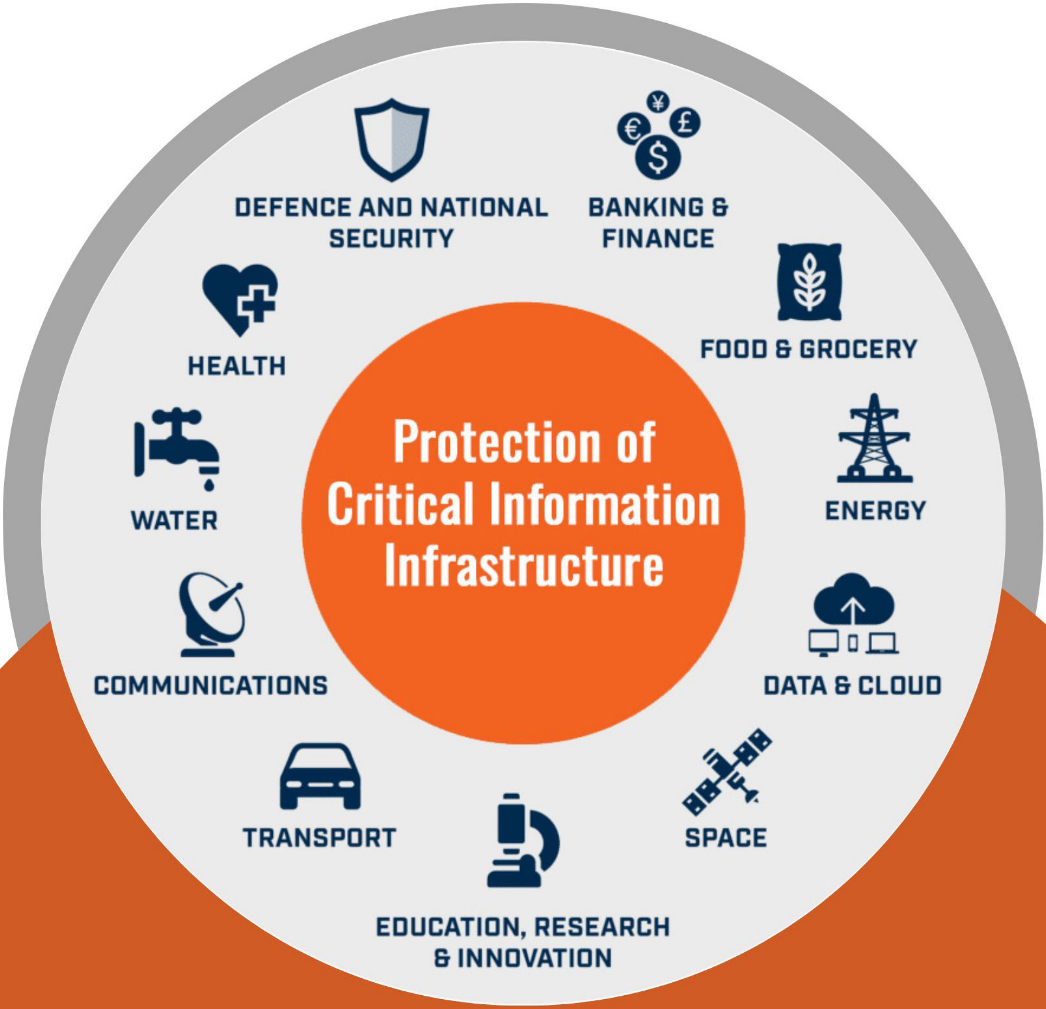
Vivekananda
International
Foundation



Protection of Critical Information Infrastructure

Maj Gen P K Mallick, VSM (Retd)

VIF Paper

Protection of Critical Information Infrastructure

Maj Gen P K Mallick, VSM (Retd)

Published in 2024 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:

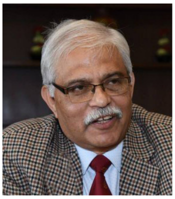
Twitter | @vifindia
Facebook | /vifindia

ISBN: 978-93-91498-97-9

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 The author certifies that the article/paper is original in content, unpublished and it has not been submitted for publication/web upload elsewhere, and that the facts and figures quoted are duly referenced, as needed, and are believed to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

CONTENTS

ABOUT THE AUTHOR



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.

1. INTRODUCTION

Today a rapid transformation is underway in the cyber domain. Our digital and physical worlds are increasingly getting connected. Growing access to high-speed Internet and the explosion of next-generation telecommunications networks are connecting people and systems around the world. Innovations in the fields of Artificial Intelligence (AI), Quantum Information Science (QIS) and micro-electronics are revolutionising the advanced computing landscape.

Critical information infrastructure (CII) refers to the systems and assets that are essential for the functioning of a society and economy. Protecting CII is vital. Any disruption or compromise of these systems can have far-reaching consequences including economic losses, disruption of essential services, public safety and threats to national security. Due to India's growing digital economy and increasing reliance on Information and Communication Technology (ICT), protecting CII is of utmost importance to the country. Critical Information Infrastructures across the country are increasingly under attack from state and non-state actors. Ransomware groups have built a business model around targeting organisations like hospitals, ports etc, tat are ill-equipped to defend themselves.

Protecting CII needs a multi-faceted approach. It requires implementation of robust cybersecurity measures, development of incident response plans, regular security audits and collaboration between the government, the private sector and other stakeholders to share threat intelligence and best practices. To mitigate the risks posed by cyber threats and ensure the continued functioning of essential services, protection of CII must be given the highest priority.

Cyber threats in India are constantly evolving. Some prominent trends are: *Targeted Attacks, Ransomware, Supply Chain Exploitation, Commercial Spyware, Emerging Technologies* like AI, *Cloud Computing, Internet of Things (IoT)* and *Social Engineering*.

In India there is the deficiency of awareness and preparedness among organisations and individuals regarding cyber security. Many businesses and government agencies do not have robust cybersecurity measures in place, making them vulnerable to cyber attacks. Rapid pace of technological advancement has outpaced the development of cybersecurity skills and capabilities, leading to a dearth of skilled cybersecurity professionals.

The Government of Indian has recognises the gravity of cybersecurity threats and several initiatives have been implemented. Some of these are legal frameworks like the *Information Technology Act (2000)* and the upcoming *Data Protection Bill*, besides the activation of Indian Computer Emergency Response Team (CERT-In), National Critical Information Infrastructure Protection Centre (NCIIPC), Public-Private Partnerships, Cybersecurity Awareness Programs, Training etc. In spite of these efforts, many challenges remain including enforcement mechanisms, resource constraints, international cooperation etc. There is a need for modern and nimble regulatory frameworks for CIIP. Two fundamental shifts in how we allocate roles, responsibilities and resources for CIIP are warranted:-

- By rebalancing the responsibility to defend cyberspace away from end users and to the most capable and best-positioned actors in the public and private sectors;
- Realigning incentives to favour long-term investments in future resilience.

2. CRITICAL INFRASTRUCTURE (CI) & CRITICAL INFORMATION INFRASTRUCTURE (CII)

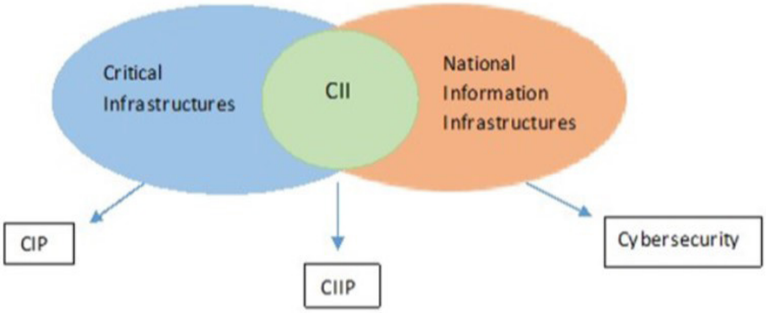
CI refers to key infrastructure which are employed for the supply of essential services such as energy, drinking water, government, finance, power, communications and transportation. CIs are becoming increasingly complex and interconnected. The all-embracing integration of ICT has introduced new vulnerabilities and created new categories of risks in the CI landscape. Traditionally, CI had been purely government-owned. It has now grown into a multi-stakeholder environment which includes government agencies, private sector companies, academia, defence agencies and international organisations.

The term 'Critical Information Infrastructure' (CII) appeared in the early 2000s. It refers to the "*material and digital assets, networks, services, and installations that, if disrupted or destroyed, would have a serious impact on the health, security, or economic well-being of citizens and the efficient functioning of a country's government*". Although the concept of CII has been widely employed at a governance and academia level, there is still little agreement regarding a widely accepted definition and a distinction with the broader category of Critical National Infrastructure (CNI).

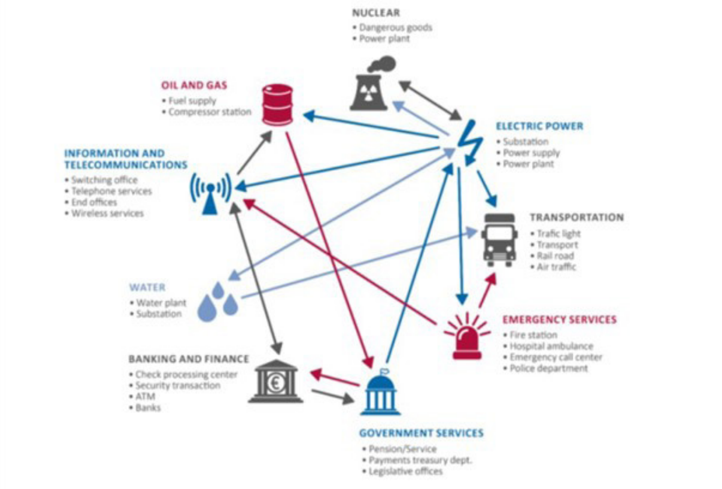
CI comprises the physical and virtual assets and systems so vital to the nation that their incapacity or destruction would have a debilitating impact on national security or safety. It is diverse and complex. It includes distributed networks, varied organisational structures, operating models, interdependent systems and governance constructs. The two concepts are firmly interconnected and recent frameworks for defending critical sectors have adopted a 'service-oriented approach', which focuses on protecting the supply of essential services against cybersecurity threats. CI is increasingly reliant on digital assets, where the exchange of data between different CIs is essential to the operation of infrastructure as well as to the supply of services. Generally, we can affirm that CI is broader than CII, but CII constitutes the backbone of CI.

As nations continue to develop and grow globally, there is the need to ensure cooperation and dialogue between the different actors to implement an all-encompassing cybersecurity posture.

3. RELATIONSHIP BETWEEN CIP, CIIP AND CYBERSECURITY



Interdependencies between different CI Sectors



Source: Duane, Petit, and Kim 2017.

Source: https://digitalregulation.org/enhancing-the-protection-and-cyber-resilience-of-critical-information-infrastructure/

Examples of CII of Different Countries

Israel. According to the Israel National Cyber Directorate (INCD), Critical Cyber Infrastructure is defined as the essential assets listed under the Laws for Regulating Security in Public Bodies, under which essential computer systems related to tele-communications, electricity, water, energy, finance, transportation, and other areas, as well as the data and confidential information handled by these systems, are subject to protection. Entities that fall under the INCD's jurisdiction include the Bank of Israel, Israel Natural Gas Lines, Energy, Infrastructures (Private Equit Infrastructure PEI), Israel National Water Co., Israel Electric Corporation, Israel Post, Ben Gurion Airport, Israel Railways, the Israel Broadcasting Authority, the Ministry of Finance, the Ministry of Transport and Road Safety, and the Civil Aviation Authority.

U.K. There are 13 National Infrastructure Sectors: Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water.

