that Russian hackers had targeted top Lithuanian officials in 2020 and used the country's IT infrastructure to carry out attacks against organisations involved in developing Covid-19 vaccines. In the same month, suspected Iranian hackers targeted government agencies, academia, and the tourism industry in Azerbaijan, Bahrain, Israel, Saudi Arabia, and the UAE as part of a cyber espionage campaign. Chinese Government hackers targeted Microsoft enterprise' email software to steal data from over 30,000 organisations around the world, including government agencies, legislative bodies, law firms, defence contractors, infectious disease researchers, and policy think tanks.

CII in India and Defence

The National Critical Information Infrastructure Protection Centre (NCIIPC) has broadly identified six 'critical sectors' whose CII is vulnerable and needs to be protected– power and energy, banking, financial services and insurance, telecom, transport, government, strategic and public enterprises. Based on above, some of the CII which need to be protected are as follows:

- ***Power & Energy.*** Nuclear power plants and reactor networks; hydel and thermal power project networks and electric grids.
- ***Finance.*** Information Infrastructure of banks, financial services and insurance companies.
- ***Telecom.*** Data centres, exchanges, switching equipment, long distance connectivity equipment.
- ***Transport.*** Infrastructure involved in management of transportation especially railways.
- ***Government.*** Management information systems and decision support systems.
- ***Strategic & Public Enterprises.*** Public services and enterprises working in strategic areas, important ministries, embassies, industrial houses etc.

The CII of Defence are either islolated/ air-gapped, or are the ones which are connected over public networks and are used for only unclass and less important communication. The CII in Defence services are Command and Control Networks, data centres at Divisional Headquarters and above, Sensor to Shooter Networks; Battlefield Surveillance Systems, Defence Communication Networks interlinking the three services, Satellite Communications forming important backbone, Repair and Maintenance networks, Supply Chain networks and Data Centres where large amount of data are stored and processed. The Army Wide Area Network (AWAN), which is used for secure mail, also falls under this category. Air Force Network which is used for ground to air communication is an important CII which works on wireless mode and hence is most vulnerable.

Capabilities: India's Adversaries

China and Pakistan are developing cyber warfare capabilities to deter a physically and technologically superior military adversary. In the last decade, China has made considerable progress in developing its cyber warfare capabilities by revising its policies, restructuring organisations, building human expertise and raising new

establishments. Cyber incidents against India have been occurring at regular intervals, especially in the last decade. This has been acknowledged at highest levels like by the former National Security Advisor of India, Mr MK Narayanan.[8] As per a report by the US Cyber Security Company named 'FireEye', China has been spying on the Indian Government and businesses for more than a decade without India being aware of it, and there is more to come.[9] The consistency of incidents indicates a dedicated India-targeted espionage system on Indian CII purportedly originating in China. Although, so far no Indian cyber intrusion investigation reports are available in the open domain, but investigation reports by foreign investigators identifies India as one of the victims of cyber breach, with intrusions attributed to China.[10]

China has been making steady progress in acquiring cyber warfare capabilities in terms of organisations, policies and expertise. In 2015, PLA decided to raise the Strategic Support Force (PLASSF) which is seen as the fifth service and not just a branch of PLA. China uses the term 'Integrated Network Electronic Warfare' to describe an integrated approach to information warfare operations and includes electronic warfare, computer network warfare and psychological operations. China aims to become a global internet superpower and have an impregnable cyber security system by 2025. Therefore, it is reasonable to assume that China would develop its cyber warfare capabilities in equal measure.

China has a 'whole of nation' approach for conducting cyber warfare and includes patriotic hackers and university students as cyber warriors along with the PLA. The PLA sees cyber warfare as a first-strike option to preclude the requirement of conventional military operations, rather than a force multiplier during conventional operations. China has elevated cyber warfare to a strategic level by adding cyber attacks on satellites or space warfare, as part of its offensive operations. It is logical to assume that PLA intends to conduct concurrent operations in all five domains vis. land, sea, air, space and cyber. China is involved in continuous cyber reconnaissance to identify weak spots and glean information which can be exploited during war. It have exported 'cheap undervalued' computers/laptops, modems and telecommunication hardware in enemy country's networks (embedded with virus, trojans, malware etc.), capable of gleaning information on regular basis that may be exploited later in wartime to cripple the nation.[11]

