PROTECTION OF NATIONAL CRITICAL INFORMATION INFRASTRUCTURE

Vivekananda International Foundation

Protection of National Critical Information Infrastructure

Vivekananda International Foundation
New Delhi

© Vivekananda International Foundation

Published in 2022 by
Vivekananda International Foundation
3, San Martin Marg | Chanakyapuri | New Delhi - 110021
Tel: 011-24121764 | Fax: 011-66173415

E-mail: info@vifindia.org

Website: www.vifindia.org

Follow us on

Twitter | @vifindia
Facebook | /vifindia

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 The author certifies that the article/paper is original in content, unpublished and it has not been submitted for publication/web upload elsewhere, and that the facts and figures quoted are duly referenced, as needed, and are believed to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

All Rights Reserved.

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

Table of Contents

Overview and Executive Summary

India is in the next phase of digital transformation. The digital presence of economic and national security infrastructure is growing in the country at a rapid pace. All critical infrastructures are dependent and have integrated cyber technologies for management, control, and operations. Different types of software are in use. The critical systems are under various types of cyber-attacks. The complexity and numbers of attacks against critical information infrastructure are increasing and becoming sophisticated by the day.

The Parliament of India passed the Information Technology (IT) Act in 2000, and since, there has been explosive growth in the digital markets. There have been many experiments to better manage the emerging issues from cyber space in the last two decades. However, Indian cyberspace continues to be split into multiple operational spaces, and respective agencies govern each component of the space. This coordination and synchronisation among the agencies is not what it should be. This has proved to be an inefficient way to solve the whole problem. Correcting the institutional dysfunctionality present in the country would bring about the required effectiveness in the national response.

A group of experts comprising professionals engaged in the activities in government, public, private, industry representing key sectors of economics have studied and assessed the current cyber security posture, structure and recommended measures and steps needed to enhance the resiliency of cyber infrastructure in the country.

The group has reviewed many cyber incidents over the past to derive valuable lessons for the future. They have suggested various critical institutional mechanisms which are necessary to be in place to defend the country from the current and emerging threats.

The group has used the framework of Process, People and Technology to formulate the critical institutional mechanisms.

The National Cyber Security Policy 2013 needs to be revised in line with the technological innovations, emerging technologies, emerging cyber threats, open and unmanaged networks. This is necessary as there has been a sharp,

complex, and intensifying trend of cyber-attacks and cyber incidents in the country. An integrated national response covering the human as well as technical challenges involved in enhancing the resiliency of the Indian cyber space in timely manner is essential.

The group has recommended that the Indian Computer Emergency Response Team (CERT-In) and the National Critical Information Infrastructure Protection Centre (NCIIPC) may be merged into one agency and a Hub and Spoke model be used for coordinating between different sectoral regulators and the national agency for cybersecurity on policy making and its adherence. To make sure that the people are aligned in this new age warfare, these bodies have to work under and with civilian organisations and therefore be under one roof in the civilian sector. The CERT-In and NCIIPC need further significant empowerment through legislation to enforce cyber policies to prevent cyber incidents.

The group has recommended that the Cyber and Information & Communication Technology (ICT) infra of the critical, sensitive, and strategic critical sector be thoroughly audited prior to commencement of their operations by NCIIPC. This recommendation is to be enforced through appropriate legislation. Incident response is to be the sole responsibility of CERT-In.

The group has recommended changes in the curriculum by the All India Council for Technical Education (AICTE) and University Grants Commission (UGC) so that industry-standard talent is available in plenty to be tapped.

To make sure that the nation's technological prowess can withstand the cyber war, the group recommends that certain platforms be strengthened by the government, which are: National Resilience Centre for Cyber, Centralised Malware Analysis Platform, Centralised Dark Web Monitoring Platform and Centralised Standards Body. The recommendations also lay down the mechanism to encourage cooperation and coordination between government, industry, and academia in providing the best tech in the cyber security space.

The National Cyber Security Coordinator (NCSC) be empowered and given additional responsibilities. His role should be expanded to coordinate all sectors and regulators, including the space sector. All regulators must get their policies vetted prior to their notification from NCSC.

The cyber capacities of the security agencies are to be enhanced considerably, particularly the forensic capabilities. Active collaboration is needed between CERT-In, NCIIPC and security agencies.

All-State Police agencies must enhance their cyber forensic and investigation infrastructure and resources considerably.

Infrastructure to test and certify the infra and equipment concerning cyber security is the need of an hour. The NCSC must take the lead in this direction.

All the entities in government, public, private and academia must mandatorily implement

cyber security policies as suited to the risks in their activities and operations.

Cyber security law should be framed, on priority, outlining the legal responsibility and accountability of organisations to implement policies to secure and enhance the resiliency of their respective Cyber Infrastructure in the country.

In the end, the group has expressed its views on the need to future-proof the Indian Critical Information Infrastructure (CII) against emerging threats providing recommendations to improve the cyber security posture of Critical Information Infrastructure Protection (CIIP).

Acknowledgement

The group would like to acknowledge and place on record the initiative taken by Dr. Arvind Gupta, Director, Vivekananda International Foundation (VIF), on the important need in the country. He had been actively participating in group meetings and guiding immensely on various concepts and policy measures that need to be taken in the country in this area. We would also express our gratitude to Lt. Gen. Ravi K Sawhney, VIF, for his participation in the meetings and further guidance.

The group is grateful to Dr Gulshan Rai, former National Cyber Secruity Coordinator and Distinguished Fellow VIF for his invaluable guidance during deliberations.

Last but not least, thanks to Mr Anurag Sharma, VIF, for sparing a lot of time and contributing to the national cause of suggesting measures to enhance the resiliency of Indian Cyber Space and, in particular—the National Information Infrastructure.

Team

R Srivathsa Ramanathan

(Partner— Cyber Risk, Privacy & Data Protection, Mazars Business Advisors Pvt Ltd)

Mr Ramanathan, an industry-leading professional with over 38 years of experience (including 12+ years of experience in Cyber Security), has held senior positions, including as CEO of a start-up healthcare company, spanning multiple blue-chip companies (IBM, HP, PwC, HCL, Deloitte), multiple industry verticals, multiple solutions and cyber security expertise.

Bharat Panchal

(CRO, FIS Global)

Mr Panchal is a Globally recognized 'Thought Leader & Evangelist' for Enterprise Risk and Cyber Security with 27 years of experience in the banking and tele-communication industry. He worked for the National Payments Corporation of India (NPCI) for nine years and was one of the strong pillars since inception and worked in the areas of risk management, controls and governance at NPCI. He has previously worked with Kotak, Reliance, Tata and Citigroup.

Saikrishna BVS

(CEO, Saptang Labs & Pinaca Labs)

Mr Saikrishna is an IITian and ex-IRS (2011 Batch). He has extensive experience in handling complex challenges associated with securing cyberspace during his tenure at National Critical Information Infrastructure Protection Centre (NCIIPC). He runs two start-ups in Chennai, India, focused on requirements of defence & security agencies.

List of Abbreviations

AI	- Artificial Intelligence
AICTE	- All India Council for Technical Education
APT	- Advanced Persistent Threat
BFSI	- Banking, Financial Services and Insurance
CERG	- Computer Emergency Response Group
CERT-Fin	- Computer Emergency Response Team for Financial Sector
CERT-In	- Indian Computer Emergency Response Team
CI	- Critical Infrastructure
CII	- Critical Information Infrastructure
CIIP	- Critical Information Infrastructure Protection
CIIPA	- Critical information Infrastructure Protection Agency
CIP	- Critical Infrastructure Protection
CISO	- Chief Information Security Officer
DoS	- Denial of Service
DoT	- Department of Telecommunication
DEFCON	- Defense Readiness Condition (United States)
DNS	- Domain Name System
DST	- Department of Science & Technology
EMC	- Electro-magnetic Compatibility
EMI	- Electro-magnetic Interference
FTC	- Federal Trade Commission
FTP	- File Transfer Protocol
GoI	- Government of India
IoC	- Indicators of Compromise
IoT	- Internet of Things
ICT	- Information & Communication Technology
ICWA	- Institute of Cost and Works Accountants
IDRBT	- Institute for Development and Research in Banking Technology
IEC	- International Electrotechnical Commission
IMA	- Institute of Management Accountants
IP	- Internet Protocol
IRDA	- Insurance Regulatory and Development Authority
IT Act	- Information Technology Act

JNPT - Jawaharlal Nehru Port Trust
KKNPP - Kudankulam Nuclear Power Plant
LSG - Leading Small Group
LTE - Long-Term Evolution
MeitY - Ministry of Electronics and Information Technology
ML - Machine Learning
NCCC - National Cyber Coordination Centre
NCIIPC - National Critical Information Infrastructure Protection Centre
NCSC - National Cyber Security Coordinator
NCSK - National Cyber Swachh Kendra
NERC - North American Electric Reliability Corporation
NERLDC - North-Eastern Region Load Dispatch Centre
NHS - National Health Services (United Kingdom)
NSA - National Security Advisor/Adviser
NSCS - National Security Council Secretariat
NTP - Network Time Protocol
NTPC - National Thermal Power Corporation
NTRO -National Technical Research Organisation
OEM - Original Equipment Manufacturer
PaaS - Platform as a Service
PMO - Prime Minister's Office
PII - Personally Identifiable Information
PLC - Programmable Logic Controller
POSOCO - Power System Operation Corporation
PPP - Public-Private Partnership
PTP - Precision Time Protocol
R&D - Research and Development
RaaS - Ransomware as a Service
RBI - Reserve Bank of India
SaaS - Software as a Service
SCADA - Supervisory Control and Data Acquisition
SEBI - Securities and Exchange Board of India
SI - System Integrator
SOC - Security Operation Centre
SOP - Standard Operating Procedure
SRLDC - Southern Region Load Dispatch Centre
TCP - Transmission Control Protocol
UDP - User Datagram Protocol
UGC - University Grants Commission
US - United States
VIF - Vivekananda International Foundation
WRLDC - Western Region Load Dispatch Centre

Introduction

1 Background

Cyberspace has become, perhaps inevitably, a key and risky new environment of statecraft and competition between states in the twenty-first century. Cyberspace design is based on the spirit of cooperation and sharing of information and is an integral part of all activities. All critical infrastructures are now dependent on cyber and Information and Communication Technologies (ICT). The share of ICT in critical systems is rising. The ICT technologies, though a small part of the overall cost of critical systems yet they play very important and crucial roles in operations, efficiency, and productivity of the critical systems. Due to the very sensitive nature of the role, the infrastructure is exploited by the attackers to conduct relatively inexpensive attacks against the targets, and the cost of defending against such attacks is greatly increased for the defenders.