U.S. The 16 Sectors designated as critical infrastructure in USA by U.S. Cybersecurity and Infrastructure Security Agency (CISA) include: Chemical, Communications, Dams, Emergency Services, Financial Services, Government Facilities, Information Technology, Transportation Systems, Commercial Facilities, Critical Manufacturing, Defense Industrial Base, Energy, Food and Agriculture, Healthcare and Public Health, and Nuclear and Water Systems.

There are issues within these CIs. For example, the Cybersecurity and Infrastructure Security Agency (CISA) lists a wide range of industries that by no definition should be considered critical, including cosmetics, perfumes, book bindings and vehicle paint. The risk of a scratched car, it seems, is a matter of national security! Under transportation, there are critical systems such as trains, but also vanpool and rideshare services. Commercial facilities include the nation's 2.1 million office buildings and retail shopping centers as well as the entire hotel, film, broadcast and casino industries. In the U.S. many other increasingly AI-operated services are likely to come under CI, including software-defined networks, factory automation, hospitals and medical equipment, mining rigs, city buses, trains, drones and many such applications. It will be very difficult to agencies responsible to provide support to all such organisations. Priority has to be fixed for such CIs.

Regulator for CIIP

As for the identity of the regulator in the cyber field, two options exist. The first is establishing regulation by sectors, with relevant sector regulators. For example, regulation in the field of cyber defence of the health system will be determined by the Ministry of Health; the Ministry of Infrastructure will determine the regulation of water corporations, and so forth. The other option is regulation through a central regulator. USA has followed sector-specific regulators. A Sector-Specific Agency (SSA) will lead a collaborative process for CI security within each of the 16 CI sectors. Each Sector-Specific Agency is responsible for developing and implementing a Sector-specific Plan (SSP), which details the application of the National Infrastructure Protection Plan (NIPP) concepts to their sector's unique characteristics and conditions. Sector specific plans have to be updated to align with the NIPP. The National Institute of Standards and Technology (NIST) is responsible for improving critical infrastructure cyber security of their sector. Another option is centralised control which India is following through National Critical Information Infrastructure Protection Centre (NCIIPC)[1].

National Critical Information Infrastructure Protection Centre (NCIIPC)

The Information Technology Act, 2000 defines Critical Information Infrastructure (CII) as "… *those computer resource, the incapacitation or destruction of which shall have debilitating impact on national security, economy, public health or safety*". National Critical Information Infrastructure Protection Centre (NCIIPC) is an organisation of the Government of India created under Section 70A of the Information Technology Act, 2000 (amended 2008), through a gazette notification on 16 January 2014. It is designated as the National Nodal Agency in terms of CIIP. It is a unit of the National Technical Research Organisation (NTRO) and comes under the Prime Minister's Office.

NCIIPC has generally identified Critical Sectors as: Power & Energy, Banking, Telecom, Financial Services & Insurance, Transport, Government, Strategic & Public Enterprises. Of late health sector has also been included in this list.[2] The role of NCIIPC is to coordinate, share, monitor, collect, analyse and forecast national-level threats to CII for policy guidance, expertise sharing and situational awareness for early warning or alerts. However, "the basic responsibility for protecting CII system shall lie with the agency running that CII."

The NCIIPC is the nodal agency for CII, and it assesses the criticality of the functions and services provided by the organisation / entity and the magnitude of impact on national security, national economy, public health, or public safety in case of in Information Technology. NCIIPC and Manner of Performing Functions and Duties Rules, 2013 further define 'Critical Sector' as sectors, which are critical to the nation whose incapacitation or destruction will have a debilitating impact on national security, economy, public health, or safety.[3]

CII Protection vs CII Resilience

Critical Information Infrastructure Policy (CIIP) and Critical Information Infrastructure Resilience (CIIR) have significant overlaps. However, they reflect different organisational perspectives and requirements. CIIP emphasises the identification, prioritisation and protection of infrastructure assets. Criticality is normally defined in terms of the consequences of asset loss or system disruption. Cyber Resilient System are those systems that need security measures or safeguards to be 'built-in'. The systems can withstand a cyber-attack, and can continue to operate even in a degraded or debilitated state, further carrying out mission-essential functions.

Resilience is the ability of the CII systems to quickly respond and rebound and continue functioning regardless of a disruption or destruction. A perfectly resilient system resists disruption or destruction and ultimately one that can very quickly continue functionality in some form in the event of destruction or disruption. CII resilience stresses broad investments in hazard mitigation and preparedness during steady-state periods and adaptation during emergencies, to ensure availability of CII functions that enable provision of essential services.[4] Problems that need to be addressed are:-

- Technology refresh cycles are too long;
- Critical infrastructure is locked in to a limited number of vendors;
- Vendors are not always designing with security in mind.

Increasingly, CII resilience is being favoured over CIIP. However, most countries' national CII policy follow a hybrid approach that contains elements of both CIIP and CIIR.

Strengthening Resilience. Strengthening the resilience of infrastructure and minimising disruptive effects are critical as threats continue to evolve and vulnerabilities will always exist. Efforts should be on ensuring the capacity to anticipate/ identify, prepare respond and recover from cyber incidents affecting CII including through more effective and comprehensive strategic planning, risk awareness and management and greater cooperation and engagement between and across sectors and actors - nationally, regionally and internationally. Key Stakeholders involved in CIIP are:-

- CIIP coordinating agencies: MHA, Law, ICT, Defence and Prime Minister's Office
- ICT Ministries: Ministry of Information and Information Technology (MeitY), Media, ICT departments
- Ministers responsible for specific CI: Economic Affair, Power, Health departments
- Regulators for specific CI domains: ICT regulator, Finance regulator, power regulator
- Law enforcement and similar agencies
- National security and intelligence agencies
- Crisis and safety management agencies, NDMA
- Public and private CI and CII operations (and owners) of relevant utilities
- Politician and Parliament
- ICT security companies, software vendors, SCADA manufacturers, system integrators and 3rd party maintenance companies
- Cross-sector (Brand) organisation
- Computer Security Incident Response Team (CSIRT): National and sectoral CSIRT
- NCSCs.

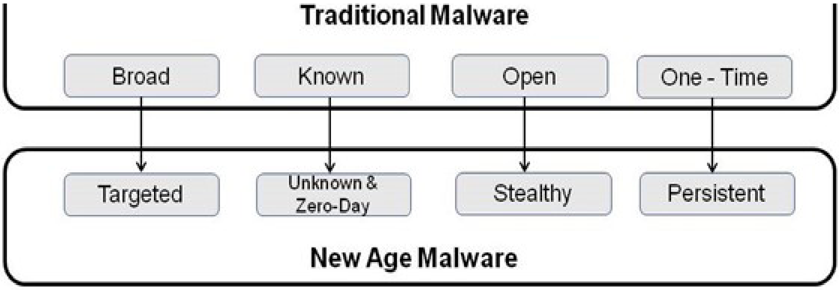
4. CII THREAT LANDSCAPE

Cyber Critical Infrastructure Targeting

Threats to CII have undergone major changes. Not only the number of attacks has increased, the complexity and the sophistication of the attacks have also gone up considerably. The inter-connectedness of critical infrastructure assets, devices and the software supply chain systems with third parties have made identifying attack paths more complex. This interconnectedness creates numerous potential entry points for attackers to exploit. Activities of some of the advanced persistent threat (API) actors and state sponsored actors are a constant source of worry for CII protectors.

The traditional focus on military and intelligence targets in cyber operations has expanded to include a broader spectrum of targets, including CIIs. The aim is to undermine governments by digitally taking citizens hostage changing the character of the threat environment. Recent attacks on Colonial Pipeline and water treatment plants in U.S. demonstrate the potential for malicious actors to cause huge impacts. CII defenders are most worried when the attacker has access to tools which are available in open domain or very cheap to acquire, motivation, resources in terms of deep pockets to break into CIIs, persistence and patience.

Evolving Cyber Threat Landscape



Cyber attacks have become sophisticated, complex and more challenging; Result: Longer periods of time before the infection is found out.

Major Trends

Threats that have emerged are given below:-

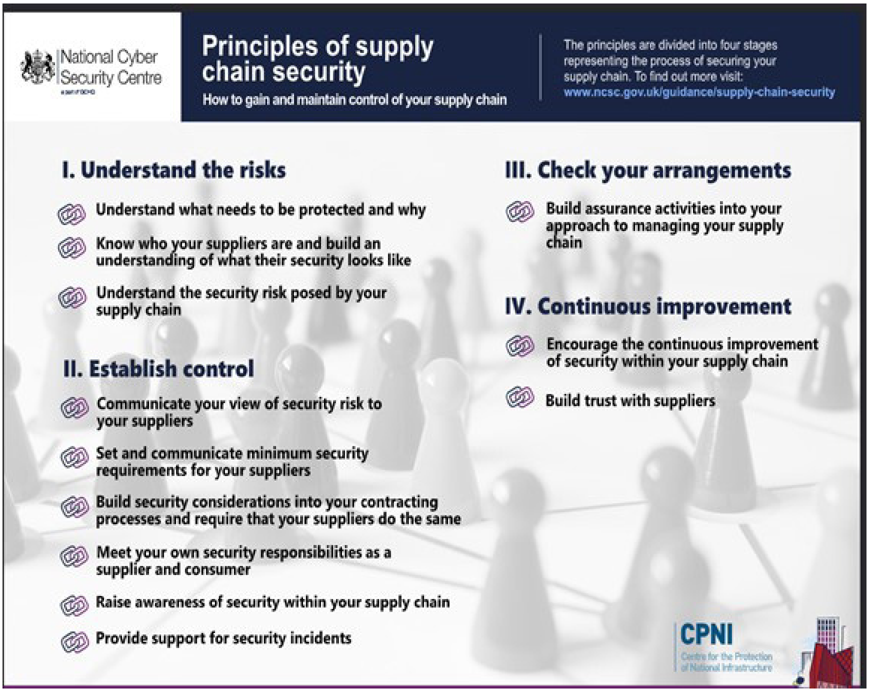
- **Willingness to use cyber war capabilities to compromise adversary CII systems and assets.** This is in consonance with their broader strategic objectives. This may not have any inherent espionage value.
- **Ransomware**. Ransomware remains a persistent threat to national security, public safety and economic prosperity. Criminals are increasingly using Ransomware to target industries knowing that downtime can result in significant financial losses. Ransomware-as-a-Service (RaaS) has further triggered the proliferation of ransomware attacks, making these attacks more accessible to a wider range of threat actors. Ransomware groups constantly develop sophisticated strategies to evade or circumvent defensive and disruptive measures designed to frustrate their activities. Unfortunately, these threats are further aggravated by complacency across CII organisations and a lack of commitment to invest in this area.

The 2021 Colonial Pipeline Company ransomware attack is an example of how targeting even a single company responsible for a vital sector segment can have disproportionately adverse consequences. The attack caused a shutdown of nearly half of the gasoline and jet fuel supply delivered to the U.S. East Coast. A bitcoin address connected to the alleged hackers, a group known as AlphV or BlackCat, received a $22 million transaction that some security firms say was probably a ransom payment made to the group.

Presently the health sector in the U.S. is in chaos due to a Ransomware attack in February, 2024. The nation's biggest healthcare payment system, United Health Group, has been shut down causing financial chaos that affected a broad spectrum ranging from large hospitals to single-doctor practices. The ransomware attacks have caused $872 million in losses.[5]

- **Supply Chain Exploitation**. The digitalisation of critical infrastructure, coupled with increased dependence on third parties for supply chain for software and other information technology and services, has made it vulnerable to cyberattacks across multiple vectors to compromise victims at scale. All the known attack vectors can be addressed, but on these supply chains one does not have much control. The risks to monitor and manage include: employee workforce risk, third, fourth, and nth parties (not just their vendors, but their partners and suppliers' networks, too), the native technology stack, compliance and regulatory frameworks.

