KAUTILYA
SCHOOL OF
PUBLIC POLICY

CAPSTONE PROJECT

Towards a Cyber Resilient Critical Information Infrastructure of India

Capstone Project Number: CP-2026-05

Submitted by: Ms Anoushka Sharan (MPP Cohort: 2024-26)

Under the Supervision of: Dr. Vishnu S Pillai, Assistant Professor, Kautilya School of Public Policy

Cite this Report *as Sharan, A (2026) Towards a Cyber Resilient Critical Information Infrastructure of India. Available at: https://kspp.edu.in//capstone-project/towards-a-cyber-resilient-critical-information-infrastructure-of-india*

Towards a Cyber Resilient Critical Information Infrastructure of India

Submitted to Kautilya School of Public Policy in Partial Fulfillment

of the Requirement for the Degree of

Master of Public Policy (MPP)

2024-26

Anoushka Sharan

2024009398

Under the Supervision of

Dr. Vishnu Pillai

Assistant Professor

Kautilya School of Public Policy,

Gandhi Institute of Technology and Management

(Deemed to be University)

Rudraram, Telangana 502329

April 4, 2026

SELF-DECLARATION

This is to certify that the thesis titled Towards a Cyber Resilient Critical Information Infrastructure is my original work and has not previously formed the basis for the award of any Degree, Diploma, Associateship or Fellowship to this or any other University.

Anoushka Sharan

April 4, 2026

CERTIFICATE OF THE SUPERVISOR

This is to certify that the thesis titled "Towards a Cyber Resilient Critical Information Infrastructure" is original work undertaken by Anoushka Sharan under my supervision and guidance as part of hher Master's degree in this Institute. The thesis may be sent for evaluation.

Supervisor's Signature

Dr. Vishnu Pillai

04/04/2026
<Date>

Assistant Professor

Kautilya School of Public Policy

Table of Contents

Table 1 Glossary

AI	Artificial Intelligence
AIIMS	All India Institute of Medical Sciences
API	Application Programming Interfaces
APTs	Advanced Persistent Threats
BFSI	Banking, Financial Services and Insurance
CBA	Cost Benefit Analysis
CERT-In	The Indian Computer Emergency Response Team
CSIRT-Fin	Computer Security Incident Response Team for the Financial Sector
CII	Critication Information Infrastructure
CI	Critical Infrastructure
CR(s)	Cyber Range(s)
DARPA	Department of Advanced Research Projects Agency
DBT	Direct Benefit Transfer
DoS/DDoS	Denial of Services/Distributed Denial of Services
ECSO	European Cyber Security Organisation
FI	Financial Institution
GoI	Government of India
I4C	Indian Cyber Crime Coordination Centre
IADF	the Institutional Analysis and Development Framework
ICT	Information Communication Technology
IDC	International Data Corporation
IoT	Internet of Things
ISP(s)	Internet Security Provider(s)
LEAs	Law Enforcement Agencies
LLMs	Large Language Models
MeitY	Ministry of Electronics and Information Technology
MO	Modus Operandi

MTTD	Mean Time to Detect
MTTR	Mean Time To Respond
NCIIPC	National Critical Information Infrastructure Protection Centre
NCRP	National Cybercrime Reporting Portal
NIST	National Institute of Standards and Technology
NTRO	National Technical Research Organisation
US/USA	United States of America
UPI	Unified Payments Interface
PII	Personally Identifiable Information
RBI	Reserve Bank of India
R&D	Research and Development
SaaS	Software-as-a-service
SBI	State Bank of India
SOC	Security Operations Centre
TTP	Technic, Tactics and Process
VAPT	Vulnerability Assessment and Penetration Testing

Towards a Cyber Resilient Critical Information Infrastructure of India

Abstract

Cyber ranges are gaining prominence as an operational tool to achieve cyber resilience in an increasingly digitalised world. India is going through a rapid digitisation, placing its banking sector in the middle of this revolution. The Banking sector, described as the "heart of all [systems]" by a participant of this study, is also the backbone of the critical information infrastructure of India. As a response to the increasing number of cyber threats, and the lack of nationally recognised and banked upon cyber resilience initiatives, this paper attempts to position cyber ranges as a policy capacity tool to further such initiatives, arguing for the viability of having an open-source dummy cyber range that is customisable. The study uses a multimethod qualitative approach to analyse the same, opting to interview experts and professionals, and draw comparative analysis of global frameworks to narrow down on relevant insights. It uses the Institutional Analysis Development Framework by Elinor Ostrom and Policy Analysis Capacity Framework by Michael Howlett. The study proposes a cyber range component blueprint for the BFSI sector, along with a broader cyber range framework for a cyber resilient critical information infrastructure of India.