This situation has worsened in the aftermath of the pandemic. Due to the pandemic situation, all businesses have been forced to move to cyberspace for business. This change has been

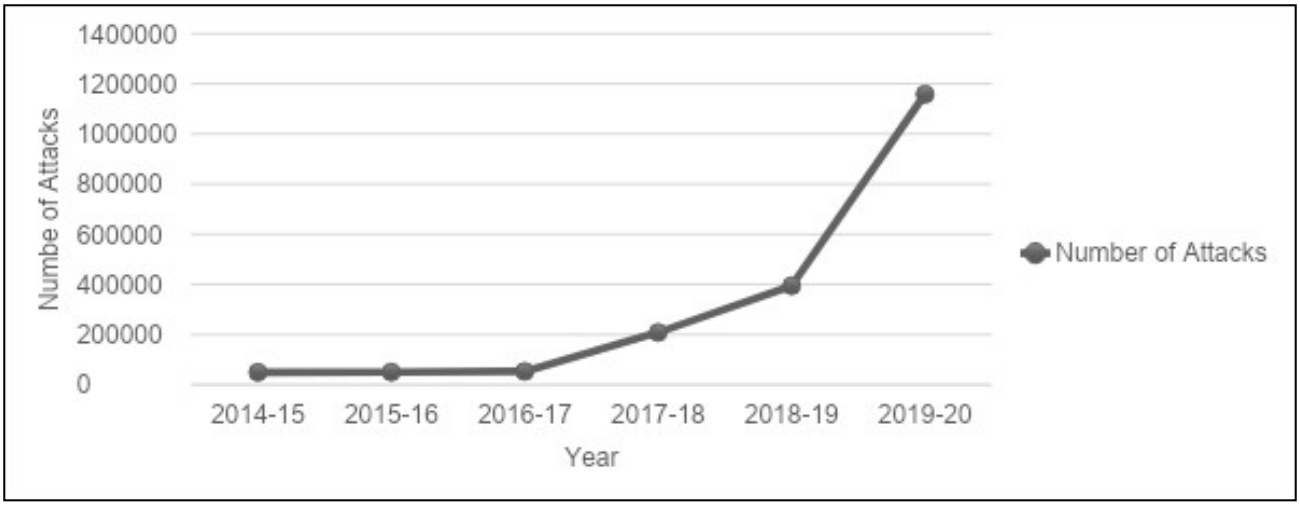


Figure 1. Cyber-attacks against Indian targets (Parliament of India, 2020)

sudden and has impacted the cyber space of the country in an irreversible manner. This has also attracted lots of attention from the cyber threat actors, who intend to secure their access to the vulnerable networks amidst the pandemic. The recent spike of attacks on Indian enterprises is a case in point – Bigbasket, Dominos, MobiKwik breaches are too frequent to be ignored or dismissed. India's threats appear to come from sophisticated and motivated state actors with access to large amounts of resources.

The world has witnessed plenty of recent attacks on Critical Infrastructures (CI). One of the most famous is the WannaCry ransomware[1] cryptoworm – a virus encrypting data and demanding money to re-access it – which, in May 2017, infected more than 2,00,000 computers in over 150 countries. The National Health Services (NHS) in England and Scotland, with over one-third of the trusts being disrupted, was one of the largest organizations hit by the attack, together with the German national railway operator Deutsche Bahn and Spanish telecommunications company Telefonica.

After just a couple of weeks, the Petya ransomware spread globally, causing tremendous disruptions to big firms in the United States (US) and Europe, including food company Mondelez and shipping giant Maersk, and dozens of key organizations in Ukraine, among those, state power plants, banks, airports, and metro. India's busiest port—Jawaharlal Nehru Port Trust (JNPT), was forced to shut down one of the terminals managed by Maersk, as their systems got compromised, which were located in Copenhagen.

Financial institutions, although comparatively having stringent privacy and security protocols, are not completely safe either. One of the biggest breaches in 2017 of Equifax saw hackers steal the personal data – including credit card details and social security numbers – of 143 million US citizens when they took advantage of a security vulnerability in the open-source framework Apache Struts, which formed part of Equifax's IT infrastructure.[2] This vulnerability had been discovered two months previously, but Equifax had not installed the required patch that had been issued to close this vulnerability. Equifax has paid the price now for its negligence, racking up a recent $700m fine from the Federal Trade Commission (FTC). In India, Hitachi payment services were impacted due to a malware attack in May 2016 which resulted in 3.2 million debit cards being compromised.[3] Customers of many banks lost more than 15 crores rupees in this attack. In August 2018, Cosmos Bank, Pune,was attacked by cybercriminals, and the bank lost Rs. 94 Crores.[4]

On 4th September 2019, the Kudankulam Nuclear Power Plant (KKNPP), one of India's most advanced such stations, was under cyber-attack.[5] Though it was contained immediately, and no damage was caused, there was every chance of massive damage had the attack gone unnoticed.

On October 12, 2020, a power grid failure in Mumbai, Maharashtra, resulted in a massive power outage, stopping trains on tracks, hampering those working from home amidst the COVID-19 pandemic, and hitting the economic

activity hard.[6] Later, this was traced to unknown Chinese entities in mounting a cyber-attack on Indian electricity infrastructure, leading to a large-scale power failure in Mumbai.

It is not just the Mumbai outage. The government also confirmed that the number of cyber-attacks on the power grid and the cases and sources of malware found in the energy supply system have gone up heavily. In the recent past, cyber incidents have been reported in Southern Region Load Dispatch Centre 1(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.

In May 2021, two major cyber-attacks on the supply chain and healthcare infrastructure were reported. On 10th May 2021, the US declared a state of emergency as a cyber-attack shut down a major pipeline—Colonial Pipeline, which operates the largest fuel pipeline in the US.[7] On 7th May 2021, the pipeline was hacked, and operations shut down, which led to fuel shortages and lines at gas stations as it delivers roughly 45 per cent of the fuel consumed on the East Coast. This attack is considered the worst cyber-attack on the US critical infrastructure. It is understood that after paying $5 Million as ransom money in Bitcoin, the pipeline started functioning after almost five days.

In the second incident, on 14th May 2021, Ireland's health service was forced to shut down IT systems over ransomware attacks by 'international criminals'.[8] A cyber-attack on Irish health service computer systems was possibly the most significant attack on the Irish state as declared by the government. The health service IT systems would take days to return to normal after being shut down, which caused a severe impact on health and social care services, especially during pandemic times.

These two major cyber incidents have clearly shown us that, increasingly, critical infrastructure and essential services are more vulnerable to widespread cyber threats. As a result, cyber security is becoming a strategic challenge requiring the highest level of oversight in the complex global industrial environment.

Looking at the intensity of cyber-attacks on critical infrastructure and the damage it can cause to the nation, it is now almost compulsory to continuously raise the bar to protect mission-critical systems from these threats by implementing best security practices, best of the technology, and highly skilled human resources. It may be pertinent to note that the current philosophy of restraining the adversaries out, or the assumption that they will be detected if they get through the first line of defence, is no longer valid.

With the exponential growth of ICT and the value offered by digitalization, businesses and governments must reimagine how we use and manage our critical infrastructure to mitigate potential risks. This involves calibrating the national blueprint to protect our critical infrastructure, allocation of adequate budget, augmentation of skilled resources and

importantly, making it bureaucracy-free. This is needed on top priority to ensure a collective, reinforced and established a framework for shared responsibility.

1.1 Rationale for Report

Indian cyberspace as a domain now appears to be fully weaponised. It is generally accepted that in the cyber domain, skill to cause damage to the infrastructure is easier to recruit, but the will to do damage is the key missing point. In the fast-changing economics and geo-political scenario, that is no longer the case.

This calls for a review of the recent cyber-attacks to answer questions from a slightly long-term perspective. The institutional establishment should be able to understand and answer the following questions:-

(a) Who are the attackers?

(b) Are the attacks part of a larger design of things?

(c) What is the response from the Indian State?

(d) How do the threat actors see the response from the Indian State?

(e) What is working in favour of the Indian State?

The focus of this report has been to develop suitable mechanisms and suggest interventions that build the capacity within the institutions of the country to safeguard India's cyberspace with reasonable confidence.

1.2 Recent Cyber Attacks in India

Cyber-attacks commonly seen in the recent past fall under two known categories – stealing of sensitive information (commercial and personal) and downright destruction of computer assets (devices/data). It is necessary to state that the list below indicates only the tip of the iceberg. It is still a widely held belief that reporting the cyber incident to law enforcement agencies leads to further scrutiny and reputational risk than any meaningful assistance to the company.

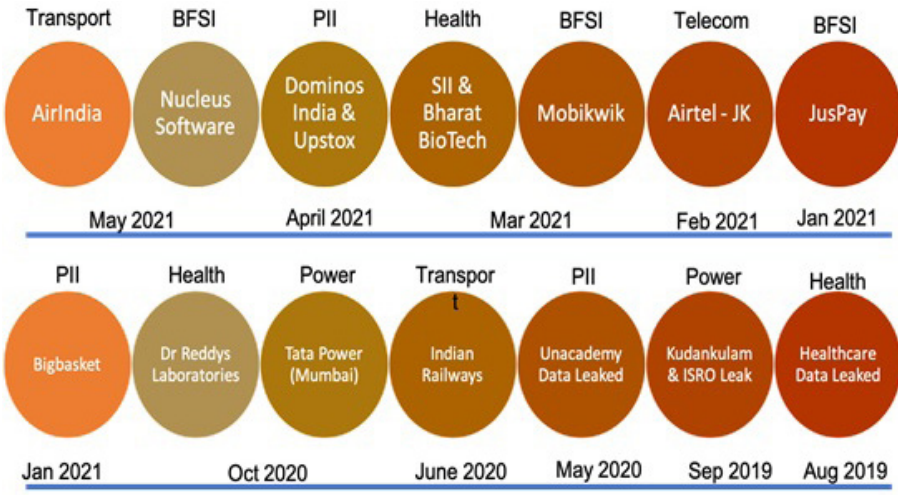


Figure 2. Recent cyber-attacks along with sector and timeline

S.No.	Victim
1	Air India
2	Nucleus Software
3	Dominos and UpStox
4	SII and Bharat Biotech
5	Mobikwik
6	Airtel - J&K (Airtel Denied.)
7	JusPay
8	Bigbasket
9	Dr Reddy Laboratories
10	Tata Power - Mumbai
11	Indian Railways
12	Unacademy
13	Kudankulam Nuclear Power Plant
14	ISRO
15	Healthcare Data Leakages

The scope of stealing sensitive information can be gauged through the news of various breaches scooped through the sources in the Dark Web. A review of the recent breaches over the last two years indicates a wide coverage of victims. Most of the victims that have garnered public attention include many top players from the critical sectors, including Banking, Transport, Telecom, Health, and Power. It is tough to verify if the breach is genuine or not due to the nature of the digital data – it is easy to copy but difficult to verify or track the source. However, when seen as a larger trend, it undoubtedly points to many more leaks that have neither been reported nor noticed by the respective companies.

A more dangerous trend is the use of ransomware by various organized crime groups in the country. While there are many cyber groups, the recent spate of attacks is attributed to more extensive campaigns by various dangerous groups such as REvil. Their ransomware attacks have disrupted and affected the operations of multiple entities. A study of the ransomware attack sample seen recently indicates the increased sophistication and its ability to evade detection by most of the commonly seen anti-malware solutions. This sophistication can be possibly seen as a result of two trends.

(a) Ransomware operators are running their operations as professional business ventures and hiring high-

grade talent.

(b) State actors are funding and sharing the knowledge of their operations to the ransomware operators.

From an Indian viewpoint, there has been a sudden surge in cyber-attacks since 2014, the wide variety of breaches, and the spike in ransomware attacks against entities based out of India. It is also not a pure coincidence that the attackers have been going over the most critical infrastructure and entities that collect massive amounts of personal data. This indicates that there could be a method in the madness, and this could be a concerted effort by a motivated threat/state actor.