  Link between supply chain security, CIIP and national security is clear. A chain is only as strong as its weakest link. Poorly protected partners can be exploited by adversaries to target critical operators. Public authorities should address this risk by fostering a secure market for digital products, setting minimum standards and implementing certification systems. Operators must ensure that all third parties have sufficient cybersecurity measures in place, with specific criteria included as binding conditions in contracts. This ensures CII operators can select partners with verified cybersecurity maturity, enhancing overall infrastructure resilience. In the U.K. both the NCSC and the Centre for Protection of National Infrastructures proposed 12 principles designed to help companies, including CI/CII operators, establish effective control and oversight of their supply chain.



National Cyber Security Centre
a part of GCHQ

Principles of supply chain security

How to gain and maintain control of your supply chain

The principles are divided into four stages representing the process of securing your supply chain. To find out more visit: www.ncsc.gov.uk/guidance/supply-chain-security

I. Understand the risks

- Understand what needs to be protected and why
- Know who your suppliers are and build an understanding of what their security looks like
- Understand the security risk posed by your supply chain

II. Establish control

- Communicate your view of security risk to your suppliers
- Set and communicate minimum security requirements for your suppliers
- Build security considerations into your contracting processes and require that your suppliers do the same
- Meet your own security responsibilities as a supplier and consumer
- Raise awareness of security within your supply chain
- Provide support for security incidents

III. Check your arrangements

- Build assurance activities into your approach to managing your supply chain

IV. Continuous improvement

- Encourage the continuous improvement of security within your supply chain
- Build trust with suppliers

CPNI
Centre for the Protection of National Infrastructure

- **Commercial Spyware**. Private vendors are selling sophisticated cyber-surveillance tools to nation-state actors. These tools allow remote access to electronic devices, content monitoring, extraction and component manipulation without user consent. This market is thriving, with vendors offering top-notch capabilities to the highest bidder, often for cyber operations without oversight or regulatory constraints.

- **Third Party Service Providers.** Critical infrastructure owners and operators often rely on third party service providers to manage their digital operations. This creates opportunities for sophisticated adversaries to access victims at scale and complicate the efforts of defenders to identify and manage cybersecurity risks. Cloud services, as an example, can offer better cybersecurity outcomes at scale and cost effectively. However, migration to cloud services can also bring new cybersecurity risks. Hybrid deployments, which combine locally hosted systems with cloud assets, can create complex centralised logging and authentication systems. Malicious actors are increasingly taking advantage of complex and interconnected relationships between organisations and their suppliers, vendors, customers and service providers that grant surreptitious access to victims
- **Artificial Intelligence.** Among the emerging technologies, Artificial intelligence (AI) is one of the most powerful, publicly accessible technologies of our time. Recent advancements in Large-Language Models (LLMs) and foundational algorithms, combined with more accessible computing power and data, have led to a new generation of AI tools. These tools, such as chatbots and image generators are expected to evolve rapidly in the future. In cybersecurity, AI presents new opportunities for defending critical infrastructure against malicious activity. The cybersecurity community has a history of using machine learning for tasks like data processing and malware identification. Integrating AI into cyber defence could enhance the detection of anomalous network traffic, improve coordination in defending complex systems and support an overburdened cybersecurity workforce.

AI tools also have the potential to enhance software security. By responsibly integrating AI into the software development lifecycle, developers could identify vulnerabilities in new code and improve the security of widely used software products. However, use of AI also raises cybersecurity risks. AI can generate convincing text, images, audio and video in various languages, which cybercriminals and others could use for phishing campaigns and misinformation. As the AI ecosystem evolves, there is an opportunity to develop safeguards against misuse in its core elements—data, computing, and algorithms.

5. SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA), INDUSTRIAL CONTROL SYSTEMS IN CRITICAL INFRASTRUCTURE – VULNERABILITIES AND THREATS

Operational Technology (OT)

Industrial control systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems are critical components for operating industrial facilities and critical infrastructure. Many CIs rely on Operational Technology (OT), a set of technologies that connect physical elements, networks and communication protocols to execute industrial operations. OT is used in the control room and IT is used to monitor the physical process. Typical examples of OT are SCADA (Supervisory Control and Data Acquisition), ICS (Industrial Control Systems) and DCS (Distributed Control Systems) etc.

OT is inherently insecure as it interfaces with physical processes (warming, cooling, chemical reactions, liquid flow, etc.) and needs to respond to immediate real-time requirements where data availability becomes more important than its security.

In an OT environment, applying standard cybersecurity measures has become difficult. Using standard routines such as antivirus, firewalls and encryption might delay the immediate exchange of data and affect the readiness of a system. Similarly, patching and updating require infrastructure downtime, which must be planned long in advance. For a long time, OT was protected by "security through obscurity". This means that control systems were "air-gapped," i.e., not connected to the internet and employed legacy systems and proprietary networks. Bad actors had to have extensive knowledge of the system in use and physical access to the site.

However, to respond to the primary need for operability and reduce reliance on custom and legacy systems vendors, many CI sectors have turned to off-the-shelf systems and have increased their connectivity. Today, industrial assets are primarily equipped with an internet connection. While the integration of IT protocols and internet connection have significantly improved the performance of OT-based CII, it has also exposed IT systems to cyberspace threats with a dramatic increase in the number of attacks. Securing OT environments is essential, and organisations must prioritise cybersecurity investments to defend themselves against evolving cyber threats effectively.

OTs are the most complex targets. Attacking them requires considerable sophistication and resources. The employment of Artificial Intelligence and Machine Learning significantly reduces the duration of training within the targeted network. These open up new ways to transform cyber means into tactical tools that can quickly be deployed.

SCADA

Software used to collect and present data about the state of a physical process is called SCADA. SCADA systems are utilised to monitor and control geographically dispersed processes from a central location and make informed decisions. Many organisations in critical infrastructure have deployed SCADA/ICS to automate the control of processes and data collection. The digitisation of critical infrastructure and increased dependence on third parties have made it vulnerable to cyberattacks across multiple vectors. Threat actors employ sophisticated malware to target SCADA systems, with potential impacts ranging from espionage to disrupting essential services. In connecting these networks and introducing IT components into the industrial control system domain, security problems arise because of:-

- Increasing dependency on automation and industrial control systems.
- Increase connectivity to external networks.
- Usage of technologies with known vulnerabilities, creating previously unseen cyber risk in the control domain.
- Lack of qualified cybersecurity business case for the industrial control system environments.
- Some control system technologies have limited security and are often only enabled if the administrator is aware of the capability (or the security does not impede the process).
- Many popular control system communications protocols are absence of basic security functionality.
- Considerable amount of open-source information regarding industrial control systems, their operations and security vulnerabilities is available.

Difference between Information Technology (IT), Operation Technology (OT) and Industrial Control Systems (ICS)

Control system technology differs from the IT used in a company's billing and administrative departments, where the activity is data or information-centric. It also differs from the Operational Technology (OT) used in the control room, that uses IT to monitor the physical process. The workstations in the control room use control software that processes and presents the acquired information using a human-machine interface (HMI). The software used to collect and present data about the state of a physical process is called SCADA. Industrial control systems (ICS) are the technology closest to the actual physical process, which monitors and controls those processes according to pre-set parameters and can report this information to the control room. Devices found in ICS have computer-like qualities. Unlike the general-purpose PC found in offices, these devices are designed to perform a specific task. A Programmable Logic Computer (PLC) is a computer-like device that has a Central Processing Unit (CPU), a memory and communication ports. It can be programmed to perform specific actions. However, it will not do well as a word processor.

These three industrial environments IT, OT and ICS have different requirements. A one-size-fits-all approach based on IT security best practices will not work. The traditional approach of isolating critical infrastructure from the outside world is no longer viable. While CII sectors are maturing in their cybersecurity practices, many organisations still operate with a reactive mindset, only addressing cyber threats after they occur. This approach is costly and unsustainable, as the impact of cyber incidents can be significantly higher than proactive prevention measures.

Threats and Vulnerabilities

OT Systems Lack Basic Security Controls. Some of the most common threats are:-[6]

- **Legacy software**. Lacks sufficient user and system authentication, data authenticity verification or data integrity checking features that allow attackers uncontrolled access to systems.
- **Lack of Encryption**. Legacy SCADA controllers and industrial protocols cannot encrypt communication. Attackers use sniffing software to discover usernames and passwords.
- **Lack of Network Segmentation**. Internet-connected OT flat and misconfigured network, firewall features that fail to detect or block malicious activity provide attackers a means to access OT systems.
- **Policies and Procedures**. Security gaps are created when IT and OT personnel differ in their approach to securing industrial controls. Different sides should work together to create a unified security policy that protects both IT and OT technology.
- **Web Application Attacks**. Traditional OT systems, including human-management interfaces (HMI) and programmable logic computers (PLC) are increasingly connected to the network and are accessible anywhere via the web interface. Unprotected systems are vulnerable to cross-site scripting and SQL injection attacks.
- **Remote Access Policies**. SCADA systems connected to unaudited dial-up lines or remote-access servers give attackers convenient backdoor access to the OT network as well as the corporate LAN.
- **Default Configuration**. Out-of-box systems with default or simple passwords and baseline configurations make it easy for attackers to enumerate and compromise OT systems.

Recommendations to Secure ICS/SCADA Systems

Some of the actions CII organisations can take are:-[7]

- Use virtual patching to help manage updates and patches.
- Apply network segmentation.

- Use adequate security measures between the ICS network and corporate network.
- Properly manage authorisation and user accounts.
- Use endpoint protection on engineering workstations connected to SCADA for device programming and control adjustments.
- Maintain strict policies for devices that are allowed to connect to SCADA networks.
- Restrict the roles of transitory SCADA nodes to a single purpose.
- Prevent the use of unknown and untrusted USB devices.

6. CII PROTECTION - CRITICAL ISSUES

CII Protection (CIIP) has three strategic objectives: Prevent cyberattacks against critical infrastructures, reduce national vulnerabilities to cyberattacks and minimise damage and recovery time from cyber attacks that occur. To attain these objectives a new strategy is needed that combines more than the technological issues and includes the following elements:-

- Taking preventive measures at all levels.
- Improving early detection and rapid reaction capabilities, both for damage control and pursuit of the culprits.
- Limiting the impact of disruptions on government and society.
- Ensuring that the affected systems continue to function at a minimum level or can be restored within the shortest possible time

Strategies, Policy, Regulations and Standards

A cohesive CII Policy requires top-down guidance through strategies, policies, regulations, and standards. These documents vary in specificity, with strategies and policies providing general principles, while regulations and standards offer specific requirements. While not all standards need enforcement, they serve as benchmarks for best practices. The goal is to ensure all critical sectors maintain a minimum level of cybersecurity for systemic resilience.

Principles and Objectives

The aims to enhance the security and resilience of its critical infrastructure should be based on the following principles:-

- **Shared Responsibility.** Safeguarding CII is a shared responsibility among various agencies, including Central, State, public or private owners and operators and independent regulatory and oversight agencies.
- **Risk-Based Approach.** CII security efforts must adopt a risk-based approach, considering the relationship between specific sector infrastructure and national security, economic security, safety and the Central Government's ability to provide essential services.
- **Minimum Requirements.** Regulatory and oversight organisations at all levels should establish and implement minimum requirements for risk management, leveraging existing guidelines where applicable and ensuring alignment and scalability.
- **Accountability.** Robust accountability and enforcement mechanisms are essential for effective risk management, involving various entities from Central Government to private sectors.
- **Information Exchange.** Timely and actionable information sharing among relevant entities are crucial for effective risk management, supported by a robust information sharing environment and public-private cooperation.
- **Expertise and Technical Resources.** The Central Government should utilise expertise and technical resources from relevant departments and agencies to enhance the capacity and capability to manage sector-specific risks.
- **International Engagement.** Given the global interconnectedness

of critical infrastructure, the Central Government should collaborate with international partners to strengthen the security and resilience of CII.