Keywords: cyber ranges as a policy tool, cyber range framework for CII, operationalising cyber resilience, BFSI specific cyber range

Chapter 1. Introduction

The fourth Industrial Revolution has ushered in a wave of innovation that actively blurs the boundary between digital, physical and biological worlds (WEF, 2016). In doing so, there has been a rapid digitalisation of national critical sectors, that has fundamentally changed how they function in most digitalising/digitalised countries. What was previously performed manually, has been completely replaced by digital software, allowing for stronger linkages across sectors (Reis & Melão, 2023). Today, we find critical infrastructure (CI) of most digitally advancing countries to be tightly coupled with each other. CI consists of physical and virtual systems, sectors and industries that are crucial to a country's services and security as a whole, such as energy, water, power grids, railways, etc (Sarker et al., 2024). These sectors, along with being critical assets of a nation, are critical for each other, i.e., the disruption in one could lead to disruption in others. The most recent example of such a case can be seen in the 2026 war between Iran and Israel-United States of America (USA/US) (S. V. Kumar, 2026). The physical disruption in oil and gas sectors has led to a crisis in many other fields. The destruction of the energy grids across the Gulf have led the countries into a national turmoil. In such a case, the CI dependency on trade, and the means to trade, also become a crucial consideration, and demand protection.

The CI, in order to have synergy in functioning and coupling, also demonstrates having a strong dependency on the information communication technology (ICT). The digital system of the CI in isolation from the physical assets is known as the Critical Information Infrastructure (CII) (GoI, n,d.). For a CI to continue functioning efficiently and delivering services, regardless of its physical condition, it requires the CII to be safe and engaged. Each country has a different understanding and listing of the CII. The financial systems are generally seen as the backbone of the critical infrastructure, and their increasing integration within the ICT, resulting in almost virtualisation of the financial system, has made them largely a CII (Mallick et. al., 2024). Vis-à-vis, the nature of risk has now shifted from being facing purely technical failures, to becoming systematic vulnerabilities with cascading consequences.

Risk is no longer isolated to any single interface. The cyber threat landscape evolves everyday with increasing sophistication and becomes more systemic in nature. Incidents suggest that there is a growing tendency of the cyberthreat actors to attack an entire industry,

taking down institutions one by one (Andrew, 2023). Not only is the modus operandi (MO) evolving, but so are the frequency and state-linkages. Thus, cyber threats are also being used as strategic weapons. State-linked attacks generally target operational disruption, that causes the shutting down of systems and disrupting critical services (Iftikhar, 2024). Russia is infamous for manufacturing the Petya and NotPetya cyberattacks aimed at the Ukrainian servers that crippled the logistics and transportation of the country, with the wiper malware spreading across systems in an uncontrollable manner. This attack, one of the most sophisticated in nature, aimed at not just data theft, but at a full system paralysis (Hypr, 2025). Second category of cyberattacks are financial and economic in nature, with their main focus being fraud, financial manipulation, and systemic economic disruption (Khiaonarong et al., 2026). These include banking malware, payment system attacks, and Society for Worldwide Interbank Financial telecommunication (SWIFT)- related frauds. Alongside the direct monetary loss, they also result in the erosion of public trust in institutions. The third category is that of cyber-physical or infrastructural attacks, also known as 'phygital'. These have a focus on critical systems like the CI, that can potentially cause a country to halt its operations, while also leading to cascading failures (Morrás, 2024). There have been instances of power grid attacks, and ransomware attacks launched at hospitals. Thus, a cyber threat is no longer limited to the virtual world. It has a hold on the real-world consequences, which cause non-negligible safety and societal impacts. Research shows that many individuals who suffered from cyberattacks, specially of financial nature, stopped using that interface altogether. They also reported mental health issues and exhibited lack of conscious and subconscious trust in systems and strangers (Waliullah et al., 2025). To sum up the cyber threat landscape, it has evolved into a flash speed of propagation, the impact is more non-linear in nature due to the interdependence, it has also become hard to identify attackers due to their sophistication in hiding trails, with the nature of the attacks now spanning across cyber, economic and geopolitical.

Governments across the world are building cybersecurity guardrails that focus on traditional ways of deterrence and perimeter defence. The instalment of certain features like firewalls fuels the assumption that threats can be/have been/will be stopped (Kovács et al., 2022). However, the inevitability of breaches, human errors and zero-day exploits hint at the contrary. Systems are repeatedly breached across the world, even in the most secure and advance countries (Guo, 2022). The question then becomes of what happens when the security systems are bypassed? In order to deal with cyber threats in real time while

continuing with its operations, an organisation requires what is known as cyber resilience (Susnjara & Smalley, 2026). Cyber resilience focuses on the ability of an organisation to detect, respond and recover from cyber threats, all the while continuing its operations and services. In order to prepare for the same, many organisations invest in tools, but fail to build the capacity and preparedness, because trainings remain theoretical in nature, and not experiential (Cedergren & Hassel, 2023). Some experts believe that organisations mistake their platforms to be cyber resilient just because they follow due procedures. The stakes for CII sectors, the BFSI for India[1], are particularly high. Press Information Bureau reports that in the decade between 2015-2025, India's domestic deposits and credit have tripled (PIB, 2025). Thus, the sector cannot afford to have a downtime. Therefore, the gap between capability and performance must be filled.