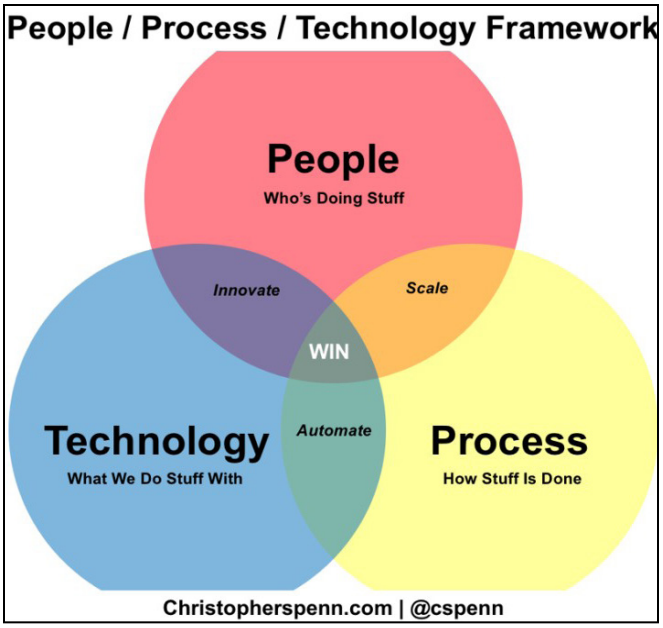
1.3 Framework for Analysis of Security Cyberspace

Digital transformation requires multiple items to come together. **People, Process & Technology** as a model for understanding the current system and proposing suitable interventions to bring desirable change.

People: Assembling the right group of people in three domains — technology, process, people at leadership roles with organizational change capacity — may be the single most important step that is needed to secure successful transformation.

Technology: In the technology domain, organizations need to make choices that support and develop the potential of the existing people and processes. People with technological depth and breadth and the ability to bring their insights into relevant areas of work/mandate of the organizations. Leaders of the technology domain must be able to communicate clearly with the big picture in mind.

Processes: Transformation requires an end-to-end mindset, a rethinking of ways to meet the requirements of the various stakeholders, seamless connection of work activities, and the ability to manage across various stakeholders when going forward. Process orientation is a natural fit for these needs. Processes design faces a big challenge in overcoming the hierarchical reporting structures mandatory in the Government infrastructure. This makes the process design a critical task that takes advantage of technological innovations.



The broader message appears to be the following:

- Scale-up what is working well with better processes.

- Innovate and develop suitable products & solutions.
- Automate as much as possible in the realm of processes to improve reliability and speed.

These three are interconnected systems requiring calibration and coordination in bringing change in all three dimensions to achieve a smoother transformation process.

2. Current Technological Trends

All critical infrastructures deploy computer information infrastructures for management, control, and communications. The government defines critical infrastructure as systems and assets, whether physical or virtual, so vital to India that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health, or safety. Critical Information Infrastructure (CII) comprises special equipment like Programmable Logic Controllers (PLCs), industrial controllers, Software-based Relays, Supervisory Control and Data Acquisition (SCADA), computers, communications, load dispatch systems, load distribution and balancer systems and sensors, etc. to control or manage production, and many other services important for the economy and daily activity. So far, the infrastructure has been deploying proprietary hardware, software, communication protocols. However, emerging technologies are now being deployed in critical systems. The systems are now being designed around Open Web Interfaces, Open general-purpose hardware & software and adhering to Open standard and Open-source products. Artificial intelligence (AI), Machine Learning (ML), next-generation communication, cloud-based systems in different models like Soft are as a Service (SaaS), Platform as a Service (PaaS) etc.,and software based on future programming are an integral part of critical infrastructure. All applications are now being designed and implemented in micro architecture catering to micro services. This trend is gaining momentum. Dual protocols, both proprietary and open-source, are embedded in the systems. There is, thus, a convergence of technologies in the modern critical systems.

2.1 Current Threat Scenario and Impact

The deployment of emerging technology has enhanced the surface and potential for misuse by preparators. Different input vectors exist, and different threats may manifest, depending on different input:

- The technology and devices used in the critical infrastructure.
- Intermediate systems and stakeholders.
- The overall architecture and connectivity with systems and sub systems.

Examples of some of the typical potential cyber-attacks and attack scenarios are indicated in the table below:

Technology		
4G/LTE/ WIFI, Cellular and Cellular network	Availability	• Signal jamming; Malicious node interface (physical attacks). • Physical tampering /breakdown of the device (physical attacks). • DoS: IP hijacking to disconnect the devices (if IP routing is used) (availability).
	Integrity	• Rogue base stations for man-in-the-middle integrity and confidentiality attacks. Requires physical proximity.
TCP/UDP (transport protocol)	Confidentiality	• Eavesdropping of commands and measurements over protocol implementations.

DNS (Domain name System)
 	
GPS spoofing and blocking
	Integrity	• Spoofing and malicious domains.
		• GPS coordinates inject incorrect phase-angle—measurement Radio Frequency equipment (integrity).
		• GPS unavailability may trigger fallback to other sources.
		• The device synchronizes to a spoofed time signal to maintain an incorrect stream of timestamps
		• Potential drifting of measurements over time.
		  • Need for proximity to PMU equipment.
		  • Changes in synchro phasor and phase angle calculations.
		• Data manipulation through software (supply chain attack).

	Availability	DoS on the real-time clock (Malicious/ Accidental insiders).
	Integrity	• Adverse effects on connection to servers (Malicious/Accidental Insiders). • Data manipulation through software (Supply chain attack).
	Confidentiality	• Backdoor access on vendor device (supply chain attack)

NTP/PTP Server	Integrity	• Master announcing wrong time. Manipulation of control loop packets for controlling clocks at slave (Integrity)
		  • Synchronizes to a spoofed time signal to maintain an incorrect stream of timestamps
		  • Affects all kinds of packets (sync, delay-request/-response packets)
		• Delaying the slave clock causes an offset of us, which escalates in the order in the synchro phasor estimation (software/ component attack)

Industrial Controllers Malware, web shell in the software and embedded subsystems	Availability	• DoS on the real-time clock (Malicious/Accidental insiders)
	Integrity	• Adverse effects on connection to servers (Malicious/Accidental insiders) • Data manipulation through software (supply chain attack)
	Confidentiality, malfunctioning, stealing of data, taking over systems through remote control	• Backdoor access on vendor device (supply chain attack)
Relay Controllers	Integrity	• Adverse effects on connection to servers (Malicious /Accidental insiders) • Data manipulation through software (supply chain attack)
	Confidentiality	• Backdoor access on vendor device (supply chain attack)

The impact of each of the scenarios presented in the table varies according to the attack vector, system specifications and the type of services that are affected. Most modern critical information infrastructure utilizes a higher level of automation that further enhances the attack surfaces. Each of the scenarios may result in very high, high, and moderate impact depending on the infra-architecture and grid systems and may disrupt services over a wider area and longer times. The introduction of fraudulent activities, as a result of the cyber-attack, can trigger different actions (either by accident or on purpose) and even cause instability of the entire infrastructure resulting in heavy losses. There are discussions of the special cyber vulnerabilities found in industrial control systems that operate critical infrastructure

facilities. These special vulnerabilities like zero-day vulnerabilities help make important critical infrastructure look like easy targets for possible cyber-terrorist attacks. There are numerous recent cyber incidents and attacks on critical information infrastructure. The gas pipeline attacks in the US, Solar Winds, the cloud infrastructure compromise in the US. The recent high impact cyber-attacks in India, e.g. cyber-attacks on power systems in Maharashtra, resulted in severe long-duration power shut down, a cyber-attack on the atomic power plant etc. Most of the technology and equipment is imported. The technological understanding of the design of a product, therefore, is a weak point in the critical infrastructure in the country.

3. Cyber Security Landscape of Country

3.1 People: Threat Actors

Reports published on the Indian Cyber Space have seen various threat actors attempting to steal information about the 'specific' targets of interest to hostile nation powers of records containing Personally Identifiable Information(PII) of the general population. It is broadly agreed that the threats to cyberspace come from the following group of threat actors based on their competence to operate in Cyberspace.

(a) Script Kiddies - Low Competence.

(b) Hackers – Medium Competence.

(c) Crackers – High Competence.

Threat actors who are operating cyberspace can be broadly categorized into three categories based on the nature of their organization and sophistication.

(a) Unorganized Mobs – Individuals or loose coalitions/factions.

(b) Organized Groups – Organised criminal enterprise.

(c) State Actors – Government Agencies or their fronts.

Threat actors' purpose for operating in cyberspace is another critical pointer, and based on the purpose, threat actors can be grouped into the following categories.

Table 1. Critical Sectors according to the NCIIPC

Category of Motive	Motive	Description
Profit	Personal Gain – Monetary or Glory	Ransomware Attackers, Blackmail, Hacktivists etc
Profit	Corporate Espionage	Stealing of Intellectual Property & Confidential Information
War	Planning & Preparing for Cyber Conflict	Disruption, Degradation and Destruction of Infrastructure.
War	Espionage	Collecting classified material or sensitive content for securing state interests

Script Kiddies are usually young and aspiring hackers with rudimentary skill sets in the art of cyber warfare or cyber espionage. They primarily rely on the tool kits, which are publicly released and ready to use exploits released in the public domain. Their capabilities are usually limited to the direct damage of the tool or exploit they are using. They do not leverage the initial access to exploit the network and computer systems to cause more serious damage.

Script kiddies' usual intent as a cyber-threat would be usually driven by either curiosity or an attempt to seek fame or glory among the community. This would usually drive them towards launching attacks using tools without a deeper understanding of the catastrophic impact they would create on an unprepared opponent. They are seen in usually working as a part of unorganised mobs with an aspiration to either join the organised groups or state actors.

Threats posed by the Script Kiddies require the agencies to be quick-footed in patching the critical systems that are vulnerable to a publicly released exploit or tool kit. The script kiddies are also usually effective in using the anonymity inherent in the design of cyberspace as a domain and pose a challenge to the investigators. They pose a tough challenge to the investigators to track, but they usually lack the skills to leave a significant adverse impact on the security of the network or system. Following the best practices in cyber hygiene and remaining vigilant about network vulnerabilities in light of freshly released vulnerabilities and exploits would keep them away.

Hackers have practical experience in understanding the way cyberspace works. They have significantly toiled and built a deeper understanding of the network architectures, common cyber defence tools and protocols. They are serious attackers who have sufficient competence to plan and launch an attack against an adversary by clearly profiling the target and customizing the exploits or tools they have access to.

Hackers' usual intent as a cyber-threat would be usually driven by profit or war. They are usually seen working as a part of organized groups or state actors. As part of an organized group, they see a larger impact of their work in terms of both learning opportunities and profit/glory.

Threats posed by the Hackers are sophisticated and require an active blue group inside the organization to keep track of this infiltration and monitor any attempts to expand the initial access gained in the course of the cyber-attack.

Crackers have a much deeper understanding of the underlying designs of cyberspace and have a very high competence level to understand and manipulate the design of cyberspace. They are the ones who identify critical vulnerabilities and develop patches for securing them. They also usually have a broader understanding of the domain and have usually worked in the past as a part of various organised groups to gain valuable experience.