Important Cyber Organisations in China

The major cyber organisations of China comprises of PLA's 3rd Department which is responsible for Signal Intelligence, Computer Network Defence, and Computer Network Exploitation. It also involves PLA's 4th Department which is responsible for Electronic Warfare (EW), Computer Network Attack and Integrated Network Electronic Warfare– IW militia units, strategic support bases were established in the year 2015 with an aim to integrate intelligence, communication, electronic warfare with cyber warfare to create an integrated information warfare force. If reports are to be believed, then in China hackers are recruited under the guise of software engineers and security experts. Civil telecommunication companies are part of China's cyber espionage system. Firms like Huawei and ZTE are closely associated with the government and receives preferential funding for R&D and predatory trading.[12]

India is also in the line of fire of Pakistan backed cyber attacks over the last few years. After the abrogation of article 370, cyber attacks on Indian institutions have increased and in many cases the attackers openly acknowledged allegiance to Pakistan.[13] Currently, 'Digital India' has come under the radar and is continuously facing threat from state-sponsored cyber terrorists based in North Korea, Pakistan and China. CYFIRMA, a Singapore based cyber intel firm in its latest report - *India Threat Landscape 2020/21* - highlighted multiple cyber hacking groups who have been taking a keen interest in India. The report has specially named four hacking groups suspected to be sponsored by China, Pakistan and North Korea. The report further suggests that, the hacking groups are eying to especially target government agencies, discoms and news organisations by defacing websites using a weakness in web applications, data exfiltration using specialised malware, denial of service, impersonating companies' website and launching malicious phishing campaigns to attack Digital India.[14]

Implications for India

'Penetration testing' by own agencies have divulged that Indian networks/computers are flooded with virus, trojans etc. This includes the hardware of important and critical organisations like the DRDO, National Thermal Power Corporation, Police Force, Public Works Department, Finance, Space, Ministries etc. Chinese firms like ZTE and Huawei have been underbidding in the tendering process, both in India and outside, and

becoming the lowest bidder. To do this, they probably get the financial support from state owned banks in China. As a result, a number of computers and telecommunication hardwares used in the Indian telecommunication networks, government departments, railway networks, power networks etc. are of Chinese origin and are (in all likelihood) infested with virus, worms and trojans. China is also collecting all the critical information about our networks/systems which may be used to disrupt them at a critical time. China is the major source of silicon integrated microchips (being used in all electronic devices) for all manufacturers across the globe, including American and European brands and therefore, the possibility of 'undesired alterations' in these integrated circuits cannot be completely ruled out. Consequently, China's intelligence collection and system vulnerability identification would give the PLA a tremendous advantage during a confrontational situation with India.

Way back in August 2012, when the northern power grid failed, cyber analysts suspected 'China-Pak' nexus for the failure. In 2015, in a letter to the NSA, Ajit Doval, Indian Electrical and Electronics Manufacturers' Association (IEEMA), suggested a complete ban on the use of Chinese equipment in the Indian power sector citing security concerns.[15] According to IEEMA's database, in order to make power distribution network efficient, many cities in India have awarded the contract to deploy Supervisory Control and Data Acquisition system (SCADA) to Chinese firms. This might be of great concern for the power infrastructure. Similarly, other critical infrastructures like railways, irrigation etc. which are dependent on telecommunication/ IT hardware and SCADA systems are also equally at risk.[16]

The rapid pace of digitalisation poses new national security risks for countries like India with over 700 million internet users. The 'multilayered digital ecosystem' comprising of infrastructure, devices and applications is complex where security threats evolve at a breakneck pace. This makes it all the more difficult for states to develop an effective response mechanism to individual or organisational security threats.[17] The news about availability of personal ADHAAR data of Indian citizens at a mere Rs. 500 should be a major wake-up call for the government. [18] India has various organisations dealing with cyber issues like the National Technical Research Organisation (NTRO), National Critical Information Infrastructure Protection Centre (NCIIPC) etc. However, they are not integrated with each other and operate independently. There is a need to have a single policy level agency and a single execution level agency, which can coordinate at national level, so as to derive maximum dividends out of the efforts being put in. The total strength of cyber security experts deployed in various government agencies is

merely 550 compared to more than a lakh in China, 91,000 in USA and 7000 in Russia. There is, thus, a dire need to hire cyber security experts by the government and exploit their talent to protect CII as well as acquire cyber offensive capabilities.

The Enemy Within

The Fissile Materials Working Group's recent report mentions that organisations must transfer data in and out of their operational networks for a variety of reasons, and these are all pathways for attacks. [19] New data have to enter even an air-gapped operational network to update its software and hardware. The Stuxnet attack penetrated Iran's air-gapped Natanz uranium enrichment facility by means of data despite the fact that, the facility was well defended and isolated from the Internet. If an organisation allows flash drives and USB keys to enter and exit their operational technology network, then the firewalls or switches will fail to stop them. Organisations also allow external hardwares like laptops, mobile phones etc. to enter and exit their operational networks as part of facility and operations' vendor maintenance. Commercial 'off-the-shelf software', that an organisation does not really own, can also be infected.