- **Policy Alignment:** Efforts to safeguard CII should be integrated and coordinated with complementary central policies and frameworks, ensuring alignment with domestic incident management, cybersecurity, national preparedness, continuity, counterterrorism and other relevant policies and frameworks.

Objectives. Objectives of the Central Government should be to:-

- Refine and clarify the roles and responsibilities of the Central Government for CII security, resilience and risk management.
- Identify and prioritise CII security and resilience based on risk and implement a coordinated national approach to assess and manage sector-specific and cross-sector risk.
- Establish minimum requirements and accountability mechanisms for CII security and resilience, including effective regulatory frameworks.
- Utilise Central Government rules such as grants and procurement processes to incentivise sectors and private sectors to meet or exceed minimum security requirements.
- Improve intelligence collection and analysis related to threats to CII.
- Enhance real-time sharing of actionable threat intelligence among Central, State, private sector and international partners.
- Encourage investments in technologies and solutions to mitigate evolving threats to CII.
- Engage international partners to enhance the security and resilience of CII globally.

Roles and Responsibilities

There is a need to take a *de novo* look at the roles, responsibilities and capabilities of different stakeholders responsible for security of the nation's CII. The Central Government relies on specialised authorities, capabilities and expertise of Central Government departments and agencies to ensure effective protection of CII. NCIIPC should provide strategic guidance and coordinate cross-sector risk management efforts. Respective CII sectors should oversee day-to-day operations for designated sectors and manage sector-specific risks. The Intelligence Community (IC), law enforcement agencies and regulatory bodies also play vital roles in enhancing CII security.[8]

Close coordination between NCIIPC, Cert-In, National Cyber Security Coordinator, Ministry of Information and Information Technology (MeitY), Ministry of Communications, MHA and other relevant Central Government ministries including law enforcement and the Intelligence Agencies is crucial for a unified national effort. Both government and private sector share responsibility and incentive to mitigate risks. NCIIPC should set basic guidelines for safeguarding CII, which sector-specific regulators can then tailor to suit their sector's requirements. However, this approach should not result in the proliferation of regulations or reporting channels within the same domain. Presently, NCIIPC has issued fundamental guidelines, such as cybersecurity audit requirements for protecting CII. However, it has been noticed that at times, other regulators issue guidelines in the same realm instead of building upon the existing framework.[9]

Responsibility of Respective CII Sectors. Each CII sector requires a designated agency to oversee sector-specific activities and enhance security and resilience. It should be responsible for:-[10]

- Acting as the primary interface for coordinating sector-specific activities, providing technical expertise and leading outreach efforts.
- Leading outreach efforts to educate sector owners and operators on security and resilience issues.
- Designating Accountable Senior Officials to oversee its functions and ensure their effective implementation.
- Leading sector risk management efforts and supporting cross-sector risk management initiatives.
- Identifying, assessing and prioritising sector-specific risks and supporting national risk assessment efforts.
- Identifying critical infrastructure-related workforce needs and priorities for security and resilience.
- Incorporating national priorities into sector risk management responsibilities.
- Identifying sector-specific information and intelligence needs and facilitating information exchange among stakeholders.
- Sharing and receiving information and intelligence directly with critical infrastructure owners and operators.
- Supporting domestic incident management, emergency preparedness, and national continuity efforts.
- Serving as lead cenral agencies for incidents primarily impacting their sectors, as requested or directed by the President.
- Providing technical assistance to sector owners and operators to mitigate risk and collaborating to identify joint priorities for sector security and resilience enhancement.

Risk Management

CII operators should adopt a risk management framework, offering a systematic approach to identifying, assessing and responding to cybersecurity risks. Understanding the likelihood and impact of events helps determine risk tolerance and prioritise actions. Prioritising risk management efforts entails identifying the criticality of assets and systems within and across sectors. NCIIPC along with respective sectors should adopt a unified risk-based approach to mitigate risks to CII.[11]

National Crisis Management

A comprehensive national Critical Information Infrastructure Protection (CIIP) strategy should include both preventive measures and crisis management mechanisms. This involves planning for significant disruptions, ensuring minimum service levels and restoring normal operations promptly. Emergency response plans should align with the cyber risk landscape, outlining roles, responsibilities and actions for potential incident scenarios, including stakeholder communication. Drawing insights from past incidents and industry standards, operators can develop effective plans.

Coordination at the national level, possibly through a dedicated team representing all stakeholders, is crucial for decision-making during crises. Regular testing, such as cyber drills and wargames helps assess preparedness. Continuous monitoring and improvement are essential, with clear objectives, indicators and integration of lessons learned. A designated authority should oversee CIIP implementation.

Incident Response & Reporting

CERT-In recently issued directions on information security practices for Safe & Trusted Internet, with a focus on CII. These guidelines mandate all government and private agencies, including ISPs, social media platforms, and data centers, to report cyber security breaches within six hours. Incidents concerning CII include targeted scanning/probing, compromise of critical systems/information and attacks on critical infrastructure. However, industry stakeholders have expressed concerns that the six-hour timeframe is inconsistent with international norms. They worry that such stringent obligations could divert resources from managing security incidents effectively.[12]

How to mitigate or even avoid these attacks? CIIs face complex cyber risks, necessitating continuous proactive management. State and local entities are leading efforts to assess and prioritise threats. Public and private sectors collaborate through Information Sharing and Analysis Centers, sharing best practices. Despite existing tools, the challenge lies in reactive defence. Real-time risk visibility is crucial. Cyber risk quantification, grounded in data science, offers a solution.

Organisational Challenge: Siloed Security Functions

Cyber and physical assets pose substantial risks to security when targeted individually or concurrently, compromising systems and infrastructure. However, security divisions often operate separately, leading to a fragmented understanding of threats. This siloed approach increases vulnerability to attacks, potentially causing severe consequences.

Organisational Solutions:-

- **Converged Security Functions.** Convergence necessitates the integration of formerly separate security functions.
- **Benefits of Convergence.** An integrated threat management strategy recognizes the interconnected nature of cyber-physical infrastructure and its cascading impacts. As technology continues to intertwine physical and cyber assets across various sectors, the advantages of merging security functions surpass the hurdles of organisational

change. This convergence facilitates a flexible, sustainable strategy grounded in shared security practices and objectives.[13]

Monitoring and Improvement

Implementing CIIP is vital, requiring formal processes for ongoing monitoring and evaluation. Designating an authority to oversee implementation is crucial. For CII operators, developing policies involving people, technologies, processes and programs supporting a robust security posture is essential. Key activities include establishing a risk management framework, testing emergency plans, training, supply chain security, information-sharing, legal compliance and continuous monitoring.

An inter-departmental committee should be instituted, comprising members from NCIIPC, Cert-In, and Sectoral CERTs. This committee would evaluate the continuous monitoring process and responsibilities, ensuring effective responses to emerging threats.

Training and Education. Organisations must continually ensure employees possess the necessary skills, knowledge and mindset to address evolving cyber risks. Regular cybersecurity awareness training and educational activities should be provided to all personnel, tailored to their roles. Emphasising security awareness is crucial, as human behaviour often contributes to incidents. Employees should be familiarised with information security policies and their significance, fostering a culture of security and promoting behaviour change.

Cyber threat Information Sharing and Cooperation. In today's inter-connected world, individual CII operators can't manage cyber risks alone. Establishing trusted communication channels with stakeholders is integral to CIIP. Cyber threat information includes indicators of compromise, tactics used by threat actors, vulnerabilities exploited, targeted organisations and suggested actions for detection and prevention. Sharing information on threats, vulnerabilities, standards and best practices, before, during, and after incidents, is crucial for security and preparedness. This collaboration helps reduce incident spread and minimizes infrastructure damage. By sharing information about observed malicious activity, organisations enable others to identify trends and disseminate strategies for detection and prevention. Given the sensitivity of such information, engagement in trusted networks with public authority involvement is essential. Information sharing spans public and private sectors, nationally and internationally.

Challenges. There are six major challenges to Cyber Threat Information sharing: limited relationships, limited funding and resources, limited sharing of classified or sensitive information, lack of timely sharing, limited voluntary sharing and lack of actionable information.[14]

Adoption of Global Best Practices & Cross Border Knowledge Sharing. In our modern interconnected world, no nation can effectively address cyber threats to its CII independently. It is crucial to establish internationally recognised standards for CII and implement them at the national level. Equally important is the adoption of global best practices in national legislation and the establishment of a framework for sharing knowledge across borders. These efforts will not only enhance India's cybersecurity posture but also contribute to its geopolitical standing.

Legal Compliance. CII operators must adhere to legal guidelines tailored to their industry, sector, customers and location. These regulations typically cover cybersecurity and data protection/privacy requirements, ensuring compliance with national security standards and international norms. Operators should establish repeatable processes to assess their cybersecurity maturity level regularly, considering objectives and constraints. This assessment should evaluate preparedness in incident detection and response, business continuity and various cybersecurity incident scenarios and their potential consequences.

Establishing Government's Internal Communication Channels. The current notification requirements within the CII framework, involving multiple regulators, need to be reassessed to address duplicative and conflicting obligations. A proposed solution is for the government to create an information sharing system where all relevant regulators are notified when the primary regulator, such as NCIIPC, receives information from regulated entities. Under this system, critical sector enterprises would only need to inform the primary regulator, while the government would establish internal communication channels to ensure all regulators are kept informed. This streamlined approach would create a single interface between the government and critical sector enterprises, linking all regulators at the backend.[15]

Management of CII

Management of CII is getting more and more complex. Angles of attack are constantly increasing. The current attack surface contains many possible points of entry, such as Internet of Things devices, hybrid cloud architecture, SaaS applications, and other tools. Ransomware as services has become a big menace.

Managing critical infrastructure involves implementing robust software solutions and systems to monitor, control and secure the various components of the infrastructure. Critical infrastructure can be effectively managed using software solutions' power, ensuring its reliability, security and resilience. It involves Asset Management, Network monitoring and security, Data analytics and predictive maintenance, Risk-based approaches, Remote monitoring and control, Incident response and disaster recovery, Redundancy and backup systems, compliance and regulatory requirements, Training and education, Collaboration and information sharing and Public-private partnerships.

Every organisation that operates critical infrastructure should have dedicated cybersecurity personnel to protect against evolving threats.

7. ROLE OF PRIVATE SECTOR

CIIs are owned by both government and private industries. In India, ownership of CIIs by private parties is less although some important CIIs like telecom, non-conventional energy etc are dominated by private sector. It is important to promote cooperation within and between the government and private industries in the format of Public-Private Partnership (PPP).

Information sharing between government and the private industry has always been a key component of strengthening a country's resilience to hacking campaigns by adversary governments, non-state actors, criminals and hacktivists. While the industry is responsible for sharing instances of breaches, there are issues like proprietary, privacy and reputation that can hinder their willingness to do so easily. Also, there are major reservations to the free flow of information from government to industry as there is risk of compromising intelligence sources and methods.

Public-Private Partnership (PPP) can be developed through several initiatives like: through regulations, information sharing, pooling of resources, mutual support, trainings and capacity building, sharing of best practices, inter-organisational networks of collaboration and joint decision making.

In the U.S. government bodies like Department of Homeland Security (DHS) insulates intelligence agencies from industry. However, adding layers of bureaucracy to public private collaboration in cybersecurity decreases the timeliness of the information shared. Dormer Director of National Intelligence of USA James Clapper argues, "The DHS is the appropriate storefront and that's the way it ought to be. I don't think the spy crowd should be directly engaging with the private sector."