Crackers' usual intent as a cyber-threat would be driven on similar lines as hackers. They are far tougher threats to organisations than hackers are. They understand the design flaws of the security and protection tools seamlessly and have the competence to exploit them. The exploits seen in the cyber world are the results of their work, and they are also usually adept at chaining multiple low-end vulnerabilities into an opening into the network. They are adversaries that cannot be stopped by deploying products and tools.

They are usually seen among the organised crime gangs, state actors and, in rare cases, actively as hacktivists.

Organised Cyber Groups

Organised cyber groups are on a global cybercrime spree. They have grown from targeting individual computers to corporate networks; organised cyber groups have evolved over the years. They have evolved from traditional ways of bringing together cyber criminals with the necessary skill-set to work on a stand-alone basis where nobody knows anyone in person and all contact is restricted to virtual contact. This allows the members of such groups to be shielded from detection by law enforcement agencies.

Ransomware has one designated task - to encrypt all data available on a system. As the connectivity throughout the globe increased, so did the dangers of Ransomware attacks. The groups' interests are not limited to money anymore. Such groups now aim at stealing data from the network before encrypting it. This serves two purposes:-

a. The threat of leaking data adds the pressure factor on the company to pay the ransom. The trust of the customers and the reputation of the company in the community should not be compromised at any cost.

b. It acts as an insurance policy. If an organization refuses to pay up, the black market of leaked data is always an option for them.

The complexity has grown too. The attacks are not based on a single malicious binary masquerading as a legitimate file anymore; the attacks nowadays are targeted campaigns.

These groups have built their business strategies with an influence from legitimate B2B models. It is a full-fledged market for professionals, recruiting people from their close circles. These groups have a straightforward playbook. They identify, attack, and then extort targets. Moreover, these attacks are not limited to motivated attackers anymore. Ransomware-as-a-Service, or RaaS, is now on the rise. It allows people to buy and/or subscribe to pre-built tools with ready-to-launch ransomware campaigns.

State Actors

China has the second-largest budget in the defence sector globally, and they perpetuate a concept called "network warfare" to house their cyber warfare. With more than 20 APTs (Advanced Persistent Threats) groups attributed

to China, it is an ever-increasing threat to the world's nations. State-sponsored (speculation) Chinese cyber groups have (allegedly) targeted various verticals of Indian critical infrastructure numerous times. Even though many of those attacks have been thwarted through the intelligence gathered by the Indian cyber agencies, it is not always possible to gather the intelligence, and therefore we must always be on guard.

Pakistan has not been inactive in the meantime. Government officials have reported the uncovering of various Pakistani groups interested in attacking the State of India. Various reports list website defacement, both government and non-government, by patriotic hackers often publicly claiming responsibility for such operations. These operations are motivated by and can lead to a physical event that causes friction between the two States.

Pakistani APTs target military and diplomatic personnel to compromise national security as part of espionage. They heavily indulge in spear-phishing attacks to gain access to social media accounts belonging to critical personnel.

3.2 Strategy and Policy

The cyber security policy of India is outlined in the "National Cyber Security Policy, 2013". This policy is supported by several guidelines and directions issued by NCIIPC, CERT-In, Department of Telecommunications (DoT), Reserve Bank of India (RBI), and other regulators of the respective economic and technical segments in the country. Along with the National Cyber Security Policy, 2013, the government had also outlined the responsibilities of the organizations/ministries/ agencies for addressing cyber security challenges. Certain provisions in the Information Technology (IT) Act, 2000 also support the cyber security policies in the country. The aim and the intention of the government at the time of announcing such policies was to establish a system clearly outlining the responsibilities of the different entities to address the cyber security challenges in the country. However, the policy and structure so far have not matured. The synergy between the entities has also not matured. It would not be wrong to infer that the present cyber apparatus of the country needs to be well equipped to handle cyber emergencies and vital resilience planning to address the emerging challenges and sophisticated, serious cyber-attacks. Unlike countries like the United States, Europe, and some Asian countries, the base for knowledge of technological products currently deployed is weak.

3.3 Institutions: Cyber Security Establishment

The cyber security system of the country is divided into Defence and Civilian systems. There are predominantly two players in the civilian sector and their counterparts in the defence setup. Each has its own versions of the incident response agency and critical information infrastructure agency. Due to the intimate nature of the activities of protection and remediation/ mitigation in the cyber security sphere, both agencies must have overlapping jurisdictions. A new institutional innovation in cyberspace

has been undertaken in the country to create the post of National Cyber Security Coordinator (NCSC).

NCSC: National Cyber Security Coordinator

Cyber Security of the nation as a major concern is shared by multiple stakeholders, and there appears to be a critical need felt at the top to streamline the national response by bringing in more focus and synergy. This led to the creation of the role of National Cyber Security Coordinator (NCSC) in the National Security Council Secretariat (NSCS). The primary job of the NCSC is to bring synergy in the functioning of the various agencies dealing with cyber security.

NCIIPC: Critical information infrastructure protection agency

The National Critical Information Infrastructure Protection Centre (NCIIPC) is a nodal agency for the Critical Information Infrastructure Protection (CIIP). The NCIIPC functions under the administrative control of the premier technical intelligence agency—National Technical Research Organisation (NTRO). Its mandate and powers emerge from the Information Technology (IT) Act.

Under the Information Technology Act, 2000, amended from time to time, a dedicated section 70A has been incorporated to identify a Nodal Agency for undertaking the job of Critical Information Infrastructure Protection (CIIP). Through a Government Notification issued on 16th Jan 2014, this job was assigned to National Critical Information Infrastructure Protection Centre (NCIIPC), under the administrative control of NTRO, a technical intelligence agency working under the control of the Prime Minister's Office. This is very similar to the setup in the US, and it appears to be intended to provide the office of National Security Advisor (NSA) and the National Security Council Secretariat (NSCS) a better way at handling the national security-related incidents in the country.

The NCIIPC has identified six critical sectors for focussing on the task of Critical Information Infrastructure Protection. The sectors appear to be very clearly focussed on ensuring they cover sectors impacting the country's economy.

The sectors are as follows: -

S No	Sector
1	Power & Energy
2	Transport
3	Telecom
4	Banking, Finance, and Insurance
5	Government
6	Strategic Public Enterprises

NCIIPC has published a number of standards and audit guidelines. So far, most of the focus of NCIIPC has been on Power Sector.

Indian Computer Emergency Response Team (CERT-In): Premier incident detection & response agency

Under section 70B of the Information Technology Act, 2000, as amended from time to time, a dedicated institution of "Indian Computer Emergency Response Group" exists. This is more popularly known as Indian Computer Emergency Response Team or CERT-In. It is part of the Ministry of Electronics and Information Technology (MeitY) and coordinates various computer emergency response groups located in the country.

The primary responsibility of the agency remains focussed on activities around the cyber security incidents,and the law mentions the following explicitly:-

(a) Collection, analysis, and dissemination of information on cyber incidents.

(b) Forecast and alerts of cyber security incidents.

(c) Emergency measures for handling cyber security incidents.

(d) Coordination of cyber incidents response activities.

(e) Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.

The CERT-In runs the BOTNET Cleaning Center. It is also known as *Cyber Swacch Kendra* for detecting botnet infections in India. It does notify, enable cleaning, and secure systems of end-users to prevent further infections.

We also have the National Cyber Coordination Centre (NCCC) working closely with the CERT-In. It is intended to screen metadata of the traffic inbound and outbound to the sensitive agencies and help in tracking and developing a coherent threat perception to the investigative agencies in protecting and defending the critical information against the threats. NCCC needs to be set up to its full mandate quickly.

3.4 Processes

Identification of Threats

Cyberspace of the country is vast and is rapidly growing, and there have been some efforts by the government and the private sector to work together in monitoring the threats to the cyber security of the specific sectors in particular andthe country in general. It appears that the majority of the threat information to the organisations is now coming from the following sources.

(a) Open-Source feeds – There are multiple places where the information about the malicious files, Internet Protocol addresses, and domains of the various attackers (popularly known as IOCs – Indicators of Compromise) are shared. Companies who are proactive usually monitor these feeds and see if their network shows any indicator of compromise.

(b) **Government Agencies** – Monitoring the Cyber Space on their own or receiving tips from anonymous or private parties about the breaches.

(c) **Cyber Security Product Companies** – Receive and Analyse various feeds of data collected open and through their products deployed in customers' premises to generate a list of attacks they see. They distribute the threat feeds to all their customers.

(d) **Dark Web Monitoring Companies** – These companies keep continuously and anonymously monitoring chatter about various companies in the dark web forums where the hackers communicate and try to sell the stolen data or access to a network.

In case of any observed breach, it will usually be intimated to the company; either the organisation's internal group will investigate and confirm quickly to the Chief Information Security Office (CISO) or engage a third-party expert to validate and confirm the breach or an attack. This leads the company to a process of reporting.

Protection from Threats

The NCIIPC has issued various guidelines for the notified Critical Information Infrastructure to follow and implement by the various CIIs.

The aim of these guidelines is to ensure that relevant security mechanisms are built into Critical Information Infrastructure as key design features. In July 2013, the National Security Advisor (NSA) had released a document listing forty controls and corresponding guiding principles for the protection of CIIs. These forty controls are grouped into five families/buckets.

They are Planning Controls, Implementation Controls, Operational Controls, Disaster Recovery and Reporting and Accountability Controls.

Planning controls ensure that security is taken as a key design parameter for all new CIIs at the conceptualisation and design level.

Implementation of Controls translates the design/conceptualisation planning into mechanisms for protecting the CII.

Operational Controls are for ensuring that the desired security posture is maintained in the operational environment

Disaster Recovery Controls ensures minimum downtime and the restoration process.

Reporting and Accountability Controls ensures adequate accountability and oversight exercised by senior management, as well as reporting to concerned Government agencies where required enforced through compliance controls.

Please refer to the NCIIPC's **Guidelines for Protection of Critical Information Infrastructure** for detailed information regarding the family of controls.[9]

Reporting and Follow-up

The process of reporting the cyber incident is assigned to the respective CISO - Chief

Information Security Officer of the organisation under attack and shared with various agencies under whose jurisdiction or license the business is carried out. The agencies then would work with the organisation to remediate or mitigate the attack. These instructions are guided by the CERT-In CISO Rules and the Information Technology (NCIIPC) Rules:

a. In case of any security incident, the victim organisation should report the same to NCIIPC at the earliest either through email: ir@nciipc.gov.in or through Helpline number (1800-11-4430)
b. The organisation must nominate a suitable official and convey his contact information to NCIIPC. This individual must be able to provide technical details related to the incident.
c. All relevant logs to NCIIPC through secure FTP hosted by NCIIPC are provided.
d. The organisation should also arrange a meeting with OEM /System Integrator (SI).

This is a summary of the Standard Operating Procedure (SOP) to be followed in case of a cyber incident. Please refer to NCIIPC's **Standard Operating Procedure (SOP)-Incident Response** guide for more details.[10]

4.Gaps

Despite increased spending, there seems to be little improvement in cyber security posture. National capability in Cyber Security is a simple sum of the Government and Private Sector capabilities. The academic partners can also aid both players. Attacks in cyber security focus primarily on the man behind the machine. Logically, the same type of protection should be available for the personal devices and the network used by the VIPs and other prominent players in the economy, public health,and order. Recent breaches of the Pegasus data revealed how easy it is to affect the decision-makers.