Safeguarding CII

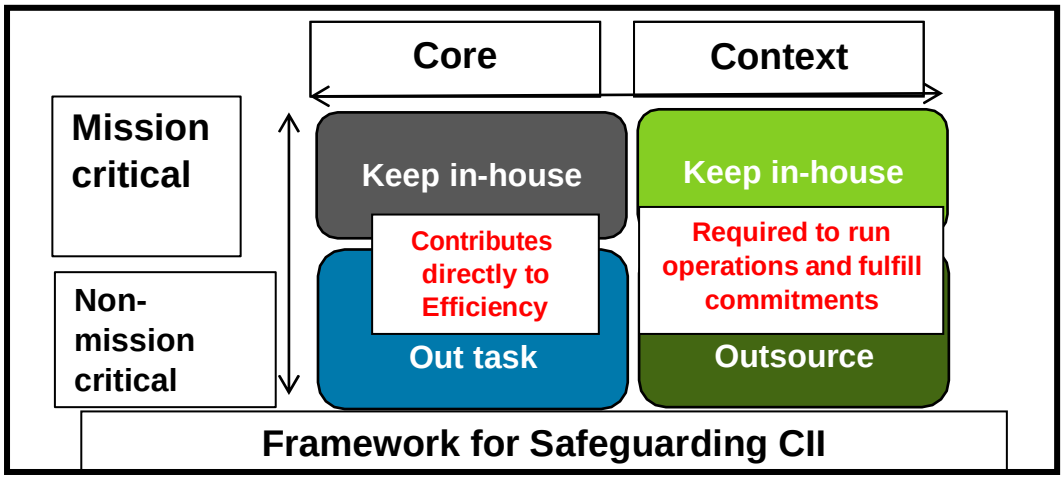
With such strong adversaries, India needs to take strong steps to prevent, re-mediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. CERT-In coordinates efforts on cyber security issues and is tasked with responding to cyber attacks, while the National Technical Research Organisation (NTRO) is the elite technical intelligence agency. Depending on the intensity of risks, actions could include changes in tactics, techniques, or procedures, adding redundancy, selection of another asset, isolation or hardening, guarding etc. The need for effective cyber security strategies, policies and activities specific to each CII, thus becomes evident. However, designing an effective protective measure for CII is challenging as several factors have to be taken into consideration. It is important to adopt inter- sectoral approaches aimed at increasing the maturity of cyber security strategies in a coordinated manner. CII which traditionally had been purely government-owned has now evolved into a multi-stakeholder environment which includes government agencies, privately owned companies, academia, defence agencies, and international organisations. Hence, there is a need to ensure cooperation and dialogue between different actors to implement an all -

-encompassing cyber security posture in a coordinated manner.

CII, at the national level and in the defence sector, needs to be safeguarded from unauthorised access, modification, use, disclosure, disruption, incapacitation or distraction through coherent coordination and synergy among all the stakeholders. In addition, any framework to safeguard the CII must address the risk of backdoors leading to loss of data security, technology denial in case of an attack on CII. It should also consider the cost associated with proprietary OS or cost of *ab initio* development. Deployment on specialised devices, for which no standard proprietary OS is available, is also essential. A suggested framework for building up of a suitable ecosystem for safeguarding CII against cyber attacks explained below:-

- Mission critical areas and context Information Infrastructures are fundamental key building blocks, which should be kept in-house in terms of development, deployment and overall management as the risks associated with them, due to shortfall in performance in the event of a cyber attack, are huge. In terms of CII, it implies that the mission critical CII must be indigenous in terms of hardware, software, firmware and all associated peripherals. Such CII must continue to be isolated and air-gapped despite indigenous ecosystem.
- Out-tasking of non-mission critical and core information infrastructure will be a safe choice.
- Outsourcing of non-mission critical and context CII can be resorted to with the help of strict checks and balances.

Figure 1: Framework for safeguarding CII



Source: Annotated by the Author

Following important aspects must be worked upon before adopting this framework:

- ***Scope.*** Determine scope of each CII for risk management. Identify institutions for audit, validation and testing of new technological development.
- ***Policy Making.*** A policy established and carried out by any oraganisation, involves several stages from inception to conclusion vis. formulation, adoption, implementation, evaluation, and termination.