Private industry has the following advantages in cooperating with the government agencies:-

- Enhanced access to risk information from government sources on security threats.
- Value of analyses of national-level risks that surpass the capabilities of most private companies to provide for themselves.
- Opportunity to engage with government to influence CII policy.

Government's efforts to increase resilience can inadvertently create incentives for freeriding by companies that want the benefits without contributing to it themselves by risking proprietary information.

Private sector operators might be reluctant to share information if they fear it will lead to extra costs that they will have to finance, once their vulnerabilities are known. The private sector often complains that government agencies either declassify information too slowly or keep it tightly restricted to only executives with security clearances. Many companies feel that without timely access to the government's detailed intelligence about hackers' activities, it is difficult to stay ahead of those adversaries.

At the policy level it is often difficult to work out precisely who should bear responsibility for costs of investment and what mandatory requirements, regulatory oversight measures and cost-recovery mechanisms might be necessary in a given case. The private sector often complains that agencies declassify information too slowly or restrict it to only executives with security clearances. Many companies say that it is challenging to stay ahead of those adversaries without timely access to the government's detailed intelligence about hackers' activities.

Dealing with ransomware attacks requires a joint public-private effort. Government agencies should collaborate with the industry to develop tailored strategies to protect them. Both public and private sectors should be actively involved in making actionable, sustainable strategies that meet the unique needs of respective CIIs.

Role of Big Tech

On March 24, 2024, the Cyber Safety Review Board (CSRB) of the U.S. issued a report strongly criticised Microsoft for its handling of cybersecurity for the US government. The CSRB questioned Microsoft's security culture and held it directly responsible for numerous large cyber intrusions on U.S. government networks in the last two years. The report found that a cascade of Microsoft's avoidable errors allowed breaches from Chinese and Russian government-connected interests to succeed.

Microsoft failed to detect the breach from the Russian Intelligence Service and relied on a customer who reached out after detecting and observing severe anomalies. It has come out clearly that Microsoft performed negligently. To keep the CIIs secure, government procurement and compliance officials should not rely on private companies, even big tech companies like Microsoft. However, to ensure effectiveness, the CII sectors must do it themselves. The question is, do they have the capacity to do it? Unlikely. What they can do are the following:-

- Stringent adherence to contract protocols and statements of work (SOW).
- Strict definitions should be made about expectations, timeframes and deliverables in SOW. Any deviation from agreed-upon terms must be addressed immediately before the original issue gets out of control.
- Reliance on the name brand of the service provider instead of the actual quality of work delivered must stop.
- Ensure quality of in-house cyber experts charged with managing contracts and contractors. Generally, there are too few experts who are spread too thin and perform too many tasks.
- CII sectors must receive the necessary resources to ensure that they can compete for and retain top cyber talent. Cyber experts should be part of the organisation.
- Should avoid nearly single-source reliance on contractors. Lack of options available to contracting officers is a critical shortfall in holding these big guns to account.
- A workable system to share information on contractors and their performance in real-time that allows cyber professionals of various CIIs to be established. This would alert CII sectors considering proposals and SOWs to companies performing poorly and allow them to make procurement decisions based on all the available facts.

Capacity Building and International Collaboration

The 2021 UN Group of Government Experts (GGE) report enumerated several tangible cyber capacity-building measures that link directly to CII. These are:-

- Developing national ICT policies, strategies, and programs.
- Improving the security, resilience, and protection of critical

infrastructure.

- Enhancing the capacity of CERTs and computer security incident response teams (CSIRTs) and strengthening arrangements for their cooperation.
- Enhancing the technical and legal capacities of all states to investigate and resolve serious ICT incidents.

Results of these measures have been uneven. The international community must consider adopting a global cyber treaty to protect CIIs. In an area where many states are actively involved, a treaty could complement existing rules and contribute to raising the international level of cybersecurity. Binding, prohibitive measures may meet resistance from governments. Positive obligations focused on cybersecurity and the safety of CII operators could be a game changer in strengthening cyber resilience globally.

8. EFFECT OF EMERGING TECHNOLOGIES IN CII

Emerging technologies play a key role in people's lives and in the functionality and protection of infrastructures that ensure the availability of goods and essential services. The rapid development of emerging technologies has a significant impact on CII. People responsible for CIIs have to be nimble on their feet when thinking and taking action. Otherwise, they will be left behind and events will overtake them.

Artificial Intelligence, Cloud Computing, Quantum Computing, the Internet of Things, Big Data, blockchain, 5G, robotics, drones, 3D printing and others represent the innovative technologies that are part of the reality we live. Only the three emerging technologies: cloud computing, AI and crypto computing, are discussed here.

Cloud Computing

Cloud computing usage is growing. Soon, most organisations will rely on some form of cloud computing services. Cloud computing is also being adopted in critical sectors, like finance, energy, transport and even governmental services. Earlier applications would be run on servers on their own premises or dedicated data centres. This may no longer be the case. Now, applications are outsourced to large cloud service providers, which might be in foreign countries and run in a few large data centres. Aggregating and sharing common digital services and functions across borders is possible. It is expected that 80 percent of organisations will soon be dependent on cloud computing. This will increase the attack surface as CIIs are exposed to more cyber risks. The malicious actors would find new ways to reach their target.

Today, cloud computing is widely available and used. Data and software may be hosted in the cloud. Earlier, it was the norm that CII physical systems were entirely owned or controlled by the CII owner. For example, the energy sector uses the cloud to update old interfaces and increase data transmission efficiency. Smart grids are partially or wholly reliant on the cloud. Through activities such as dynamic load balancing and additional visibility into grid operations smart grids increase the resilience and capacity of the grid.[16] Cloud services were proven to be a strategic asset as Russian forces physically destroyed Ukrainian facilities holding critical data. Since the government's essential data was transferred to Microsoft cloud, no harm was done.

Cloud Vulnerabilities. The shift towards cloud computing has driven efficiency, scalability, and innovation within critical sectors. However, this transition also introduces new vulnerabilities, as sensitive data and critical operations increasingly rely on cloud-based platforms. Misconfigurations, lack of visibility into cloud environments and insufficient access controls are among the top cloud security challenges. The widespread adoption of public, private and hybrid cloud models necessitates a comprehensive security approach encompassing rigorous access management, data encryption in transit and at rest and continuous monitoring for anomalous activities. Embracing a shared responsibility model where cloud service providers and users have defined roles in securing cloud environments is crucial for safeguarding against these vulnerabilities.[17]

From a CIIP viewpoint, this concentration of IT resources is a double-edged sword. Large cloud providers can deploy state-of-the-art security and resilience measures and spread the associated costs across the customers. Alternatively, if an outage or security breach occurs, the consequences could be big, affecting many organisations, a large number of citizens, and a lot of data at once.

Cost savings, scalability and outsourced infrastructure management, security and availability have led to rapid adoption of cloud computing. Cloud service providers are currently self-regulated by engineers and leaders without understanding the responsibility and accountability that implies. The policy has not kept pace with how essential cloud computing has become to the functioning of CIIs. Regulators and cloud companies need to work together to make reasonable rules.

To solve these significant cloud security challenges, recommendations are:-

- Regulators need more information about cloud providers and how their agencies use these cloud services. Until they have this information, they can't make informed decisions about their systemic cloud-related risk.
- Policymakers need the data to understand complex webs of interdependencies that create risks in the cloud environment.
- Regulators must update cloud policies, rules and regulations with that information. .

NCIIPC, in its Guidelines for the Protection of National Critical Information Infrastructure, has provided best practices for the cloud. These guidelines include using robust encryption methods, the onus on the enterprise to manage data backup on its own, barriers to keep critical information separate from other information and organisations, securing cloud-organisation and cloud-cloud interlinkages, maintaining logs, securing access to critical information, network services, operation system, application and system, adequate authentication mechanism, risk management strategy, breach reporting mechanism, regular updating and patching.[18]

Artificial Intelligence (AI)

The revolution in AI systems may occur even faster than the development and adoption of the Internet. Advances in large-language models (LLMs) and other foundational algorithms, combined with more affordable computing power and access to data, have given rise to a new generation of AI tools. AI technologies could be powerful tools for advancing the seventeen UN Sustainable Development Goals (SDGs).

However, the rapid growth of AI technology comes with significant risks. AI may require workforce adaptations across economies; the rising energy demands of high-end AI chips and data centres could become a significant barrier to developing local capabilities. State and non-state actors are using generative AI systems for malicious purposes.

These narrow AI uses reflect areas in which technology maturity has been achieved. They are early use cases, likely to become more sophisticated as AI technology and the individual component technologies mature. CIIs will see a significant proliferation of AI capabilities to improve the effectiveness and efficiency of current infrastructure. This presents challenges and opportunities that will need to be carefully managed.

Potential Applications and Benefits of using AI in CIIs are: infrastructure operational awareness, active controls, automation of operations, high-complexity modeling & simulation, anomalous event detection &

diagnosis, forecasting, system planning, scenario generation, predictive maintenance, customer service automation, malicious event detection & diagnosis and resource exploration & extraction, research & development (R&D) and physical security.

AI applications, after deployment, could give rise to cybersecurity risks, unethical decision-making, jurisdictional and sovereignty challenges and supplier dependency. It has the potential for cybersecurity breaches and intrusions into critical systems, which increases as the CIIs become more digitised. Relying on limited companies to develop and supply core infrastructure for AI poses important risks to critical infrastructure that could lead to monopolisation and create vulnerabilities that could affect service quality and price.

The evolving AI landscape will present cyber defenders with new opportunities to defend critical infrastructure against malicious activity. New cyber defence tools that integrate AI would enable cyber defenders to detect anomalous network traffic and other adversary activity efficiently, coordinate the defence of complex systems and networks and augment a cybersecurity workforce that is already stretched thin.

AI tools may also make our software development ecosystem safer and more secure. Responsible integration of AI tools into the software development lifecycle may enable developers to identify vulnerabilities in new code and suggest potential fixes. As AI tools mature, they can make widely used software products more secure by rewriting existing code into a memory-safe programming language.

At present, there are no policies or principles explicitly tailored to CIIs. With the current speed of AI development, many unknowns and emerging risks are challenging development of robust policies. The development of resilient and adaptable infrastructure is important to ensure that the benefits of AI are realised while minimising the risks and potential negative consequences. The key is to strike the right balance between innovation and regulation.[19]

Potential Risks. Irrespective of whether AI technologies are deployed in service of CIIs, hostile actors who wish harm to the sector may find ways to leverage AI to their own ends. Many significant risks can be mitigated through best practices, putting appropriate protections around important data and models and funding research on mitigation techniques.

The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. recently released safety and security guidelines for critical infrastructure. The guidelines are meant to address both the opportunities made possible by AI for CII and the ways it could be weaponised or misused. CISA instructs operators and owners of critical infrastructure to govern, map, measure and manage their use of the technology, incorporating the National Institute of Standards and Technology's (NIST) AI risk management framework.[20]

To improve AI security, CIIs should focus on critical defences like rigorous testing of open-source components, implementing code signing and employing software bill of materials (SBOM) and provenance verification. Continuously monitoring for vulnerabilities is essential. For example, in the energy sector, the emergence of generative AI is driving a rapid expansion of AI capabilities and tool deployment. As their use increases, so does the potential that malicious actors might target energy sector AI systems directly or use AI to enhance attempts to attack critical energy infrastructure. We must steer AI with a keen, technically grounded and risk-informed awareness of its potential and pitfalls.

Attacks Using AI. Ai can be used to automate, enhance, plan or scale physical attacks on critical infrastructure or cyber compromises. Examples are:

- AI-Enabled Cyber Compromises.
- Automated Physical Attacks.
- Physical Target and Vulnerability Identification.
- Social Engineering.
- Supply Chain Disruptions.
- Theft of Intellectual Property and Reverse Engineering.
- Weapon Development.