4.1 Processes: Complex Guidelines for Securing the Infrastructure & Reporting

Every organization has to follow instructions and directions from various stakeholders, and since the stakeholders see issues from their narrow lens, there is a lack of coherence in their instructions. Therein lies the roots of the chaos in the response. In the case of Banking, Financial, and Insurance sector companies, this includes filing details with the sectoral regulator, Department in the Union Government Level, NCIIPC, CERT-In, CERT-Fin, and local cyber crime wing of the Police. Each agency has its separate form for reporting the incidents.

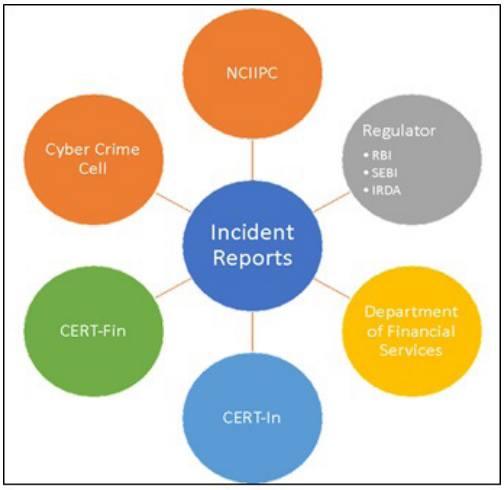


Figure 3. Reporting of cyber incidents to various agencies (BFSI Sector)

The time ticks for the CISO from the moment there is a detection of an incident. The Chief Information Security Officer (CISO) has to get a quick analysis of the scope of the breach and report the incident along with the forensic report or malware analysis report to the various agencies in myriad formats. Subsequently, in a few cases where the command and control of the attacker are identified, suitable action would be initiated by CERT-In for blocking the IP address or the domains for quick response.

Another aspect is the general lack of coordination among the various agencies. As such, the cyber security landscape is divided among the defence and civilian spaces. There are multiple distinctions among the civilian space too e.g. intelligence, state level, and union government level organizations. Many organizations are looking at cyberspace from their lens and focusing on meeting their mandates. A more coordinated outreach by the CIIP Agency would drastically reduce the amount of effort and improve the quality of the outcomes for everyone.

Institutional Quagmire

Information Technology as an item of business falls under the Ministry of Electronics and Information Technology (MeitY) under the Transaction of Business Rules. Business Allocation Rules makes the Ministry a nodal ministry for all matters affecting Information Technology. While this arrangement helps in benefiting from the subject matter expertise, it also restricts the scope for consultation and involvement of other stakeholder ministries. For example, Information Technology is now a matter of common importance for many ministries, including promoting literacy, public health, industry, trade, and national security. There is a need to evolve a robust consultative mechanism that lets the policy-making apparatus benefit from the experiences and demands of the various stakeholders.

The Information Technology Act fundamentally enables legislation for promoting e-commerce in the country. On the other hand, a national security responsibility like Critical Information Infrastructure Protection, which might require a different context and setup, now lies packed within fundamental e-commerce legislation. Consequently, tasks require swift "Chief Information Security Officer" (CISO). The IT Act attempted to mandate various criteria essential for the CISO for performing his mandate in securing the CIIs. While it is appreciable that the ministry is helping the private sector improve its governance, it is also critical to point out that the support from Government to CISOs is minuscule. CISOs and Private sector players essentially fight all cyber security battles unprepared and alone. Agencies with the rigid enforcement of compliance regulations after the attack would only further demoralize them and look at Government and the institutions in general with suspicion.

Ambiguity in Regulations

Multiple agencies attempt to regulate the critical information infrastructure members. It starts with their sectoral regulators to local law enforcement officials. Cyber security in the issue

of critical information infrastructure is best captured by a quote from Porteus (1999).[11]

> *"A Gordian knot around which many stakeholders circle, pulling on the strands that seem most promising and causing the entire thing to tighten even more snugly rather than loosen to reveal its internal structure."*

The agencies span across multiple ministries and cover the presence both at the State and national level. While national cyber security policy was released in 2013, the document did not receive wider attention and ministries continue to function without any synergy or unity of purpose in cyber security.

Impatient Experiments

Institutional innovation in the form of a National Cyber Security Coordinator (NCSC) was created to coordinate the issue of cyber security at the national level. The organisation now exists without any clearly defined roles responsibilities and without any organic connections with the ministries that are stakeholders in cyber security. This institution should be empowered in a creative way to plug the gaps in the current cyber security mechanisms of the country. However, it looks like it exists without any backward and forward linkages in the government system.

4.2 People

Lack of Direction for Manpower

The country has experienced rapid growth in the digital era. This growth has given rise to new markets and industries, all in the requirement of skilled cyber security professionals to protect them from cyber threats that are growing into more sophisticated and persistent attacks by the day. Therefore, the faculty responsible for imparting knowledge to the students should keep up with the demands of the constantly changing and updating fields of technology and global trades to offer world-class course materials to match the fierce competition in the global arena.

However, the lack of industry-experienced professionals in academia has over-emphasised theoretical knowledge, overshadowing hands-on practical experience. Lack of a well-managed apprenticeship and/or internship structure within educational institutions is a major cause of students lacking real-world experience. Professors not being able to incorporate hands-on opportunities within the curriculum itself creates an incomplete learning structure, with a scope limited to textbook material. Few students are able to look outside this influenced learning structure and venture into the environment of realistic cyber security challenges; the rest follow a guided path that is compromised with limited expertise.

The irony of the situation is that organizations rate practical experience above all else when hiring cyber security professionals. Therefore, either the student must pursue training and acquire certifications to prove their skills, or else they would be left without any practical experience and deemed as intangible assets. Since the training courses are outdated too, a false notion about lack of opportunities in

the industry is created in the students' minds because the skills they have acquired from both the academic courses and the certifications are no longer in demand.

Lack of Regulation: Institutions & policy

Training and certification institutions have a key role to play. They connect the aspiring candidates to the industry. The objective of the courses offered by the institutions is to form a bridge between what they were taught in academic courses and the skill sets required in the industry. Those training are, therefore, focussed on inculcating the candidate with theoretical concepts and practical experience. The candidates may choose which course suits them the best and pursue that particular skill set.

However, training and certification institutions have not been able to keep up with the demands of the market emerging as a response to sophisticated threats. Today, there is limited scope in the market to differentiate a qualified candidate from an unqualified one. The courses being offered by the institutions are now outdated and do not reflect the industry requirements to a large extent. A gap has formed between the requirements of the industry and the availability of an acceptable workforce where the candidates have certifications of outdated skills, while the organizations hiring cannot find candidates with suitable skill sets.

Limited expertise in the institutions widens this gap further as it leads to limited options available for training courses and certifications, which produces candidates with limited skill sets. The direct result of this is a saturated pool of skills where specific options have a large number of viable candidates, while other options have none that are suitable. This gap is ever-increasing because the degree of saturation keeps on increasing as per the trend in the market, which causes loss of valuable human resources in the other sectors.

There is a shortage for almost every position within cyber security, according to industry standards. There is a shortage of workforce required to properly maintain systems that have already been deployed, and there is an even greater shortage of workforce that can design new sophisticated security systems or improve on the existing ones.

The institutions have not been able to re-evaluate their courses, due to which their technical materials lack inputs in newer technologies such as smart contracts, block chains, Artificial Intelligence, Robotics etc. Moreover, they are not able to provide hands-on experience in these emerging areas, so even a certified candidate does not have exposure to emerging cyber security jobs in the industry. Training material needs to be planned out meticulously for maximized productivity and learning and needs to be revised regularly to ensure that the candidates enrolling in the courses are at par with the changing industry requirements.

Limited Policy Expertise

The aim of the cyber security policies in place is to build resilient and safe cyberspace for the citizens and the government. These policies define procedures and plans of actions on protecting information and information infrastructure and are drafted by political and administrative leadership that is experienced and well versed with the fundamentals of cyber security. Nevertheless, they are inadequately equipped to deal with the emerging challenges of cyberspace because they lack a fresh perspective on the updated landscape of cyber threats and the trends in the new digital age.

If the updated policies are not aligned with the requirements of the industry based on the current cyberspace capabilities, the academic courses and training certificates will continue to lag behind, and the gap will keep widening. This perpetuation worsens an already dire situation.

There is a requirement to tap the expertise available in the local private sector and global community to shape the policy landscape of the country. These experts lead the industry standards on cyber security from the front. These experts can bridge the gap between the leaders' fundamental knowledge and the current situation of cyberspace.

Lack of Open Spaces

There is a lack of space for debate and spreading best practices & proactive disclosure. The general environment is more focussed on compliance and is more concerned about professional education. This has created a culture of silence among the victims of cyber-attacks. Suffer in silence seems to be the mantra.

4.3 Technology

Lack of Indian Cyber Eco-System or Products

Cyber security has become an integral part of national security since its requirement is no longer limited to the military domain. Its influence is now crucial to everyday aspects of a nation's governance and functionality. The pandemic has only quickened this growth.

The Indian cyber ecosystem is practically non-existent due to the Indian law and investigative agencies being out of sync on this subject. They are at a deficit of skilled human resources, and there is a lack of robust architecture in cyber security at the national level, which results in non-coordination between such agencies. A strong cyber eco-system requires the unification of efforts between such agencies to assess and tackle any oncoming threats. This dysfunctional dynamic is aggravated by the gap in communication between the government and private sector in the field of cyber security that leads to the formation of fault lines within this ecosystem. With the lack of mandates for compliance and regulations to deal with the aftermath of attacks, the current security policies are unequipped to protect and endure a large-scale attack on the nation's critical infrastructure.

The lack of cyber security tools in both the software as well as hardware arena makes the indigenous cyber security community dependent on foreign players. On a deeper level, this opens up the nation to motivated attacks by State and non-State actors.

The lack of awareness has the most devastating effects at both the levels, company as well as individual. Data has been coined as the currency or oil of the 21st century, yet the Indian population does not know how to secure their data. With the advent of data-dependent technologies like Artificial Intelligence, Machine Learning and Data Analytics, the complexity has increased in the cyber security domain that directly gives rise to techno legal issues. A supervised framework that can guide the nation's citizens on the fundamentals of cybersecurity is therefore required at the earliest.

Lack of Indigenous Push

Every nation-state requires a comprehensive set of policies to govern one's action in the field of cyber security. With the difference in the resources that are available in a nation-state, their critical infrastructure varies, and so do their policies. These policies shall guide the nation towards cooperation and coordination with friendly states in fighting against espionage, as well as towards responding appropriately to a hostile state's aggressive campaigns. These policies should incorporate resources that would aid in building a dynamic cyber ecosystem, which should not be expensive and inconvenient to implement. Since every nation-state must leverage its position in all the aforementioned factors, there is no solution that would fit the bill for everyone. Every nation-state needs to build and tailor a security policy that would fit their requirements and protect their resources.

Lack of Investment in Fundamental Research

The majority of the cyber security attacks that are reported are unsophisticated attacks, with techniques that have low difficulty in launching. The inability of organizations in defending against such trivial attacks shows how they fail in implementing even a baseline of comprehensive security measures. A lack of investment in such fundamental security measures leads to non-awareness towards understanding the risks of the land.