Cyber ranges (CRs) have been used widely as a tool to build cyber resilience from the ground up. CRs are controlled, simulated environments that provide for safe testing of an organisation's preparedness for facing cyber adversaries. These ranges simulate attacks, test responses and evaluate systems. They are not just training labs, they are the entire operational testing environment with clear links to resilience functionaries (Ukwandu et al., 2020). They test vulnerabilities of the system and platform, with the institutional aim to translate the findings into prevention; they simulate monitoring of activities, leading to detection; they execute attack scenarios, i.e., response; and they contribute to speeding up the recovery through testing business continuity. Far from being only technical, these ranges play a pivotal role in capacity building, system validation and institutional coordination (ECSO, 2020). Many countries consider them a best practice, and have a comprehensive framework towards them[2]. However, despite their potential, several gaps remain in India with regards to their systemic integration. There is limited adoption, which is also fragmented, the lack of a structured framework or policy initiative makes conceptualisation difficult for many, and sector-specific designs do not exist in common usage.

1.1 Background

Cyber threat Landscape of India

India wishes to posit itself as a global leader in the face of the fourth revolution (PIB, 2024), recognising the pivotal impact of the technology on systems of governance,

[1] The critical information infrastructure of India consists of thirty-five financial institutes; the list can be viewed in the Annexure.
[2] Section on Comparative Analysis of National Frameworks under Chapter 4- Secondary Data Analysis

infrastructure and public services. Since its crucial role in times of the Y2K crisis, India has set a vision to a developed and progressive state-nation by the year 2047 (Virmani, 2024). In light of this, it launched the Digital India mission, the IndiaAI roadmap and various other such initiatives to strengthen its digital backbone (GoI, 2015; GoI, 2025). India is also one of the countries to prowess digitisation of its public service delivery, in order to reduce physical barriers (Sinha et al., 2023). Its critical infrastructure now sits enveloped by strong pursuits of the ICT. As a state that also has an approach of a welfare economy, India has many schemes for direct benefit transfers (DBTs) to the vulnerable and marginalised members of its society (DBT, n.d.). Digitisation of these efforts has resulted in prevention of duplication, audit trails, mechanising accountability and traceability, enhanced connectivity and beneficiary guarantee (PIB, 2025).

In spite of these developments, India's critical infrastructure is not a stranger to the cyber threat landscape. Affecting the country's CII with increasing amounts of attacks, the cyber threat vectors are evolving in scale and sophistication, improving target-orientation and impact. Critical public service systems have also been victims of such attacks in the past. Alongside data breaches, the attacks also target DoS (denial-of-service), undermine institutional trust and inhibit the power to bring down the organisation completely by exposing the systems to vulnerabilities across digital-cum-physical ecosystems, increasingly referred to as 'phygital' (Mohammed et al., 2020).

A recent and more notable example of a threat posing such severity was the ransomware attack on the All India Institute of Medical Sciences, also known as AIIMS, in New Delhi, 2022 (Uberoi, 2023). The attack was so sophisticatedly fabricated that the institute had to put a halt on all of its digital operations for over a week, and switch to complete manual operations. The disruption caused a two-week halt in most digital operations, not just in the Delhi institute, but also with other AIIMS units across the country to stop the spill-over. Multiple servers, private healthcare data of patients and their treatments, along with the delivery of healthcare in a premier national medical institution were among the many things compromised (Management Alliance, 2022).

This incident, in all its vastness and the sheer magnitude, brought forth some of the evolved characteristics of the cyber threat landscape and new attack vectors, particularly in the context of the CII.

Firstly, there was a direct and a largely "felt" impact of the cyber incident beyond just data loss and stagnation. It percolated to the failure of public service delivery systems (Management Alliance, 2022). The implication makes this a case of DoS, which, this paper

argues to be a breach of right to health- an integral part of the fundamental human right to life. Further, due to a disruption to standard operations developed as part of the daily functions at the hospital, an increased risk of human error lurked, due to the delays and creeping inefficiencies (Management Alliance, 2022).

Second, the scale of data exposure in the AIIMS attack underscores the risks associated with large, centralised digital infrastructures. Approximately 1.3 terabytes of data was encrypted, including sensitive patient records and administrative data (Management Alliance, 2022). The potential compromise of personally identifiable information (PII) highlights the intersection of cybersecurity with privacy, governance, and national security concerns.

Third, the incident revealed gaps in organisational preparedness and resilience mechanisms, including issues such as inadequate network segmentation and security practices, which enabled the persistence and spread of the attack. These vulnerabilities are not isolated to the healthcare sector but are indicative of broader systemic weaknesses across CII sectors.

1.2 BFSI-Specific Cyber Threats

Along with the three core threats of operational, economic and phygital attacks, the BFSI sector is also exposed to supply chain vulnerabilities- from the third parties in particular (Adelusi, 2023). Fintech integration also plays a role in complicating the threat landscape further as they introduce new attack vectors into what could otherwise have been safer systems with limited vulnerabilities (Dervishaj et al., 2025). The National Cyber Security Policy of 2013 states that credential theft and phishing were already party to the threat landscape of the BFSI. However, increasing insider threats also continue to exploit humans in the system, while advanced persistent threats (APTs) target the high value organisations for espionage and infiltration (S. Sharma et al., 2025). This implies that the cyber threat landscape even for the BFSI is increasingly multi-tiered and coordinated.