The framework mentioned above can be used to evaluate the CII of all important organisations including defence, all the critical ministries, banking networks, nuclear and thermal power plants, rail and air networks etc. In the defence services the above framework can be applied as follows:-

- ***Mission CII.*** This CII must be developed, deployed and managed in-house. DRDO and institutions like CDAC can play a huge role in this. The embedded firmware and mission specific application software needs to be developed in-house through either DRDO or CDAC. Role of DRDO needs to be defined and instead of assembling, DRDO labs need to come up with products which are completely indigenous.

- ***Non- Mission CII.*** The non-mission CII needs to be developed through PPP with an aim to be indigenous in long term.

Recommendations and Way Ahead

CII plays an important role in the growth of any nation or organisation. At the same time, CII continues to be extremely vulnerable to cyber attacks. To protect CII from cyber attacks, well defined strategies and plans need to be formulated. Some of the recommendations for the national level and defence are as follows:-

- ***Focus.*** Till now, more focus was on the finance sector. There is a need to shift focus to other sectors like power, especially when power sector has an integrated National Power Grid which is the backbone of India. Defence, transportation and important Government institutions also need to be part of CII.

- ***Organisation.*** At present, there is no formal organisation at the ministerial level or at the organisational level. There is a need for a dedicated organisation with a nodal officer, to respond to attack on CII immediately, else harm will be irreversible. Such organisation must be proactive in protection of its CII. Every organisation must work out SOPs and protocols for such eventualities. Every formation headquarters must nominate a nodal officer who is capable of handling the CII proactively.

- ***Multi-dimensional Doctrine.*** Attack on CII is expected to be supported by warfare in other domains simultaneously, hence planning needs to be done keeping in mind multi-dimension operations. At present, most of the doctrines are formulated in isolation. The doctrines need to be multi-dimensional. For example, a nuclear-cyber doctrine can replace the existing nuclear doctrine incorporating the multi-dimensional aspects of both the domains of warfare. The Indian Army/ defence doctrine needs to be multi- dimensional to include cyber warfare as an alternative to the offensive in case of an incident like Galwan valley standoff.

- ***Enhance Scope.*** NCIICP has defined limited areas for protection of CII. The scope of CII needs to be expanded to include private sector also as most of India's telecommunication and IT infrastructure is privatised. Commercial companies till now were out of the ambit of CII. However, at present, commercial companies have equal stakes in CII if PPP model for development is followed. Therefore, there is a need to include commercial companies into the ambit of CII.

- ***Software and Firmware Testing.*** India does not have any Software Testing and Certifying lab. Therefore, DRDO, CDAC, IITs must be tasked to create such software testing labs to ensure that all imported CII hardware is tested for embedded malwares. The capability of these labs need to be for all COTS as well as customised softwares. These organisations should also establish research facilities in the field of IT and CII.

- ***Constant Review.*** There is a need to review software patches released by developers of OS as well as other softwares which are part of integrated systems.

- ***Indigenisation.*** Indigenisation of all the hardware and integrated systems in the long term is inevitable if India wants to be a data driven economy. All public sector undertakings must work on a well-defined roadmap towards indigenisation of the entire ecosystem of CII.

- ***Multi- domain Expertise.*** Training to the individuals handling the CII, need to ensure that the individuals are 'proactive' and 'not reactive' in handling CII. Multi- domain expertise need to be developed in all organisations. Sense of Cyber hygiene in all the individuals handling CII needs to be ensured.

- ***Interim Security Architecture.*** End-to-end security architecture for CII needs to be planned and catered for in the interim until the entire ecosystem of CII is indigenous.

- ***Offensive Operations on CII.*** The Government must consider attacking the adversary's CII as a retaliatory action.

- ***Common Interest Groups (CIG).*** Make CIG comprising young professionals to develop expertise for offensive CII operations on the adversary.

- ***Coordination.*** Improve coordination among various agencies like NCCC, NTRO, DCA, and all the ministries where there is CII through a common umbrella organisation.

- ***Indigenous OS.*** At present, fully indigenous OS is a distant dream. Bharat Operating System Software (BOSS) has been developed by CDAC which is partially indigenous. Same should be standardised for all internet PCs in all government organisations and all CII.

- ***Make in India and Digital India***. For a data driven economy, there is a need to push indigenised digital infrastructure. The concept should not be revolutionary in approach but evolutionary that is 'Build a little, field a little'. The beginning can be made by developing firmware.

Conclusion

CII is the most important element of our networked environment. India is moving fast on the road to digital India, including digital economy, in a big way. India should prepare for futuristic war in cyber domain and protect its CII. With the society becoming increasingly dependent on automation and computers for day-to-day work, and concepts like Artificial Intelligence (AI) and Internet of Things (IoT) knocking at our doors, CII is vulnerable to information warfare attacks. Further, as time progresses, our adversaries will develop greater expertise and sophistication in attack on CII. Unless India takes concrete steps to strengthen its cyber security posture and develop cyber warfare capabilities to match that of China, we may be facing a grim situation, sooner or later. Individuals, corporations and governments, all need to share equal responsibility and come together in securing CII. The integration of private sector, law enforcement agencies, intelligence agencies and government organisations is inevitable for India especially when China is a neighbour.