As the nation is moving towards digitizing physical infrastructure, the exposure to cyber-attacks is increasing with it. The agencies responsible for securing such infrastructure suffer from a lack of funding in both public and private sectors. This inaction leads to a lack of skill set among the workforce as well as the lack of capability to defend and appropriately respond to a cyber-attack. The scarcity of investment thereafter does not allow the Indian cyberspace to grow as the research work is hindered, and the chances of any indigenous tool showing up in the market are diminished. This induces a perpetuation where tools are sourced from foreign players, which they use as funding to improve their platforms while the nation's cyberspace still lags.

The organizations that are willing to invest in the field struggle in determining the budget for cyber security investments and with where the investment should go. With no concrete data available about the number and nature of cyber-attacks, this makes the process trickier. Even though risk assessment models have been developed that can guide organizations in terms of investments, most organizations fail in hitting the mark because there is no generally accepted model.

5. Taking it Forward

People, Processes, and Technology are three pillars of any robust cyber security ecosystem. Any change in each one of the three systems requires changes in the other two as well. Otherwise, two systems would weaken the proposed change and work towards restoring the equilibrium or status quo. Successful transformation of the cyber security eco-system requires smoother coordinated actions in all the three categories of process, people, and technology simultaneously. Lack of effort to bring such synergy probably explains why the institutional mechanisms designed and implemented had little success in the past.

Transformational Leadership has been the widely accepted thing for bringing in the much-required change in the cyber security landscape. It can help drive the necessary change through interventions in the three components of People, Processes, and Technology.

5.1 Process

Legal Framework Changes

National Cyber Security Strategy and Policy

The National Cyber Security Policy, 2013, needs to be revised in line with the technological innovations, emerging technologies, emerging cyber threats, open and unmanaged networks. This is necessary as there has been a sharp, complex, and intensifying trend of cyber-attacks and cyber incidents in the country. An integrated national response covering the human as well as technical challenges involved in enhancing the resiliency of Indian cyberspace is the essence of time.

Audit of Cyber and ICT infra of Critical, Sensitive, Strategic sector

The group has recommended that Cyber and ICT infra of critical, sensitive, and strategic sectors be thoroughly audited prior to their operations by NCIIPC. This recommendation can be enforced through appropriate legislation. Regulations need to be issued under Sections 70, 70A and & 70B of the Information Technology Act, 2000. Incident response will be the sole responsibility of CERT-In.

Cyber Security Law

Cyber security in the country is governed by National Cyber Security Policy, 2013, regulations by regulators, guidelines by CERT-In and NCIIPC and certain sections of the Information

Technology Act,2000. Sections 70, 70A, 70B, and 43A primarily constitute the legal framework in the area of cyber security in India. These sections need significant strengthening to empower the state and make entities and organisations accountable to implement cyber security. A Cyber Security law, similar to that enacted in many countries, is the essence of time. The law must provide for accountability of organisations, be it public, private, government or academia, for securing their cyber infrastructure.

Bringing back robust institutional mechanism

The Critical Information Infrastructure sector is increasing in the private sector due to the ongoing processes of Liberalisation, Privatisation, and Globalisation. The interface between the private sector and the government agency implementing the CIIP mandate should be simple and easy to comply with. The design should ensure that the potential objective of regulation of CIIs is done in the national interest and not at a high compliance cost to the businesses.

As discussed in earlier sections, the biggest worry to the private sector is that too many agencies need to manage an adverse cyber incident. The mandatory nature of reporting to various entities makes the businesses put compliance at a higher value than the objective of ensuring business continuity. Lack of a simpler interface is detrimental to creating a friendly business environment and is also a sign of ineffective regulation.

Currently, the CIIP agency, i.e. National Critical Information Infrastructure Protection Centre (NCIIPC), is placed under the administrative control of the National Technical Research Organisation (NTRO), and the Computer Emergency Response Group (CERG) is established under the Ministry of Electronics, Information Technology (MeitY). The organizations have been created with intent during different timelines for tapping the best possible expertise and resources available in the Government to fulfil the mandate. Much water has gone down the bridge since the creation of CERT-In.

It is important to note that in the early 2000s, when the country was just recovering from the fatigue created by the Y2K bug, MeitY, which has successfully managed the transition inside the Government, appeared as the best place to host Indian CERT.

Indian Computer Emergency Response Team (CERT-In)

CERT-In was created to detect and mitigate threats emerging from the hackers who are essentially computer experts who have gone rogue. It started as a part of a larger global network of CERTs located worldwide for cooperation and coordination. CERT-In has grown into an indispensable organization in the fight against cyber-attacks in the country. However, cyber-attacks against the nation have undergone a sea change. Cyberspace as a domain has evolved from a sphere reserved for the highly technically qualified experts into a hotly contested domain for nation-states and

organized crime groups. The agency needs to significantly upgrade its resources in terms of types, nature, and number handling of cyber incidents.

National Critical Information Infrastructure Protection Centre (NCIIPC)

The NCIIPC was created in 2014 under very different circumstances. Cyberspace has emerged as one of the operational domains and is being weaponized, and the country's critical infrastructure has been going through a phase of rapid digital transformation. Another cause of concern is that cyberspace as a domain has a much simpler threshold for acquiring tools that can cause harm to others. Awareness developed in the leadership that due to a relatively low threshold in cyberspace, anti-national elements and hostile powers would use cyberspace to launch attacks against the country's critical information infrastructure. The key objective of the threat actors would be to reduce the country's ability to wage war and/or demoralize the nation. This phrase is best captured in the 'debilitating impact' part of the definition of the CIIs under Section 70(1) in the Information Technology Act 2000.

It is also critical to observe that they both have complementary roles and responsibilities. The institutional setup of the Critical Information Infrastructure Protection Agency (CIIPA) and the Incident Response and Mitigation agency under two different ministries hinders both units' smooth functioning.

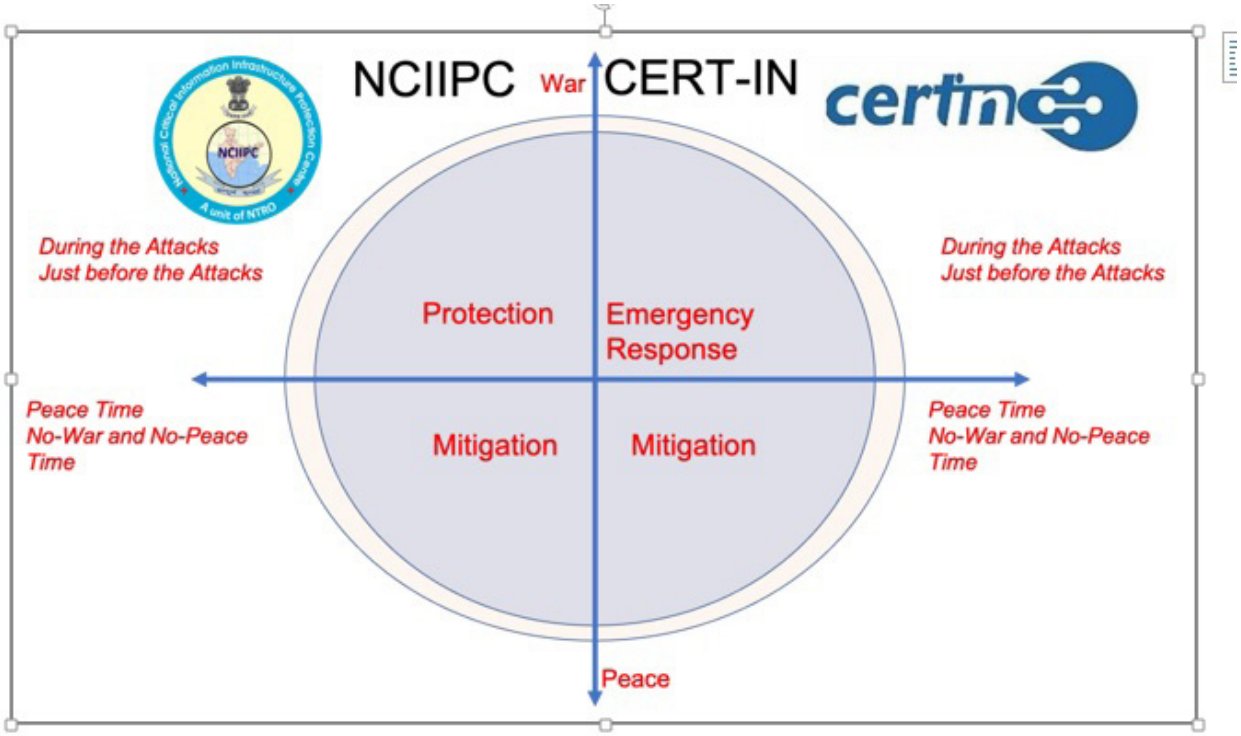


Figure 4. Mapping of the Roles and Responsibilities of NCIIPC and CERT-In

Undoubtedly, the two organizations have many different backgrounds and mandates and rightfully have 'different DNAs'. However, in executing their respective mandates, they operate on the same cyberspace and use the same tools and tap the same resource pools. There is also a need to empower the NCIIPC with accountability and responsibility.

Merging of CERT-In and NCIIPC

In the interests of efficiency and synergy, CERT-In and NCIIPC may be merged into one agency under the civilian structure. This is because both the agencies have to deal with civil and other sectors. This creates a single agency, which can be the focal point of all cyber security activity in the country. NTRO may deal with the strategic issues relating to cyber, including sensitive and strategic sectors.

National Cyber Security Coordinator: Negotiating with the Divides

The Cyber Security field in the country is fragmented in multiple ways. The primary divide is the defence and the civilian establishments. There are further divisions in the defence and civilian institutions depending on their respective jurisdictions. It would be fair to say that the cyber security system in India is fragmented.

Subsequently, it is also essential to set up an institutional mechanism that will help ensure smoother coordination of various departments' policy agendas. The latest institutional innovation, i.e., National Cyber Security Coordinator (NCSC), can act as a critical body located within the Prime Minister's Office and provide a single point of advice to the Prime Minister (PM) as a part of the significant National Security Council Secretariat (NSCS). The NCSC has to be a veteran with years of policy experience and technical expertise. The NCSC could smoothly blend both experience and expertise in his functioning and can exercise a calming and synergizing influence on the activities of the various ministries. The NCSC, as it stands, is one person in the system who retains a complete picture of the cyber security developments across the Government of India (GoI) by surpassing all divides, including defence and civilian, and has the necessary technical competence to advise the Government of India.

The mandate of the NCSC, as of date, appears to be framing broader policy and coordinating between various agencies, especially NCIIPC and CERT-In, to ensure adequate cyber security response as a country. Centralizing the execution of the policies in the hands of the NCSC may be counter-productive. This might lead to unnecessary inefficiencies and avoidable turf wars, and NCSC may not be able to secure the coordination. The senior leaders of the ministries and government must strengthen the institution by not circumventing or ignoring the advice of the NCSC, and the views should be taken into consideration on the crucial issues concerning the legislative and institutional mechanisms. Political leadership can strengthen their hands through their actions, which should help set up the institution. Another area

where NCSC's inputs may be valued would be in approving and designing schemes floated by various funding agencies acting under the banner of the Government of India. This would help resolve turf wars and ensure efficient spending of the grants to develop and equip the country to prepare for the emerging challenges in cyberspace.

The National Cyber Security Coordinator (NCSC), thus, be empowered and made responsible. The role can be expanded to coordinate all sectors and regulators, including the space sector. Regulators must get their policies vetted prior to their notification from NCSC.