1.3 Cybersecurity Landscape of India

The Indian regulatory landscape has four major actors that determine the laws, policies, frameworks and guidelines to protect the cyberspace. The Indian Computer Emergency Response Team, or the CERT-In, is the national nodal agency for cybersecurity incident response in India, operating under the Ministry of Electronics and Information

Technology (MeitY). Alongside cyber incident management, it issues advisories with the objective of enhancing national resilience against cyber threats. The Section 70B of the 2008 Amendment to the Information Technology Act[3] authorises the agency to collect, analyse and disseminate information on cyber incidents, and gives it statutory powers to release national guidelines and directing ISPs for taking preventive measures and course correction (GoI, 2008). CSIRT-Fin, Computer Security Incident Response Team for the Financial Sector, is the nodal agency under the CERT-In dedicated to the BFSI sector.

The National Critical Information Infrastructure Protection Centre (NCIIPC), under the aegis of National Technical Research Organisation (NTRO), is responsible securing the Indian CII against cyber threats. Its focus areas include critical sectors of power, banking, telecom, energy, transport and government networks. It identifies vital assets, assesses their vulnerabilities and issues security guidelines to the designated sectors. It also promotes partnership and capacity building. In 2023, it launched a National Cybersecurity Reference Framework[4] (NCRF) and held Bharat Cybersecurity Exercise (BCX) in collaboration with the Rashtriya Raksha University (PIB, 2024).

The Indian Cyber Crime Coordination Centre (I4C), under the Ministry of Home Affairs, is the nodal agency for cybercrime coordination. It has seven verticals for the purposes of research and development (R&D), joint cooperation across law enforcement agencies (LEAs) of different states, threats analytics, child sexual exploitative and abuse material, and for training purposes. It also operates and handles the National Cybercrime Reporting Portal (NCRP).

Finally, the Reserve Bank of India (RBI), is the central bank and the sector regulator of the BFSI. The RBI has spearheaded the implementation of security guardrails around the digital revolution, particularly for systems like the Unified Payments Interface (UPI), and the advent of artificial intelligence (AI), issuing guidelines like the FREE-AI[5]. The RBI is one of the most proactive regulators across sectors, which also oversees the ethical development and integration of cryptocurrency and virtualisation of assets (IIPA, 2025).

[3] The Information Technology Act, 2000, has been amended been twice, in 2008 and 2026.
[4] Though launched, the NCRF was supposed to be in public circulation in 2023 itself. However, there has been no update regarding the same.
[5] Framework for Responsible and Ethical Enablement of Artificial Intelligence, RBI, 2025

1.4. Cyber Ranges For India

While the Indian ecosystem is well-placed and detailed, the number of systems and the chains of communication fragment the implementation of many policy initiatives. Most work of these bodies is also compliance focused (Sharma, 2022). At the moment of cyber incident occurrence, the communication gaps and lack of synergy between institutions and LEAs opens up a window for the cyber threat actor to extract more and cover tracks (DSCI, 2023). The system is long and complex, which is why it is important for public-facing institutions, specially the banking sector which also doubles up as the CII of the country, to have institutional capacity to respond to these threats. As of now, there is a gap of integration and simulation comprehension- although the RBI does promote red-teaming exercises as part of its directory. However, traditional methods lead to failure because they are focused on theoretic training and no real testing (CERT-In, 2025). This becomes a vital sign for India to develop and adopt sector-specific CRs which focus on real-time simulations, monitoring and testing.

1.5 Problem Statement

Analysing the ambitious prowess and the journey already started by India versus the infrastructural safeguards, or the lack of, reveals the gap that this study aims to cover: between technological dependence and defensive depth. As of now, India lacks an adequate policy or a framework that addresses the rising concerns and threat vectors in cyberspace. CII of India is particularly vulnerable, containing nationally significant data while also being a repository of the most marginalised of the country. While numerous initiatives have been made, they remain fragmented in nature. I posit that active measures for cyber resilience require structure and national cognisance. The study aims to lay down a national framework for cyber ranges, aimed at the operational capacity of the policy acumen for cyber resilience. The research questions this paper aims to answer are:

What are the factors that shape the cyber resilience capacity of India? What components of cyber ranges overlap and differ in the cyber ranges of critical sectors in India? What could be a potential cyber range design for the BFSI, and a supporting national framework to protect the CII? How can these factors turn into policy tools, specially fitting the context of CIIs?

The study sees cyber resilience as a construct, with CII of India as the unit of analysis. It will be mapping the factors of cyber resilience that may constitute actionable policies for

the same. It will also explore probable frameworks for cyber resilience, such as creation and adoption of cyber-ranges.

Chapter 1 Summary

The chapter contextualises the study to rapid digitalisation and increasing dependence on CII, particularly of the BFSI. It outlines cyber threats and examines India's cybersecurity landscape, including key regulatory and institutional actors. It situates CRs as tools for simulation-based resilience and highlights gaps in adoption. The chapter culminates in the problem statement, presenting the disconnect between digital dependence and operational preparedness, outlining the need for a structured CR framework.