Mitigations for AI Risks. Mitigation strategies are primarily applicable to risks from all three risk categories: attacks using AI, attacks on AI and AI design and implementation failures. General Mitigation Strategies are: [21]

- Artificial Intelligence-Generated Content Identification Techniques.
- Defensive Artificial Intelligence Capabilities.
- Encryption.
- Host Security.
- Network Security.
- Red-Teaming.
- Secure by Design.
- Building Operational Resiliency,
- Data Inventory and backup.
- End Point Security.

AI cybersecurity is a dark frontier. According to the U.S. Defense Advanced Research Project Agency (DARPA), "Today, a comprehensive theoretical understanding of machine learning vulnerabilities is lacking." Highly capable AI is so new, security researchers haven't had the time to understand cyber risks.[22]

Quantum Computing

Nation-states and private companies are actively pursuing the capabilities of quantum computers. Quantum computing opens up exciting new possibilities. Though the consequences of this new technology include threats to the current cryptographic standards. These standards ensure data confidentiality and integrity and support key network security elements.[23]

Future quantum computing capabilities are expected to be able to break the security of current implementations of public-key cryptography. Public-key cryptography forms the foundational security building block for national information and communication infrastructure. Quantum computers will create vulnerabilities in critical infrastructure. While quantum computing technology can break public key encryption algorithms, the current standards do not yet exist. Government and critical infrastructure entities must work together to prepare for a new post-quantum cryptographic standard to defend against future threats.[24] CISA of U.S. analysed how the CIIs are vulnerable to quantum computing capabilities. CISA also examined CII systems' challenges when migrating to post-quantum cryptography. It has identified the urgent vulnerabilities that are most important to address first to enable a successful migration to post-quantum cryptography. The Hudson Institute report on "Risking Apocalypse? Quantum Computers and the US Power Grid" highlights the significant threat posed by potential quantum computer attacks on the U.S. power grid. It emphasises the grid's vulnerability to such attacks, which could decrypt existing encryption systems and cause catastrophic outcomes.[25]

Quantum computing, with its ability to break current asymmetric encryption methods, could allow adversaries unparalleled access to sensitive operational data. This could lead to manipulation or sabotage of the power grid's operations, from generation to distribution. The strategic decryption of communications could enable attackers to bypass security protocols, manipulate control signals and disrupt the balance between supply and demand, leading to widespread blackouts or even physical damage to critical infrastructure components. While it presents significant threats, it also offers opportunities for enhancing the security and resilience of critical infrastructure through quantum-resistant encryption and advanced simulation capabilities for grid management.

The Hudson Institute report discusses the considerable economic damage a quantum computer attack on America's electrical grid could do. It advises that the attack's impact could be far-reaching, affecting not just the immediate functionality of the power grid but also having prolonged and severe effects on the national economy. The report highlights the necessity of enhancing the grid's security against such futuristic threats to prevent potentially catastrophic economic consequences, such as the cost of a quantum blackout and the economic impact of power disruptions.

The U.S. Government is sensitive to the issue of the use of crypto computing in CIIs. It is involved with a wide range of stakeholders to prepare for a post-quantum future. In August 2023, NIST submitted for public comment three draft Federal Information Processing Standards (FIPS) designed to resist future attacks by cryptanalytically-relevant quantum computers. NIST also continues to engage with a working group of industry, academic, and government stakeholders to identify and address the challenges related to cryptographic transitions.

Government of India needs to take appropriate action to thwart the emerging threat.

9. THE ELEPHANT IN THE ROOM – CHINA

There is a big elephant in the room – China! The National Security Agency (NSA), Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. assess that China's state-sponsored cyber actors are looking for pre-positioning themselves on IT networks for destructive or disruptive cyberattacks against U.S. critical infrastructure in case of a major crisis or conflict with the United States.[26]

PRC's state-sponsored cyber group known as Volt Typhoon (also known as Vanguard Panda, BRONZE SILHOUETTE, Dev-0391, UNC3236, Voltzite, and Insidious Taurus) has compromised U.S. Department of Energy (DOE), U.S. Environmental Protection Agency (EPA), U.S. Transportation Security Administration (TSA), Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), a part of the Communications Security Establishment (CSE), United Kingdom National Cyber Security Centre (NCSC-UK), New Zealand National Cyber Security Centre (NCSC-NZ) among others. Guam is badly affected. Volt Typhoon uses malicious software that penetrates internet-connected systems by exploiting vulnerabilities such as weak administrator passwords, factory default logins and devices that haven't been updated regularly. The hackers have targeted communications, energy, transportation, water and wastewater systems in the U.S. and its territories, such as Guam. Hackers of Volt Typhoon compromised numerous Cisco and NetGear routers. Many of these routers were outdated models no longer supported by manufacturer updates or security patches. Hackers used these vulnerabilities to embed an army of sleeper cells that could be activated in a crisis.

Microsoft's 2023 report noted that the Volt Typhoon could "disrupt critical communications infrastructure between the United States and Asia region during future crises." The March 2024 report, published in the U.S. by the Cybersecurity and Infrastructure Security Agency, likewise warned that the botnet could lead to "disruption or destruction of critical services in the event of increased geopolitical tensions and military conflict with the United States and its allies." Gen Paul M. Nakasone, the director of the National Security Agency and the head of Cyber Command, said his organisations were working with partners to understand better what China was doing with the Volt Typhoon intrusions on critical infrastructure.

On January 31, 2024, FBI Director Christopher Wray told the House Select Committee on the Chinese Communist Party. "China's hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities, if or when China decides the time has come to strike. Chinese government-backed hackers target water treatment plants, electrical infrastructure and oil and natural gas pipelines. And let's be clear: Cyber threats to our critical infrastructure represent real-world threats to our physical safety." Jen Easterly, who leads the U.S. Cybersecurity and Infrastructure Security Agency, told lawmakers. "Unfortunately, the technology underpinning our critical infrastructure is inherently insecure because of decades of software developers not being held liable for defective technology. That has led to incentives where features and speed to market have been prioritised against security, leading our nation vulnerable to cyber invasion. That has to stop."[27]

The ultimate objective of China's Volt Typhoon hacker squad is to disrupt critical infrastructure in the U.S., causing disruption and panic and potentially slowing any mobilisation of forces. As China has increased its aggressiveness toward Taiwan, Volt Typhoon hackers have pre-positioned themselves in U.S. critical infrastructure in Guam and elsewhere. Tactics of Volt Typhoon hackers are focused on broad-based attacks against various small to medium-sized companies that serve as essential components of different supply chains. Understanding and countering these tactics is crucial in maintaining the security and functionality of these vital supply chains, thereby mitigating the impact of potential disruptions. Volt Typhoon campaign targeted U.S. entities that presented little value from an espionage or intelligence perspective. It could enable disruption of operational technology systems in critical infrastructure and interference with U.S. and allied warfighting capabilities.

Chinese Attack on Indian CIIs

India's CII is also under attack from foreign state and non-state actors. Targeting India's CIIs remains a key motivation for Chinese Advanced Persistent Threats (APT). RedEcho is a group of hackers which uses multiple ShadowPad malware attacks. This group is used by the Chinese Ministry of State Security and the People's Liberation Army. They have been associated with numerous ShadowPad malware attacks in the past.

Since 2020, India has faced multiple malware attacks against entities such as seaports, ten distinct Indian power sector organisations (including four of the five Regional Load Despatch Centres (RLDC) responsible for the operation of the power grid through balancing electricity supply and demand) and oil and gas facilities. Cyber incidents have been reported in Southern Region Load Dispatch Centre (SRLDC), Western Region Load Dispatch Centre (WRLDC) and North-Eastern Region Load Dispatch Centre (NERLDC) of Power System Operation Corporation (POSOCO), National Thermal Power Corporation (NTPC) Kudgi and Telangana State Transco. Suspected APTs behind these attacks include the notorious Chinese hacking group identified by the FBI as 'Barium' (or APT 41).

American cybersecurity company Recorded Future informed that in April 2022, Indian power grid institutions were attacked by ShadowPad malware. It was attributed to a Chinese group that used infected IoT devices to navigate through compromised networks and conduct espionage activities in the Ladakh region of India. Some attacks were even used to steal intellectual property. In March 2021. Cyber-intelligence company Cyfirma reported that two major Indian vaccine and pharmaceutical manufacturers, Serum Institute of India and Bharat Biotech, experienced hacking attempts against their IT systems from China-based APT 'Stone Panda'. This ATP works with the Chinese Ministry of State Security's Tianjin State Security Bureau.[28]

Some of the victims of malicious cyber attacks are: Air India, Nucleus Software, Dominos and UpStox, SII and Bharat Biotech, Mobikwik, Airtel – J&K (Airtel Denied.) JusPay, Bigbasket, Dr Reddy Laboratories, Tata Power – Mumbai, Indian Railways, Unacademy, Kudankulam Nuclear Power Plant, ISRO, Healthcare Data Leakages.[29]

10. THE INDIAN SCENARIO - A REALITY CHECK

NCIIPC

Under Section 70A(1) of the Information Technology (Amendment) Act 2008, the National Critical Information Infrastructure Protection Centre (NCIIPC) of the National Technical Research Organisation (NTRO) is the nodal agency that takes all measures including associated Research and Development for the protection of CIIs in India. NCIIPC was deemed to be created by a gazette notification with specific responsibilities for protecting all CII. While the law was amended in 2008, it would take six years before NCIIPC was formally created through a Government of India gazette notification in January 2014.

Since its inception in 2008, NCIIPC has done a tremendous job. Various organisations have come into being, cyber security professionals have been engaged, relevant bills have been introduced for legal compliance, many policies and SOPs have been formulated, and regular interactions with other government agencies, CII sectors, private sector and think tanks have taken place. Some of the policy documents that have been published on their website for the stakeholders to follow are: Cyber Security Audit: Baseline Requirements, NCIIPC COVID-19 Guidelines, SOP: Public-Private-Partnership, Guidelines for Identification of CII, Rules for the

Information Security Practices and Procedures for Protected System, Roles and Responsibilities of CISOs, Guidelines for Protection of CII, Evaluating Cyber Security in CII, SOP: Incident Response and SOP: Audit of CII/Protected Systems.

In the cyber domain, things change very fast. These baseline documents and SOPs are getting outdated. These require revision.

One can understand the necessity of raising NCIIPC under NTRO given the turf war between the concerned ministries and the bureaucratic hurdles at that time. The organisation has done a yeomen's job. But it is now time for NCIIPC to come out of the shadow of the intelligence organisation NTRO and assert itself independently.

Punitive Action. NCIIPC and CERT-In must be empowered to take punitive action in case of failure to report any breach of security in CII. Amendments to the IT Act and other acts should give statutory powers to impose penalties.

Role of Private Sector

In India, most CII sectors are owned, operated and managed by the Government. In rare cases, CII is being operated by the private sector. For instance, the Ministry of Finance notified the National Payments Corporation of India (NPCI) as a protected system. At that time, the system was being operated and managed by the Goods and Services Tax (GST) Network, which the Central Government had not yet taken over. In such cases, the private entity must follow strict compliance norms as the Government prescribes. Understanding inter-dependencies between the public and private sectors is vital to protecting CII. Even a government-owned CII will have associated IT infrastructure where private players will be involved.

One of the important examples of the role of the private sector is the adoption and usage of cloud computing. The Government or its agencies may own the CII. However, if the CII is integrated with the cloud, the government and the cloud service provider will have shared responsibilities concerning securing the CII. For example, the cloud service provider will be responsible for securing the cloud platform, and the Government will be responsible for configuring its tenant to apply appropriate authentication controls.

Specific to Power Sector

Providing security to CIIs like the power sector is a complex issue. Public sector undertakings like Power Grid Corporation of India, NTPC, etc work under the central government power ministry. They do a good job. The same cannot be said about various thermal and hydel power plants owned by the state governments.