Hub-and-Spoke Model for Cyber Security

Another issue for resolving is interactions between the sectoral regulators and CIIP. Law provides powers to the CIIP agency with authority for issuing directions but is silent on what happens when those directions are not implemented. It can be imagined that the order would improve the cyber security posture of the CII. It is also necessary to clarify who would bear the cost of following such directions. Another issue that requires attention is coordination between CIIP and various sectoral regulators. Their actions and directions are not in sync and confuse the sector players. For example, the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) have issued cyber security frameworks for their constituents. The framework should be issued within the broad framework of guidelines issued by the CIIP Agency for synergy and clarity to members. On the other hand, the Institute for Development and Research in Banking Technology (IDRBT), an engineering training institution exclusively focussed on banking technology and established by the RBI, has been running a first-of-its-kind security information sharing centre which is neither studied nor connected to other sectoral initiatives. Removing these legal confusions is essential for securing private sector support.

Due to the nature of the subject, there are multiple interactions required between the various sectoral regulators and the CIIP agency. The relationship between the 'Hub and Spoke' is very clearly defined. CIIP Agency is the hub, and it controls the spokes which are part of the various ministries/regulators and works very closely with them.

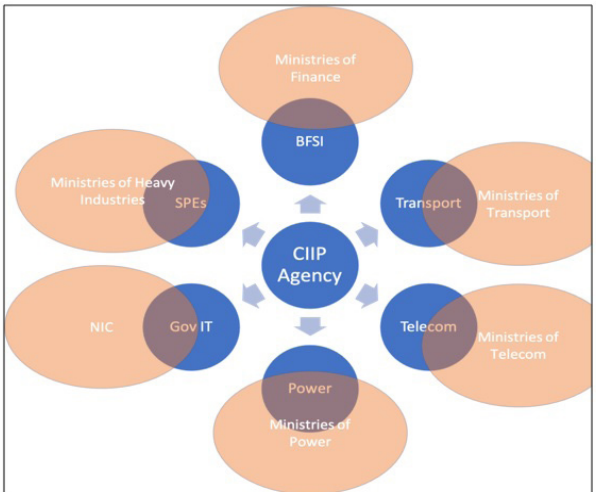


Figure 5. Relationship between Hub and Spokes

The CIIP Agency, being the hub, would drive all activities that are to be commonly implemented across the sectors, and the spokes located within the respective ministries would undertake activities that are to be customized to

the individual sectoral needs. For example, the hub issues the broader national cyber security framework and sets up standards binding on the critical information infrastructure. These standards and the framework will be consolidated and published for the sectoral-specific CIIs by the spokes. The relationship between the Hub and Spokes can be envisaged as High Courts and Supreme Court. Sector-related issues should mostly end with the spoke itself, and problems that cross beyond one sector should be necessarily escalated to the Hub level. The Hubs would also act as CERT for the respective sector itself. Since they are part of the ministry, they would be able to benefit from working closely with the sectoral regulator and be in a place to work with the private sector players seamlessly.

The ministry would appoint the head of the spoke in active consultation with the hub. Hub would specify the qualifications essential and would play an active role in running the spokes. The institutional innovation in the form of a financial advisor who reports to his department for routine financial matters and to the Prime Minister's Office (PMO) for important broad matters can be used as a great example. This would ensure that the dual control of the ministry and CIIP Agency are adhered to smoothly.

The efficiency of the hub and spoke model could be seen in the functioning of the Sector-Specific Security Operation Centre (SOC) connected to the National SOC. This model serves the sectoral players and the national hub in an excellent way.

HUB Responsibilities	SPOKE Responsibilities
Setting National Standards	Specific sectoral standards
Building National Resource pools	Efficient Utilisation for sector purposes.
Broader Policy Guidelines	Specific Instructions for sectoral players
Coordinating at national level with other stakeholders	Coordinating with sectoral players, regulator and industry lobbies.
Building National level resilience network (focussing on cyber conflict scenarios)	Developing sectoral level mitigation plans and executing & maintaining sectoral resilience network

Enforcing Accountability of the CIIP

As the old management adage goes, people focus on what is measured and not the job description. We need a national index of cyber preparedness prepared and updated regularly. Progress on the index should be a way to measure the effectiveness of the institutions. These findings then require the attention of top leadership for ensuring progress.

An Inter-Ministerial Committee on the lines of China headed by the Prime Minister (PM) is needed. China's President Xi Jinping has created the Leading Small Group (LSG) equivalent to our cabinet committee handling cyber-related issues. This would make a platform for bringing and maintaining synergy.

Expanding and Clarifying Scope of "Critical"

Attacks in cyber security focus primarily on the man behind the machine. Logically, the same type of protection should be available for the personal devices and the network used

by the VIPs and other prominent players in the economy, public health, and order. Recent breaches of the Pegasus data revealed how easy it is to affect the decision-makers. The attacks also call for the inclusion of the personal devices and networks of the government representatives to the list of critical information infrastructure.

Further, in times of pandemic and an interconnected world, many applications such as Zomato, dunzo, big basket and swiggy have become extremely critical in ensuring supplies of groceries, medicines, and food. Any disruption on their infrastructure would have a debilitating impact on the national economy, public health, and order. Pharma and vaccine companies and distribution mechanisms for the vaccine raw materials have seen a large number of attacks on their infrastructure. They also fall under the definition of critical information infrastructure.

This pandemic has highlighted the need for keeping the definition of critical information infrastructure flexible. The process for notification and, in rare cases, de-notification should be within the purview of the CIIP Agency and can be reviewed by a larger committee periodically.

5.2 People

People are the pillars and foundations of the organizations and institutional mechanisms that will defend cyberspace from the men and machines. Our dreams of becoming prosperous and strong cyber power would remain as a pipe dream without investments in developing the human resources of the country.

Market and the educational system have a symbiotic relationship. Without a robust market demand for professionals, the educational system is not expected to churn out the candidate who would meet the market's requirements. In the recent past, the focus has shifted from computer science researchers to information security researchers. This shift is created by the pressure coming from the market's rising demand for high-quality information security researchers. Multiple studies have observed that the need for cyber security professionals is very high, and this is one field that the ongoing Covid-19 pandemic has not impacted.

If we closely look at the availability of the talent pool of the information security community in India, there is a large amount of diversity in the community. It would be fair to say that a majority of the community members have no background in computer science and engineering in their graduation. Another observation that would be valid would be that most of them have spent considerable amounts of time learning and teaching themselves information security and their topics through internet-based resources and community-based training events.

It is folly to aspire to become a cyber-power without ensuring sufficient numbers of highly trained and qualified workforce available in the country.

Changing the Curriculum

Most of the human resources that are seen currently in the information security industry

are self-taught and are doing well in the information security field despite being trained in another field. This transformation happened with many struggles. We can avoid this inefficient and painful process by prescribing specialised courses. They can be approved, and teachers and resource personnel should be trained to meet the emerging demands.

Black Hat and DEFCON are considered as world's best gatherings of the information security community. On the side-lines of these conferences, multiple pieces of training are offered. A cursory look at the trainers indicates that many of them are from the Indian information security industry. It is, in a way, very disappointing to see that the world's best trainers in information security are from India, yet we find Indian students entering the market woefully underprepared.

Bodies such as AICTE and UGC must expedite the following.

a. Creation of a Bachelor of Technology/ Bachelor of Engineering in Artificial Intelligence and Information Security separately.

b. Modules for 'Training of the Teachers' for the curriculum.

c. Model of Engagement with the community to tap the trainers available in the private sector.

d. Encourage the colleges that have adopted these courses and meet quality criteria with better grading on a quality scale or showcased separately.

Career Progression & Planning for Professional Cadre in CIIs

It is also equally important that the specific sectors that fall under the critical information infrastructure category change their human resources policies to ensure that they have continuous access to high-quality cyber talent internally.

This requires changes in the individuals' recruitment, grooming, and career development and regularly calls for periodic on-the-job training, exposure visits, and workshops. Models adopted by various professional bodies for keeping their members relevant would be an excellent model to ensure that the CISOs and their immediate subordinate cadre remain vigilant and relevant.

CIIP Agency should specify minimum criteria for the candidates for the CISO Roles and his immediate subordinate roles. CIIP Agency should also help the organizations groom and develop their talent with a specific focus on the sector-based cyber threats and creating a virtuous cycle of sharing best practices between the sectoral players and ensuring the sectoral players are also aware of the trends in the attacks etc.

Regulating and Developing the Profession

For building an excellent cyber security ecosystem, we need to overcome the shortage of qualified employees in software testing, hardware design, and security topics. We need the policy to encourage new generation

institutions that create courses relevant to industry and encourage mainstreaming them. Courses such as B. Tech/M. Tech in Artificial Intelligence, Robotics, and Cyber Security are welcome in the niche segments of the industry and not widely recognized by other players. Fixing this will help India overcome the skilled workforce shortage in critical areas in a few years.

On the other hand, there is a need to set up an industry ethics body to ensure that cyber experts do not misuse their knowledge and regulate the practice of Vulnerability Assessment and Penetration Testing. This body can act like the Institute of Cost and Works Accountants(ICWA) and the Institute of Management Accountants (IMA)and promote the development of the profession in general. An efficient industry regulator is a key foundation for the realisation of the vision as a cyber power.

Synchronizing the funding

There are lots of cyber security-related projects, and institutions such as the Department of Science & Technology (DST), MeitY through CERT-In, fund research efforts. There is a need to bring synergy between them to foster the community & private sector in this field. The Indian private sector is willing to look away from services after the emergence of the Artificial Intelligence (AI) boom, which has drastically reduced the requirements of software programmers. Product development is also the next logical step for building national soft power. Our country has enough experience in delivering reliable software to the world. Product development focus could improve security posture, save taxpayers money, bring jobs and strengthen our national security.

One more thing that requires attention and focus is the government powered incubators. They get most of the funding grants and use them to build large complexes which remain primarily unused or remain on the sidelines as irrelevant due to their lack of connection with the industry and stringent funding conditions. It is tough to expect government-driven institutions to rapidly adapt to changes in a volatile and nascent industry sector such as start-ups. This approach must be re-evaluated, keeping in mind the emerging trends in funding. India sees an upsurge in the venture capital industry. The government may relook at its role change from being an inefficient funder to an efficient regulator of the venture capital industry in information security.

Creating Public Spaces for Debate & Discussion

Another major problem that affects the growth of the information security community and discussions in India is the secrecy and concerns surrounding cyber incidents.

CISOs and boards do not want to discuss cyber incidents that affect them to avoid negative media coverage or reputational risks. While this is understandable, victims and other sector players can immensely benefit from the lessons learned and solve this. This will only happen if we can create an environment free of fear and attribution. This problem is nothing

new, and many platforms have attempted to solve this. On the side-lines of the DEFCON, the top security conference in the US - a parallel community event occurs called "Sky Talks". At the event, community members openly discuss cyber incidents they encountered and solved. Attendees are expected not to quote or discuss the specifics of the issues. The Chatham House, the United Kingdom (UK) based Think-Tank, pioneered "Chatham House Rules," wherein similar discussions with a code of conduct encourage sharing knowledge without creating any controversy.

Just to recap, there is a need for a community-centred platform. This platform will help us tap like-minded experts from the industry with varied experience. Institutions like the Vivekananda International Foundation (VIF) should take the lead in giving these voices a direction and shape that would act as input to help the country grow more vigorously.