Chapter 2 – Literature Review

There is no denying the fact that the future of organisations and institutions is digital (Elia et al., 2024). A study by International Data Corporation on the Building Blocks of Cyber Resilience looked at the creation of different kinds of jobs ever since digitisation, which includes Chief Information Officer, and Chief Security Officer (IDC, 2026). These directly hint at the stakes being high for any organisation that wishes to exist digitally. As a matter of fact, the existence of digital organisations depends on the cyber resilience of that organisation. It not only ensures digital resilience, but also is one of the primary ways to ensure financial and operational resilience (IDC, 2026). A report by IBM found that public-facing applications were the most vulnerable (Nadeau, 2025). In face of the looming threats, IDC suggests that in order to have an effective decision making approach towards multidimensional resilience, an organisation must back itself up with a governance framework that prioritises cyber resilience, provides standards through benchmarking and provides clear policy settings (IDC, 2026).

The CERT-In defines cyber resilience as the "ability of [an] organisation or business to anticipate, withstand, contain, recover and evolve [from cyber adversaries]" (CERT-In, 2019). Similarly the National Institute of Standards and Technology (NIST) of the USA defines cyber resilience to be "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks or compromises on systems that include cyber resources" (Ross, et. al., 2024). Traditionally, cyber security can be seen to over-rely on tools, that also may delay patching and in fact fail to stop the attacks altogether. The approach has been prevention-focused, and its reliance on tools neglects the vulnerabilities that persist due to human error despite these systems. Moreover, the antidote of these technologies is built at a faster pace by the threat actors than the anticipation of threat, and therefore, the failure of

implementation. Research suggests that attacks are unavoidable, and that systems, by the virtue of threat vectors, will be compromised (Mersinas et al., 2024; Yeboah-Ofori et al., 2023; Alnajim et al., 2023). However, such compromises, while having devastating impacts on the organisation, also bleed the trust of the users of the institution. When the 1.3TB data was found encrypted and over 30 million patient records were leaked from AIIMS, public trust on its national medical infrastructure and healthcare facility as a whole, saw erosion (The Hindu Bureau, 2022). While cyber security tries to prevent attacks, cyber resilience assumes failure, equips the system to fight with its own capacity, and finds ways to continuity (Tzavara & Vassiliadis, 2024). Cyber resilience, therefore, matters at a systemic level, and not just organisational or institutional levels.

In a cyber ecosystem, the influences and relationships of various actors are very sensitive and complex (Steininger, 2025). Cyber resilience posture of an entity, therefore, also depends on the security level of its partners, subcontractors, customers, service providers, and the CI connected to it. Thus, not only is the ecosystem highly interconnected, it also presents cascading risks across systems which can cause cross-sector disruptions. These disruptions can be termed as an ‘attack’ if they compromise any one of the “CIA” impacts, i.e., confidentiality, integrity or availability (Morgan, 2022). A compromised entity suffers from reputational damage, operation disruption, and an increased risk of driving current and potential customers away. CII safety and services is part of the social contract of a government with its public (George et al., 2024). The failure to safeguard it translates into its violation, resulting into trust deficit between the public and its government. Financial loss, especially in a free-market, is operational and is an individual-facing damage- against which the protection should come from the state (Maurer et al., 2021). However, the landscape is grippling with increasing complexities. By the next five years, the adoption of internet of things (IoT) devices will reach around thirty-two billion (Statista, 2026). Banks are using IoT in withdrawal and deposit systems, in credit assessments, targeted product delivery, etc (Tella & Raju, 2020). Cloud storage is becoming an integral part of the BFSI supply chain, increasing the dependency on such platforms. The interaction of application programming interfaces (APIs) and its exposure are also on the rise (Alzide, 2024). While such integration and advancement is a positive step, they also increase and expand the threat landscape. Mobile banking, accessible from simple devices, while increasing accessibility, also leave open vulnerabilities, along with people who are vulnerable (Hossain et al., 2025). Acquisition of credentials through sophisticated attacks or manipulable attempts can grant access to client-specific information in the Software-as-a-service (SaaS) platforms, compounding the

vulnerabilities. This is why resilience becomes a critical must-have across industries (Tang et al., 2024).

The nature of cyber threats is dynamic across time. The National Cybersecurity Policy of 2013 includes "identity theft, phishing, [hacktivism], cyber terrorism, compound threats targeting mobile devices and smartphones, compromised digital certificates, APTs, denial of services, supply chain attacks and data leakage..."(MeitY, 2013). As of 2026, entry of large language models (LLMs) and enhanced social engineering has lowered the barriers for threat actors, while introducing new vulnerabilities in the system. These would include man-in-the-middle attacks, deepfakes, algorithm-manipulation, evading emails, generating malware. Lending credibility has become easier and more thorough by exploiting services like GitHub pages, cloud platforms, and messaging applications like Discord and Telegram (SISA et. al, 2025). Phishing is no longer a singular act, but persistent in its application through its campaign-like designs (Gallo et al., 2023). A report on Digital Threats for the BFSI by SISA suggests that the average time taken to exploit a recently disclosed vulnerability has decreased exponentially, to a duration of mere hours of its public disclosure. It also suggests that with the advent of AI, zero-day threats have become easily accessible and targetable (SISA et. al, 2024). Further, the sophistication of attacks is magnified, increasing by almost 100% every month (Ciso, 2026). Figure 1 enlists the attacks manufacturing sophistication through an increased use of social engineering. AI LLMs like FraudGPT and WormGPT are enabling pretexting[6] through behaviour manipulation and simple analysis (Brissett & Wall, 2025).