The private sector owns almost entirely the non-conventional sources of energy. Private sector power generation capacity in thermal is 36 percent of total thermal power generation. In renewables, the private sector owns 96 per cent of the capacity. Wind and solar power contribute 32 per cent, and nuclear power contributes 1.6 per cent of total power generation. By 2030, the Government of India's fossil and renewable energy target is 50-50. We have to ensure that the private sector follows the rules set by the government. The usage of cloud computing is an apt example. When the CII is integrated with the cloud, the cloud service provider and the Government will have shared responsibilities for securing the CII. In this case, the cloud service provider will be responsible for securing the cloud platform and the Government will be responsible for configuring its tenant to apply appropriate authentication controls.

The private industry is very sensitive to any cyber breach in their respective organisations. First, they have to determine if the cyber event was an incident – data was lost, business was disrupted, etc. Finding sufficient evidence to prove loss takes time. Second, the impact has to be substantial. They always do damage control first and would not like to share the information for commercial reasons. Though the private industry is duty-bound to report any cyber security breach to government agencies, many such incidents go unreported. Tata, Ambani, Adani, etc., are significant players in the energy field. The private sector would first try to find out what happened if any breach occurs. Then mitigation efforts start. Since their reputation, stock value, etc., are involved, they would not like this information to be in the open domain. In any case, six hours is not a practical time frame for reporting. The private operators may not trust NCIIPC or CERT-In enough that these breaches will not be leaked. NCIIPC and CERT-In should develop mutual trust and ensure that this information of compromise is shared immediately to initiate mitigation action across the sectors.

Partners from the Private Sector

The U.S. Cyber Infrastructure Security Agency (CISA) has partners from civil sectors like AWS, AT&T, Google Cloud, Crowd Strike, Fire Eye, Mandiant, Palo ALTO Networks, Verizon, etc. In the U.K., GCHQ has direct links with BAE. In our case, Infosys, TCS, and other big players can be incorporated into our scheme of things. Private sector bigwigs like INFOSYS or TCS can happily work with the Government. They need to be given due recognition.

Dealing with Trusted Sources

A telecom bill was introduced that required telecom companies to secure their assets, evaluate equipment and devices for vulnerabilities and only source equipment from vendors that do not share information with foreign governments. This restriction should also apply to OT vendors.

Infrastructure with due sophistication levels needs to be available to the Government to certify that the hardware sources can be trusted. Our telecom network operators, including government agencies like BSNL, have cheap Chinese network equipment in our networks, including the CII. The only thing that concerns them is 'LI'. Defence forces are no exception. Nobody can beat the Chinese equipment when L1 is the main criterion.

Presently, the Government has taken measures so that unwanted network equipments are not put into our networks with national security implications. But those CIIs where these networks are already in place must be sanitised.

Who Regulates the Regulators?

The process of appointing regulators needs a relook. This highly technical job needs subject matter experts in niche technology areas. The generalists have a minimal role here. The issues relevant to the appointment of regulators are : the process of their competencies and professional know-how and experience.

The regulators should consult vertically and horizontally with other regulators of critical information infrastructure. These interactions should be organized under a central regulator, preferably NCIIPC.

Cyber Attack on India's Nuclear Power Plant

The September 2019 cyber exploitation by North Korean threat actor Lazarus in India's largest civil nuclear facility, the Kudankulam Nuclear Power Plant in Tamil Nadu, was certainly a wake-up call. If a cybercrime team from North Korea can penetrate India's largest nuclear power plant, surely state-backed cyberattacks can cause much more damage. The power sector comes under NCIIPC.

The questions that arise are: our concerned agencies should be able to detect these attacks before any outside cyber security company flags it, the Nuclear Power Corporation of India Limited (NPCIL) under the Atomic Energy Commission (AEC) should have come under NCIIPC, the arrangement of audits of NPCIL networks etc.

Cyber Attack on AIIMS

There was an attack on a single hospital, albeit an important central government hospital, All India Institute of Medical Sciences (AIIMS), in Delhi. From Delhi Police to everybody else got involved, Statements were coming from all and sundry. The health sector is the latest CII included in the mandate of NCIIPC. NCIIPC should have addressed media. Reactions to the attack could have been better. Since more attacks are expected, the lessons should be learned quickly and remedial measures implemented. Some of these attacks can occur even when the advisories issued by NCIIPC have been complied with. A well-trained and funded state actor can penetrate a reasonably well-defended network.

Organisations Not Under Any Oversight

NPCIL under the AEC is not the only one which does not get cyber audited. Defence services, Defence Research & Development Organisation (DRDO), Ordenece Ordnance Factory Board (OFB) and its factories and Intelligence agencies do not get audited. They do self-audit.

With the push for Atmanirbharta, many Defence Industrial Base companies have come into play. They deal with highly sensitive equipments. There is an urgent need to take them under the CII cyber security umbrella.[30] NCIIPC has the requisite security clearance and expertise. NCIIPC must be empowered to audit these organisations. One may consider the Space, Election Commission, Social Media, and the cloud services supporting CI to be Part of CII.

We have only seven CII sectors. It is time to include some more sectors as CII.

Coordination and Exchange of Information

RBI does the job of regulator for the financial sector excellently. The power sector is doing a good job. However, some other CII sectors are not doing as well. With constant exchange of information and exchange of ideas, sectors lagging behind should be pulled up rapidly to be in the same plane.

The problem is not unique to India. Some of the challenges of cyber threat information sharing identified by them are : limited relationships, funding and resources, sharing of classified or sensitive information, voluntary sharing and lack of timely sharing and actionable information.

Public Private Partnerships (PPPs)

The concept of Public-Private Partnerships (PPPs) has been in vogue for many years. NCIIPC has published a detailed SOP on PPP. The process of PPP needs to be taken to the next level.

11. RECOMMENDATIONS

NCIIPC

Command and Control. NCIIPC was raised under NTRO in 2008. Since then, NCIIPC has done a yeoman's job of protecting CII in India. Under the circumstances, it was a correct decision to raise NCIIP under NTRO. In 16 years, the organisation has grown and can work independently. The private sector is uncomfortable dealing with an organisation under an intelligence agency like NTRO.

NTRO may be taken out of NTRO's ambit and made an independent organisation under PMO.

Legal Empowerment. Though NCIIPC sends detailed advisories for CIIP, it does not have the authority to ensure implementation. Authority and responsibility go together. NCIIPC must be given legal power to take punitive action in case of failure to report any security breach in CII. Amendments to the IT Act and other acts should give statutory powers to impose penalties.

Overlap with CERT-In. The responsibilities overlap in several issues like audit, emergency response, mitigation, etc. For CIIs, NCIIPC should be the lead agency. For others, it should be CERT-In. Both can work together for emergencies, but the lead agency should be responsible for coordination, reporting and media handling.

Increase in Span. Presently, only seven sectors have been notified as CII. There is an immediate requirement to include some more sectors as CII. Space, Election Commission, Defence Industrial Base, and MoD, including Service Headquarters, DRDO, OFB, AEC, and Cloud Services, are recommended to be included as CII.

State Data Centres. All State Data Centres (SDC) were built under the National e-Governance Plan (NeGP). They keep important and sensitive information, land records, state financial data, instances of criminal record databases, etc. Another key area is the State Wide Area Network (SWAN).

Government E-Market Portal. Government E-Market Portal (GEMP) is a very critical CI. All government procurements, especially hardware/ network/ security devices and solutions, including customer geo-locations, are captured, processed, and stored through this application. Unauthorised access to this portal can divulge all necessary information to an adversary group to map which government organisation is procuring the solution, for which location, and who the supplier or service providers are. Data mining to strategise a successful attack may become easier if access is gained or data gets leaked.

SDCs, SWANs, and GEMP should be under the purview of NIIPC. The National Informatics Centre (NIC) data centres and the National Knowledge Network (NKN) link should also be covered as CII.

Vulnerability Disclosure. Vulnerability disclosure is a process through which vendors and vulnerability finders may work cooperatively to find solutions that reduce the risks associated with a vulnerability (ISO/IEC 29147).

NCIIPC runs a Responsible Vulnerability Disclosure Program (RVDP) to report any vulnerability in CII that may cause unauthorised access, modification, use, disclosure, disruption, incapacitation, or distraction[31].

Private sectors and telecom operators must disclose their vulnerabilities to NCIIPC in the required time frame.

Partners from Private Sector. The U.S. Cyber Infrastructure Security Agency (CISA) has partners from civil sectors like AWS, AT&T, Google Cloud, Crowd Strike, Fire Eye, Mandiant, Palo ALTO Networks, Verizon, etc. In the U.K., GCHQ has direct links with BAE. In our case, Infosys, TCS, and other big players can be incorporated into our scheme of things. Private sector bigwigs like INFOSYS or TCS will happily work with the Government provided they are given due recognition.

Research and Development. The NCIIPC needs to promote research efforts. We should be well versed in the latest in these technologies, especially regarding the threats emanating from emerging technologies like cloud computing, AI, or crypto communications.

Testing Labs. Testing Labs are immediately required to meet the requirements of CIIP and detect embedded malware. Testing systems and sub-systems involve examination at chip level and source code validation.

Security Standards. Security standards have also been developed for specific CII sectors. NERC-CIP is a set of standards that specifies the minimum security requirements for bulk power systems. NIST 800-13 contains some security guidelines for the telecommunications management network, and ETSI GR IP6 008 V1.1.1(2017-06), is focused on IPv6-based Internet of Things deployment.

Respective CII sectors must be made to follow the latest international security standards till such time we develop our own standards.

International Best Practices. Respective CII operators and their security teams in cyberspace must utilise the dynamic open-source toolkit that leverages experience and successes from the global community. This toolkit would incorporate proven effective materials that could be adapted from existing guidance, international standards, industry good practices, and insight/ lessons provided by respective regulatory agencies, cyber security experts, or experienced sector personnel. This model has been tried and tested. For example, looking at the cyber security of nuclear power plants gives an idea of how nuclear cyber security can be organised from open sources until its own standards are made.

The issue of concern is the cyber attack on Kudankulam Nuclear Power Plant. AEC should be made accountable for: following the available International Best Practices for the cyber security of nuclear power plants and responsibility for ensuring following of International Best Practices in the absence of its own security standards[32].

Audit

Designated organisations do regular cyber security audits of these extremely sensitive nuclear installations. Typically, auditors see whether standard instructions are complied with. Some standards like ISO 27001 are used as benchmarks. Standards such as ISO/IEC 27001 and ISO/IEC 27002 are not directly applicable to cyber security of digital I&C systems in nuclear power plants due to their specificities, including regulatory and safety requirements. IEC 62645, a new standard by the International Electrotechnical Commission (IEC) was published at the end of 2014.

The issues are: how to ensure the latest audit standards are followed, selection of internal auditors and their capability to detect sophisticated attacks like the attacks by North Korean group Lazarus.

National Cyber Security Strategy

The National Cyber Security Policy was published in 2013. In the cyber domain, many changes have occurred due to technological innovations, emerging technologies, cyber threats, and unmanaged networks. The National Cyber Security Policy of 2013 needs a major revision in parallel. All government, public, private, and academic entities must mandatorily implement cyber security policies suited to the risks in their activities and operations.

The National Cyber Security Strategy is being formulated under the National Security Council Secretariat (NSCS) and coordinated by the National Cyber Security Coordinator (NCSC). This document should be published as soon as possible.