On the other hand, there is a large pool of talent available in the industry. There is no platform to tap their shared experience without the domination of bureaucracy, which sets its status quo agenda. Creating an engaging public space that is not part of the hierarchical setup would help the country tap its talent for national security and nation-building activity.

5.3 Technology

There is a need for promoting the research efforts by the NCIIPC. The NCIIPC is required to be empowered to build and develop a nationwide network for tracking and defusing cyber-attacks. The government should focus on building the local cyber ecosystem to develop tools that meet our Internet security requirements. The reason for the failure of the National Cyber Coordination Center (NCCC), National Cyber Swachh Kendra (NCSK), is apparent. Excessive dependence and lack of indigenous alternatives call for a broader study on how the research grants are spent and the outcomes are measured. One point that comes out is that there seems to be an apparent mismatch between our requirements and the focus of our Research and Development (R&D).

Encouraging the Private Sector

Most of the cutting-edge research in the world is now happening in the Private sector. The scope of the research grants is limited mainly to a few research institutions. Government should widen the grantee's network as research institutions are primarily interested in publishing research outcomes. They do not necessarily share the passion for creating usable products. Partnering with the private sector jointly for grants is a better model to build an ecosystem. It would enable true partnership for innovation and commercialization of technology developed in the national interest. Partnership and interactions also inform academia of the demands of the market. This interaction would then also include trickle-downs to make the curriculum more relevant.

The Government of India can start a national challenge with respect to cyber security products/applications where different needs of the cyber security space would be presented as challenges, and companies completing the

challenges would get milestone-based grants.

Another way of encouraging the Indian cyber security or tech ecosystem, in general, is to have a worldwide cyber security/tech/electronics expo on the lines of Dubai Expo where companies, investors, tech enthusiasts would gather at one place to talk about partnerships, latest tech happenings, investments, talent scouting etc.

5.4 Building Foundations: Testing Labs & Fundamental Research

Few national capabilities are urgently required to be built for meeting our requirements of critical information infrastructure protection (CIIP). The key national capabilities are:

Availability Of Labs And Techniques For Detection Of Embedded Malware:

As of now, techniques or procedures or standards specifying required tests for detecting the presence of any kind of embedded malware/ Trojans/cyber threat (like deliberate hard-coded or embedded logic in the chip) in the equipment/ devices /components used in systems and sub-systems of critical systems are not available in India. Published R&D literature suggests a few methods based on heuristic algorithms like power consumption pattern, electromagnetic interference (EMI)/ electromagnetic compatibility (EMC), noise emission, traffic monitoring, physical inspection of chips, internal layout at the microscopic level, etc. However, all these methods are product specific and not foolproof methods. The R&D in the area of testing critical systems is still at a nascent stage in the country. The testing of systems and sub-systems involves examination at chip-level and source code validation. To mitigate cyber security risks for reliable operation of critical systems, most of the Indian entities deploying critical infra have adopted Indian Standards, International Electrotechnical Commission (IEC) Standards and North American Electric Reliability Corporation (NERC) reliability standards for Critical Infrastructure Protection (CIP).

The requirement of mandatory testing to check for any kind of embedded malware need to be made applicable to active/intelligent equipment only and not to passive equipment/ components. In the present scenario of the limited availability of cyber testing facilities meeting the international benchmark, alternate tests like Common Criteria be adopted for equipment, components, and parts imported for use Critical System and Networks. However, to meet the huge requirement of testing, the testing facility for critical Infrastructure needs to be built at three levels:-

a. Specialised test labs at the government level.

b. Not so specialised test labs with Public-Private Partnership (PPP).

c. Day to day test laboratories to be developed by each utility.

Testing Labs & Accreditation is essential for creating an ecosystem that will further the objective of creating high-quality hardware and allied software ecosystem.

Test Suits at the National Level

India should develop standards on cyber security tests to suit the equipment being designed and developed by the Indian industry. International standards, even if followed in India, may have little relevance since they have been developed based on prevailing conditions in Europe or other countries.

National Resilience Center for Cyber

It is vital to shield the critical information infrastructure from the regular attacks that we see in cyberspace. The CIIP Agency must run a dedicated specialized "white-listed network", which is a backdoor for providing uninterrupted access of essential services to at least a limited set of citizens and institutions. The network's focus would be to ensure that, as a nation, our critical assets remain resilient, especially in the face of ongoing cyber-attacks.

Centralized Malware Analysis Platform

There is an urgent need to track and profile threats and threat actors at a national level. Accurate identification of the threat actors and their tools would help us with remedial actions. This activity requires setting up a national malware repository. The malware samples collected from the various victims' IT infrastructure should be stored and shared among the country's interested information security researchers and enterprises to build local solutions and knowledge about combatting them.

Centralized Dark Web Monitoring Platform

A complement to the same would be national agency level monitoring of the dark web actors and compilation of threat reports. Many private sector players are providing the service, and this is a matter of grave importance and a concern for the whole industry. Imagine a situation where a minor player who is part of a network of critical information infrastructure, i.e., a small bank, is breached. Small banks do not have access to the services of a private sector player who could have alerted them about the breach. This breach of a smaller player would eventually become a beachhead for further attacks against the financial system.

Because of such weaknesses, a dedicated dark web monitoring platform is required at the national and sectoral levels to take care of the sector's requirements in total. Such initiatives will help the CISOs of the sectoral players greatly. Alerting organizations about the attackers' plans and potential breaches of the network and some assistance or guidance in protecting themselves would be a great help to CISOs.

Centralized Standards body

The CIIP Agency as a hub is expected to take care of the standards. This specialized job requires bringing together a particular category of people with years of experience in the corporate world, technology pioneers, futurists, and legal experts. It is difficult to engage such a variety of talent continuously within the limitations of the government. CIIP Agency may run a small, dedicated secretariat

to constantly engage with the talent and regularly issue amended standards. The same activity would be undertaken by the spokes located within the ministry to further customize the standards to emerging needs of the sector through interactions with the sectoral regulator.

This guidance would help the national efforts and act as a critical input for the Critical Information Infrastructure members to get the security right from the beginning.

Future-Proofing against emerging threats

The critical information infrastructure sector will continue to face pressures to open up its network to seek synergies, increasing the attack surface. Emerging technologies such as the Internet of Things (IoT), extensive use of AI in manufacturing, Quantum computing and 5G have the potential to disrupt the nation's economy.

Recent trends also indicate that the attackers are more sophisticated and focussed, and the most serious concerns include Ransomware attacks, attacks against cloud platforms. CIIP Agency is expected to take this forward with the help of Hackathons and sectoral level discussions which will culminate into meaningful and informed policy decisions that would help the country.

Summary of Recommendations

In the journey of digital transformation, India is progressing with pace with digital presence of economic and national critical infrastructure. Every Critical Infrastructure (CI) is dependent and have incorporated cyber-enabled technologies for its management, control, and operations. Despite existing cyber security infrastructure in place, critical systems are under different types of cyber-attacks. In the report, group of experts who are engaged with government, public, private industries, in different capacities have assessed and recommended following measures to strengthen the existing resilience of India's cyber infrastructure. These recommendations propose a mechanism to encourage cooperation among government, industry, and academia, in the cyber security milieu.

- The National Cyber Security Policy 2013 needs a revision in parallel with advancement of technological innovations, emerging technologies, cyber threats, and unmanaged networks.
- There is an urgent need of an incorporated national response covering human resources and technical challenges involved in strengthening of the India's cyberspace resiliency.
- A single agency, comprising of the Indian Computer Emergency Response Team (CERT-In) and the National Critical Information Infrastructure Protection Centre (NCIIPC), may be formed.
- A HUB and SPOKE model can be used to establish coordination among various sectoral regulators and the national agency for cyber security on policy making and its adherence.
- The CERT-In and NCIIPC, under single agency, need further empowerment through legislation to enforce cyber policies to prevent cyber-attacks/ incidents. However, cyber incidents is to be sole responsibility of CERT-In.
- Prior to commencement of their respective operations, the NCIIPC shall perform a thorough audit of the cyber and ICT infrastructures of critical, sensitive, and strategic sectors.

- Certain platforms, such as National Resilience Centre for Cyber, Centralised Malware Analysis Platform, Centralised Dark Web Monitoring Platform, and Centralised Standards Body, must be strengthened to ensure India's technological prowess to withstand cyberwarfare scenarios.

- The National Cyber Security Coordinator (NCSC) must be empowered to coordinate with all sectors and regulators, including the Space. As an additional responsibility added, the NCSC must take lead in direction to test and certify the infrastructure and equipment in relation with cyber security.

- In line with legal responsibility and accountability of organisation, a cyber security law must be framed on priority basis. The law will outline the implementation of policies to secure and ensure the resiliency of India's cyber infrastructure.

Endnotes

1. Fruhlinger, Josh. "What is WannaCry ransomware, how does it infect, and who was responsible?", *CSO Online*, 30 August 2018, Available from: https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

2. Fruhlinger, Josh. "Equifax data breach FAQ: What happened, who was affected, what was the impact?". *CSO Online*, 12 February 2020, Available from: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
3. Ghosh, Sugata. "Hitachi hackers cashed in on security gaps in India's worst-ever cybersecurity breach", *Economic Times*, 23 February 2017, Available from: https://economictimes.indiatimes.com/industry/banking/finance/banking/hitachi-hackers-cashed-in-on-security-gaps-in-indias-worst-ever-cybersecurity-breach/articleshow/57300779.cms?from=mdr
4. HT Correspondent. "2-day hack, Rs 94 cr gone....15 months later, still no lead in Cosmos Bank cyber fraud case", *Hindustan Times*, 16 November 2019, Available from: https://www.hindustantimes.com/cities/15-months-later-no-lead-in-rs-94-cr-cosmos-bank-cyber-fraud-case/story-Ar6lk69HLJmBEyt9jGsxoK.html
5. Das, Debak. "An Indian nuclear power plant suffered a cyberattack. Here's what you need to know", *Washington Post*, 04 November 2019, Available from: https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/
6. Chari, Seshadri. "Don't rush to give clean chit to China. Mumbai power grid failure is a strong warning", *ThePrint*, 05 March 2021, Available from: https://theprint.in/opinion/dont-rush-to-give-clean-chit-to-china-mumbai-power-grid-failure-is-a-strong-warning/615969/
7. Turton, William and Kartikay Mehrotra. "Hackers breached Colonial Pipeline using compromised password", *Bloomberg*, 05 June 2021, Available from: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password
8. McNamee, Michael Sheils. "HSE cyber-attack: Irish health service still recovering months after hack", *BBC News*, 05 September 2021, Available from: https://www.bbc.com/news/world-europe-58413448
9. India. "Guidelines for Protection of Critical Information Infrastructure", *National Critical Information Infrastructure Protection Centre*, 16 January 2015, Available from: https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf
10. India. "Standard Operating Procedure (SOP)-Incident Response", *National Critical Information Infrastructure Protection Centre*, June 2017, Available from:https://nciipc.gov.in/documents/SOP-Incident_Response.pdf
11. Porteous, Holly. "Some Thoughts on Critical Information Infrastructure Protection". In: Canadian IO Bulletin, Vol. 2, No. 4 (October 1999), Available from: http://www.ewa-canada.com/Papers/IOV2N4.htm

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