[6] Pretexting is a type of social engineering attack where cybercriminals fabricate a scenario, or 'pretext', to manipulate individuals into divulging confidential or sensitive information
Source: McAfee, https://www.mcafee.com/learn/what-is-pretexting-and-how-to-avoid-it/

Figure 1: BFSI Attack Vectors

Source: SISA, CERT-IN, CSIRT-FIN, & Krishnan, S. (2024). Digital Threat Report 2024. In *Digital Threat Report 2024*.

The BFSI sector is considered to be 300 times more vulnerable to cyberattacks (Tyagi, 2021). The magnitude of cyber incidents in the past, such as the 2019 SBI data breach resulting in compromise of millions of users' sensitive information, reflects the high cost attached with these attacks (John & John, 2019). With this, the BFSI can be termed as a high value and high risk system. According to Perrow's normal accident theory, a high risk system is bound to have an accident (Perrow, 1984). Therefore, it becomes imperative to minimise the impact of such incidents. This can be achieved truly when there is a shift from only cyber security measures, to cyber resilience. With an increasing use of behavioural manipulation by the threat actors, the integration of behaviour analysis in solution is a given (Antonopoulos et al., 2022). Additionally, detection must now be coupled with response. In light of this transition, cyber resilience itself requires a systemic tool.

Cybersecurity maturity assessments, along with failover[7] and failback operations[8] has become the need of the hour, which must be realised timely (Gaidosch et al., 2019). Evolving MO of cyber threat vectors shows that they target an entire industry, one bank after another. The MO for similar types of banks remains similar, which becomes the part of the rationale for a common framework to deal with cyber threats (Sarkar & Shukla, 2023). Cyber ranges provide a systematic approach to equip organisations and individuals with cyber resilience. ELETS proposes CRs not just for training purposes, but also for compliance strategies, and an active Vulnerability Assessment and Penetration Testing (VAPT) architecture (Shin et al., 2024). They suggest that in-house CRs should be the way forward with robust attack libraries.

NIST proposed a cyber range framework, which is a part of its broader cybersecurity framework, the CSF 2.0. Its pillars of govern, identify, protect, detect, respond and recover- are a fundamental structure for hosting cyber ranges. They define "[cyber] range [as] interactive and simulated platforms that replicate networks, systems, tools, and applications. They provide a safe and legal environment for acquiring hands-on cyber skills and offer a secure setting for product development and security posture testing" (NIST, 2023). European Cyber Security Organisation, (ECSO, 2020), also released a guide for cyber range designs. According to the ECSO, a CR is

> "[a] cyber range is a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organisation's ICT, OT, mobile and physical systems, applications and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend upon."

The first CR was created by the Department of Advanced Research Projects Agency (DARPA), at the USA. The capability testing of that CR was limited to laboratory-based

---

[7] Failover- the automatic, or the manual, redirection of traffic and workloads to a secondary, standby system when the primary system fails to ensure business continuity.
Source: https://www.starwindsoftware.com/blog/failover-vs-failback/#:~:text=Benefits%20of%20Implementing%20Failover%20and,systems%20and%20automated%20recovery%20processes.

[8] Failback is the subsequent process of returning operations the primary system once it is repaired and stable
Source: https://www.starwindsoftware.com/blog/failover-vs-failback/#:~:text=Benefits%20of%20Implementing%20Failover%20and,systems%20and%20automated%20recovery%20processes.

single testbed infrastructure, which evolved into ‘massive’ infrastructures, findings its place in national systems (DARPA, 2008). Many scholars propose a cyber range design based on the five layers suggested by the NIST. However, those layers rely intensively on technologically heavy components, with little scope for human-driven processes. CR has also been described as a “digital war room” (Widodo, 2025), or a “cyber shooting range” (Finio & Downie, 2026) the aim of which is to strengthen the soldiers before actually walking into live fire ranges and battle fields. This description, combined with the absolute need of CRs in the current world of increasing vulnerabilities, exhibits the requirement of governance and institutional choices that exist at the operationalisation of CRs. Therefore, this paper frames CRs as a proactive security measure and that of leadership.

Mika Karjalainen establishes cyber ranges as a cyber arena, similar to the concept of an action arena given by Ostrom (Karjalainen & Kokkonen, 2020). Karjalainen gives the following as the requirement for a cyber arena: realism, reflecting the complexity and interdependencies of the real domain; should be an isolated and controlled environment; must have internet simulation in the sense that it must simulate global internet with its structures and services; it must mimic the user and network traffic; it should also have the capability to execute and simulate attacks; it must exist exactly like and within the organisation’s infrastructure; in order to remain real and have fluent R&D, there needs to be collaboration and cooperation with other training platforms; lastly, the planning, executing, monitoring and analysing must remain of authentic activities with real-life scenarios. Such an arena is dependent on the technical and operational design of the scenarios. However, there do remain complexities and challenges. Scenarios remain resource intensive and their generation calls for expertise. The scenarios, in many CRs, require a manual setup due to the lack of automation. Orchestration, simulation and analytics also exhibit difficulty because they are dependent on the scenario. The design, therefore, emerges as a major bottleneck.