Legal Provisions

Protection of National Critical Information Infrastructure Technology Act,2000. Sections 70, 70A, 70B, and 43A primarily constitute India's legal framework for cyber security. These sections need significant changes to empower the state and hold entities and organisations accountable for implementing cyber security. A Cyber Security law, similar to that enacted in many countries, is necessary. The law must provide for accountability of organisations, be it public, private, government or academia, for securing their cyber infrastructure

The NCSC should be the lead agency in framing cybersecurity law. The law will outline the implementation of policies to secure and ensure the resiliency of India's cyber infrastructure.

Trusted Source. Action has been taken for not allowing unwanted network equipment in our networks with national security implications. Necessary testing facilities and standards should be put into place.

Regulating the Regulators

More transparency is needed in the appointment of regulators. This highly technical job needs subject matter experts in niche technology areas. The generalists have a minimal role here.

12. CONCLUSION

\Rapid digitisation and connectivity of CII have introduced new vulnerabilities and significantly broadened the categories and reach of risks threatening the resilience of modern essential services. The multifaceted nature of CII requires a comprehensive and coordinated approach to safeguard these infrastructures against cyber threats. This requires a collective effort from government, private sector, academia and international partners.

India has immense complexity in its vastness, demography and geography. One-fifth of humankind resides here. It takes time. A lot of good things are happening. ITU graded India among the top ten cyber secure countries a few years back.

India can significantly enhance its cybersecurity posture by addressing the technical, regulatory, and human resource challenges, harnessing the opportunities presented by technological advancements, regulatory reforms, capacity building, skilled workforce development, and fostering both domestic and international partnerships.

Threat actors include States, non-state actors acting under the authority or control of a State, criminal groups and individuals. Their tools, techniques and procedures continue to evolve, in some cases in the form of highly sought-after professional and specialised services.

Advisories are issued to CII operators and other entities with timely guidance to detect and respond to threats. There is a need for modern and agile regulatory frameworks for critical infrastructure cybersecurity implementation. Successful implementation is a collaborative endeavour, requiring contributions from all stakeholders.

India faces numerous challenges in its quest to secure its CII. Technical advancements create a double predicament - offering new security tools and vulnerabilities. Emerging technologies present a larger target for attackers. Legacy systems are especially risky as they weren't designed for modern cyber threats. India's cyber regulations are scattered and lack a unified approach. This makes enforcement inconsistent and leaves gaps in protection. There is a critical shortage of skilled cybersecurity professionals. Educational programs struggle to keep pace with the evolving threats, leaving the workforce unprepared.

Despite these challenges, India has ample opportunities to strengthen its CII protection framework. Leveraging these opportunities requires a strategic and coordinated approach across various domains.

- **Tech Solutions**. AI, machine learning, and blockchain offer promising tools. They can detect anomalies, predict threats, automate responses and secure transactions.

- **Stronger Regulations**. A centralised cybersecurity authority can enforce regulations, conduct audits and improve information sharing. Updating policies and incorporating international best practices are also crucial.

- **Building Expertise**. Enhancing cybersecurity education at all levels, offering specialised training and promoting certifications are key. Public-private partnerships and attractive career opportunities can help attract and retain talent.

- **Public-Private Collaboration**. Formal mechanisms like information-sharing platforms and joint task forces can strengthen collective defences. Building trust and cooperation between these sectors is essential.

- **Global Cooperation**. Sharing threat intelligence, collaborating on research, and aligning regulations on an international level is crucial for a global defence against cyber threats. India should actively participate in international forums and leverage international expertise.

- **Strategic Actions to Bridge the Gap.** To bridge the gap between the challenges and opportunities in CII protection, India must adopt a strategic, multi-pronged approach:

- **National Strategy**. A unified plan aligned with international best practices, covering all critical sectors, emerging threats and assigning clear roles for stakeholders.

- **Enhanced Response**. Establish robust incident response mechanisms, including national and sectoral CERTs, and conduct regular drills to ensure preparedness.

- **R&D Investment**. Encouraging research and development in cybersecurity through collaboration with academia and private companies to develop advanced defences.

- **Cyber Awareness**. Public awareness campaigns and training programs to promote best practices like software updates and secure password management.

- **Stronger Laws**. Updating existing laws and introducing new legislation to tackle cybercrimes, ensure accountability and protect individual privacy.

The nation's economic prosperity, national security, and global standing all hinge on its ability to protect its CII effectively. The time for decisive action is now. By embracing a collaborative and forward-thinking approach, India can bridge the gap and emerge as a leader in the global cybersecurity domain.

ENDNOTES

1. Maj Gen PK Mallick, VSM (Retd), Cyber Security in India Present Status, Vivekananda International Foundation, Oct 2017 available at: https://indianstrategicknowledgeonline.com/web/cyber-security-in-india-present-status.pdf

2. National Critical Information Infrastructure Protection Centre, A unit of National Technical Research Organisation available at: https://nciipc.gov.in/

3. Guidelines for identification of critical information infrastructure, National Critical Information Infrastructure Protection Centre (NCIIPC), August 2019 availabe at: https://nciipc.gov.in/documents/Guidelines_for_Identification_of_CII.pdf

4. https://www.dni.gov/files/PE/Documents/2018_Cyber-Resilience.pdf

5. Jonathan Greig, Ransomware attack has cost UnitedHealth $872 million; total expected to surpass $1 billion, The Records, April 16th, 2024, available at: https://therecord.media/ransomware-unitedhealth-costs-billions-still-climbing?utm_medium=email&_hsenc=p2ANqtz-_d7VLVC3ammMYids1hSJB7v-OlqnNNd3H3lEGWsArOHyi1WfJ6RMgTk4f47fuZLVlidEEN3AXHosVfw0NFuTP4cT_QPA&_hsmi=303123790&utm_content=303128322&utm_source=hs_email

6. Chandu Gopalakrishnan, Patch These Industrial Control Systems Vulnerabilities Immediately, Warns CISA, The Cyber Express, July 7 2023 available at: https://thecyberexpress.com/industrial-control-systems-vulnerabilities/

7. Pierluigi Paganini, Pierluigi Paganini, SCADA & security of critical infrastructures, INFOSEC, July 15 2020 available at: https://www.infosecinstitute.com/resources/scada-ics-security/scada-security-of-

critical-infrastructures/

8. Guidelines for the Protection of National Critical Information Infrastructure. January 16, 2015 available at: https://www.asianlaws.org/gcld/cyberlawdb/IN/guidelines/NCIIPC_Guidelines_V2.pdf

9. Future-proof and Future-ready Framework For Protecting Critical Information Infrastructure (CII) Under The Digital India Bill, Chase India, March 2024 available at: https://www.chase-india.com/media/yw4pvnsy/future-proof-and-future-ready-framework-for-protecting-critical-information-infrastructure-cii-under-the-digital-india-bill-report-march-24.pdf

10. National Security Memorandum on Critical Infrastructure Security and Resilience, April 30, 2024 available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

11. National Security Memorandum on Critical Infrastructure Security and Resilience, April 30, 2024 available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

12. Ministry of Electronics and Information Technology (MeitY)
Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology (MeitY)
Indian Computer Emergency Response Team (CERT-In) April 28 2022 available at: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

13. Welchman Keen, SAFEGUARDING CRITICAL INFORMATION INFRASTRUCTURE RISKS & OPPORTUNITIES Whitepaper, available at: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2020/RDF2020/Post%20Forum%20Day%203/CII-Whitepaper-WK.pdf

14. National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods, Report to Congressional Addressees, September 2023 available at: https://www.gao.gov/assets/d23105468.pdf

15. Modernising policy framework for Protecting India's Critical Information Infrastructure(CII), Chase India, November 2022 available at: https://www.chase-india.com/media/pc5ddv2v/chase-india-report-

on-modernising-policy-framework-for-protecting-indias-critical-information-infrastructure-cii.pdf

16. Tianjiu Zuo, Justin Sherman, Maia Hamin, and Stewart Scott, Critical Infrastructure and the Cloud: Policy for Emerging Risk, DFRLab, July 10, 2023 available at: https://dfrlab.org/2023/07/10/critical-infrastructure-and-the-cloud-policy-for-emerging-risk/

17. Critical Cloud Computing-A CIIP perspective on cloud computing services, Enisa, February 14, 2013 available at: https://www.enisa.europa.eu/publications/critical-cloud-computing

18. Guidelines for the Protection of National Critical Information Infrastructure, National Critical Information Infrastructure, January 16 2015, available at: https://www.asianlaws.org/gcld/cyberlawdb/IN/guidelines/NCIIPC_Guidelines_V2.pdf

19. 19 Ismael Arciniegas Rueda Henri van Soest Hye Min Park, The Promise and Peril of AI in the Power Grid, The National Interest, January 25, 2024 available at: https://nationalinterest.org/blog/techland/promise-and-peril-ai-power-grid-208858

20. Rebecca Heilweil, CISA unveils guidelines for AI and critical infrastructure, FEDSCOOP, April 29, 2024 available at: https://fedscoop.com/cisa-unveils-guidelines-for-ai-and-critical-infrastructure/

21. MITIGATING ARTIFICIAL INTELLIGENCE (AI) RISK: Safety and Security Guidelines for Critical Infrastructure Owners and Operators, Department of Homeland Security, April 2024 available at: https://www.dhs.gov/sites/default/files/2024-04/24_0426_dhs_ai-ci-safety-security-guidelines-508c.pdf

22. Catherine Stupp, AI Helps U.S. Intelligence Track Hackers Targeting Critical Infrastructure, WSJ PRO, Jan 10, 2024 available at: https://www.wsj.com/articles/ai-helps-u-s-intelligence-track-hackers-targeting-critical-infrastructure-944553fa

23. Michael J. D. Vermeer, Edward Parker, Ajay K. Kochhar , Preparing for Post-Quantum Critical Infrastructure Assessments of Quantum Computing Vulnerabilities of National Critical Functions, Rand Corporation, Aug 18, 2022 available at: https://www.rand.org/pubs/research_reports/RRA1367-6.html

24. Preparing Critical Infrastructure for Post-Quantum Cryptography,

August 2022 https://www.cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf

25. Arthur Herman & Alexander Butler, Risking Apocalypse? Quantum Computers and the US Power Grid arthur_herman, Hudson Institute, Dec 15, 2021 available at: https://www.hudson.org/national-security-defense/risking-apocalypse-quantum-computers-and-the-us-power-grid

26. PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure - Resilience Engineering Institute. https://resilienceengineeringinstitute.org/prc-state-sponsored-actors-compromise-and-maintain-persistent-access-to-u-s-critical-infrastructure/

27. David Dimolfetta, China's Volt Typhoon campaign is metastasizing, Defence One, May 8, 2024 available at: https://www.defenseone.com/threats/2024/05/us-diplomats-told-china-stop-volt-typhoon-campaign-its-becoming-more-advanced-intelligence-officials-say/396400/

28. The Takshashila Institution and Anushka Saxena, The Taste of Battle', Both On-line and On-Ground, Eye on China, May 08, 2024 available at: https://eyeonchina.substack.com/p/the-taste-of-battle-both-on-line?r=14flx&utm_medium=email

29. Protection of National Critical Information Infrastructure, Vivekananda International Foundation, 2022 available at: https://www.vifindia.org/sites/default/files/Protection-of-National-Critical-Information-Infrastructure.pdf

30. SYDNEY J. FREEDBERG JR., DoD support for defense contractors' cybersecurity , Breaking Defense, March 28, 2024 available at: https://breakingdefense.com/2024/03/new-strategy-will-streamline-dod-support-for-defense-contractors-cybersecurity/

31. NCIIPC Responsible Vulnerability Disclosure Program https://nciipc.gov.in/RVDP.html

32. Maj Gen PK Mallick, VSM (Retd), Cyber Attack on Kudankulam Nuclear Power Plant – A Wake Up Call, Vivekananda International Foundation, Dec 2019 available at: https://www.vifindia.org/sites/default/files/cyber-attack-on-kudankulam-nuclear-power-plant.pdf

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