End Notes

[1]Debak Das, "An Indian nuclear power plant suffered a cyberattack. Here's what you need to know", The Washington Post, 04 November 2019. Accessible at https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/. Accessed on 01 May 2021.

[2] Utpal Bhaskar, "India may raise Chinese hack rish at global forums", *Livemint*, updated on 23 March 2021. Accessible at https://www.livemint.com/news/india/india-may-raise-chinese-hack-risk-at-global-forums-11616436387265.html. Accessed on 01 May 2021.

[3] Saurabh Tewari, "China's Cyber Warfare Capabilities" , *USI*, April 2019-June 2019. Accessible at https://usiofindia.org/publication/usi-journal/chinas-cyber-warfare-capabilities/. Accessed on 02 May 2021.

[4]"Critical Information Infrastructure",*CIPedia* . Accessible at https://websites.fraunhofer.de/CIPedia/index.php/Critical_Information_Infrastructure. Accessed on 04 May 2021.

[5] "What is a Zero-Day Exploit?", *FIREEYE*. Accessible at https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html. Accessed on 04 May 2021.

[6] Akshay Rahar, "Nuclear Power Plants: Vulnerability to Cyber Attacks", *CLAWS Web Focus Article*, 31 March 2020. Accessible at https://www.claws.in/nuclear-power-plants-vulnerability-to-cyber-attacks/. Accessed on 05 May 2021.

[7]Reuters, "Russian, Chinese hackers targeted Europe drug regulator", The Economic Times, updated on 06 March 2021. Accessible at https://economictimes.indiatimes.com/news/international/world-news/russian-chinese-hackers-targeted-europe-drug-regulator/articleshow/81366907.cms?from=mdr. Accessed on 05 May 2021.

[8]Darshan Saval, "India vs China: Research paper says Indian infrastructure highly vulnerable to Chinese cyber attacks", *Android Rookies*, 18 June 2020. Accessible at https://androidrookies.com/india-vs-china-research-paper-says-indian-infrastructure-highly-vulnerable- to-chinese-cyber-attacks/. Accessed on 05 May 2021.

[9]Reuters, "Chinese hackers spied on India for a decade: FireEye report", *The Indian Express*, updated on 13 April 2015. Accessible at https://indianexpress.com/article/technology/technology-others/chinese-hackers-spied-on-india-for-10-years-says-report-by-fireeye/. Accessed on 06 May 2021.

[10]N.7.

[11]Ibid.

[12]IANS, "Chinese hackers hit 30,000 US organisations in new attack", *The Economic Times*, 06 March 2021. Accessible at https://economictimes.indiatimes.com/news/international/world-news/chinese-hackers-hit-30000-us-organisations-in-new-attack/articleshow/81361240.cms?from=mdr". Accessed on 06 May 2021.

[13]Abhijit Ahaskar, "China-backed hackers planning attack on Indian govt,industry", *Livemint*, updated on 19 June 2020. Accessible at https://www.livemint.com/news/india/china-backed-hackers-planning-attack-on-indian-govt-industry-report-11592555270970.html. Accessed on 07 May 2021.

[14] Mohit Sharma, "Digital India under attack from Pak-China backed cyber terrorists: Report", *Times Now*, updated on 24 November 2020. Accessible at https://www.timesnownews.com/india/article/digital-india-under-attack-from-pak-china-backed-cyber-terrorists-report/686069. Accessed on 07 May 2021.

[15]Shreya Jai and Saurabhi Agarwal, "Indian power firms want ban on Chinese equipment", Business Standard, updated on 04 April 2015. Accessible at https://www.business-standard.com/article/economy-policy/indian-power-firms-want-ban-on-chinese-equipment-115040400010_1.html. Accessed on 08 May 2021.

[16]N.13.

[17] Utsav Mittal, "A New Framework for a Secure Digital India", *ORF Issue Brief*, Issue no 422 November 2020. Accessible at https://www.orfonline.org/research/a-new-framework-for-a-secure-digital-india/. Accessed on 08 May 2021.

[18]Rachna Khaira, "Rs 500, 10 minutes, and you have access to billion Aashaar details" , The Tribune, updated on 05 January 2018. Accessible at https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361. Accessed on 05 January 2018.

[19]N.6.