There have been advancements to provide potential solutions to the problem of resource-scarcity globally, particularly in the context of CRs. Federated CRs have gained attention in countries and unions. The European Network and Infrastructure Security Agency’s ISAC in a Box toolkit builds on shared experiences across multiple sectors to guide the establishment of formal arrangements (ENISA, 2020). The European Defence Agency aims to pool and share the existing CR capabilities between the member states (EDA, 2021). Countries like USA, UK, Malaysia, Estonia, and Singapore have developed their own individual national frameworks and guidelines for the adoption of CRs as national priorities. It has been realised that no operational domain is immune. If it cannot remain protected, then

fighting is their only chance at surviving (Patrick et al., n.d.). India, too, acknowledges this. There has been emphasis on capacity building through exercises like red-blue teaming in various government documents (Kumar et. al, 2018; MeitY, 2022; RBI, 2025; OPSA, 2025). The NCIIPC also held a national cyber exercise comprising of a cyber range (PIB, 2024). However, there remains sectoral and governance fragmentation, with a lack of a consolidated approach towards the creation of one. While many banks under the CII were asked to create, and have created their own cyber safety policy, capacity building for cyber-attacks still remains a gap, and smaller entities within the BFSI sector continue to remain vulnerable in front of an ever-evolving threat landscape (SISA et al., 2024).

Gap

The literature, comprising of over seventy research papers, highlighted that there is a recognition of CRs. However, most were found to be either generic, or focused on education, trade, maritime, power and energy grids, but none on the BFSI. There was particularly a lack of literature on cyber ranges generating from India, although there was much on cyber resilience, cyber security, the banking sector in the evolving digital world, etc. However, there was little emphasis on the goals of cyber resilience established by the Cyber Crisis Management Plan by CERT-In. Further, there was a deficiency of sector-specificity.
With this research, I aim to contribute to filling this gap by exploring the role of cyber ranges as a policy tool for cyber resilience, particularly for the BFSI sector of India.

Chapter 2 Summary

The chapter reviews existing literature on cyber resilience, cyber threat landscape, and the evolution of cybersecurity toward resilience-oriented approaches. It examines BFSI-specific vulnerabilities and institutional challenges, followed by an analysis of CRs, their components and design, and global adoption. It looks at federation and capacity-building roles. It identifies gaps, and establishes the foundation of the study's focus on designing a CR blueprint and framework for the BFSI within the CII.

Chapter 3 – Research Methods (Analytical Framework)

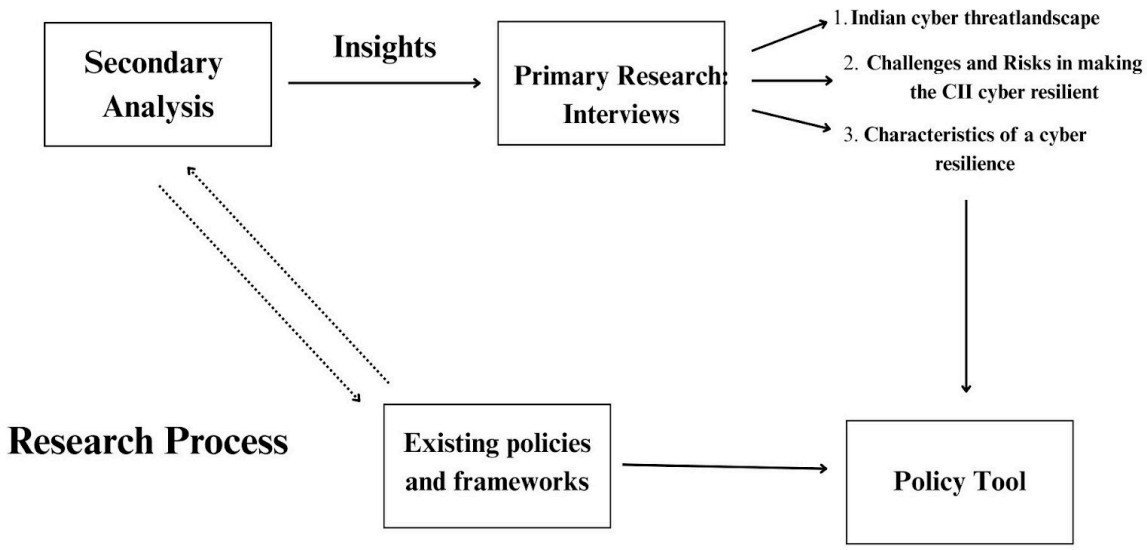

Figure 2: Research Methodology Flowchart

CR, especially for policy, is a complex and an under-explored domain that could not be understood through a single method. It required integration of multiple qualitative approaches to capture both, theoretical frameworks and practical insights. Therefore, I adopted a multi-method approach to strengthen the validity, depth, and policy relevance of my study. The study combines qualitative interviews that provide expert insights and grounded understanding, secondary data analysis based on global frameworks and the literature- resulting into the comparative policy analysis.

There were a total of eight interviews conducted of experts, cybersecurity professionals and BFSI professionals to gather insights on design (component level), governance and practice (capacity level). The average duration of each interview was of twenty-five to twenty-seven minutes, with ten pointed questions. The participants provided expert knowledge, tacit insights and a glance at the gap between simulations and real-world practices. The sampling was a mix of purposive and snowball, with participants being selected on the basis of their experience. Given the exploratory nature of the research and the specialised domain of cyber range development, emphasis was placed on depth of insights rather than the sample size. The sample was considered adequate as thematic saturation was achieved, with recurring patterns emerging across key areas. Importantly, the diversity within the sample also provided valuable insights. While most participants were familiar with CR

concepts, a small number of participants indicated limited awareness. Instead of being a limitation, it also highlighted a broader gap in awareness and adoption of CRs within the ecosystem. It reinforced the underdevelopment of CRs as policy instruments in the Indian context. Thus, the sample provided expert-driven insights and also a varying level of familiarity within the field.

Secondary analysis included governance and institutional frameworks, and global best practices. It provided for the conceptual depth and policy relevance, and a way to ground the research within the Indian contexts. The comparative analysis that followed was to compare and understand governance models in parallel, which was aided by the adoption of a conceptual framework described later. The comparative analysis also helped in identifying transferable elements, and was a caution against blind replication.

To sum up, the study adopted a qualitative multimethod approach, combining expert interviews, secondary analysis, and comparative policy analysis to address the complexity of the CR development for the CII. Given the emerging and interdisciplinary nature of the subject, it was important to capture the technical, institutional and operational dimensions concerning CRs. The interviews added the layer of the data that could have otherwise been missed if it was solely based on secondary analysis. The resulting research analysis comes as a triangulation of sorts.

The objective of conducting these interviews was two-fold: to understand the underlying mechanisms in which these challenges are manifested, and the essential components that overlap or differ in the cyber ranges of different sectors, especially for BFSI. The interviews seek answers for the following: a. How is the Indian cyber threat landscape different from other countries?; b. What challenges and risks does the cyberspace of CII currently face?; c. What indicates maturity levels in cyber ranges; and d. What are the characteristics of cyber resilience?

Upon gathering the primary data, I engaged in thematic analysis of the dataset through Atlas.ti, which helped me arrive at the broad themes. Post that, I indulged in statistic study of thematic occurrences in responses, with the help of various charts. Some interesting insights that were contrary to the secondary data were that there is no pre-established causal linkage between training and capacity building; and that many organisations declare themselves cyber resilient due to the illusion of safety. In the next stage, I used these insights to draw a BFSI-specific CR component blueprint. Analysing the eight layers in the blueprint, and

drawing insights from the secondary data of global frameworks, I recommended a Cyber Range Framework for a Cyber Resilient Critical Information Infrastructure of India.

3.1. Conceptual Framework

Cyber resilience, as a concept, exists without objective ways of measurement or framing. It has its fundamental in four factors, namely, prevention, detection, response and recovery (Linkov & Kott, 2018). In this sense, cyber resilience becomes a goal that organisations aim to achieve. Cyber ranges, on the other hands, become useful strategic tools for the organisations to achieve this goal through. They do so by conducting various activities such as red/blue teaming, attack simulations, CTF, et cetera (ECSO WG5, 2025).

In order to create a framework that helps curate a more socio-technical lens to approach the construct of CRs as a capacity building tool- a common but fundamental arm and aim of policy making, institutional and national priority- situating them within the policy capacity, the paper adopts a two-tiered approach. It explores the Institutional Analysis and Development Framework, or the IADF by Elinor Ostrom (2011), and the Policy Analytical Capacity by Michael Howlett (2015).

In the IADF, Ostrom explains institutions to be fundamentally a shared concept, through implicit knowledge between the participants (Ostrom, 2011). These participants include actors (employed and the employee) at all levels of the institution. Part of the framework deals with the identification of an action arena- a conceptual unit of an identified problem, with an action situation and actors interacting within that situation- the resulting patterns and outcomes from that interaction, and further evaluation of these outcomes. It differentiates between rules-in-use and rules-in-form. The former refers to the “do’s and don’ts”- like unsaid norms and order- of an organisation, while the latter refers to the documented regulations and code of conduct presented in the written form. Ostrom lays heavier emphasis on rules-in-use, as they determine the interaction and engagement of actors with the problem. The framework also recognises that in hierarchal organisations- which most organisations are by design- operation-level decisions generally are in the hands of the rule-makers (albeit a few). Therefore, it pushes for clearer communication within the organisational structures. In order to create pathways for clear communication, it also stresses upon having a common language understood by all levels at the organisation. Further, the framework allows for cross-institutional comparison, by giving some basic generic variables needed to analyse all types of institutional arrangements. That list includes:

a. Action Arena: consisting of participants, positions, outcomes, action-outcome linkages, control and participants exercise, information, and cost-benefit analysis (CBA) for each outcome;
b. Actor: an individual at any capacity- whether professional or personal- bringing resources to a situation, assigning valuation to states of the world and to actions, their ways of acquiring, processing, retaining and using knowledge and information, and the processes they use for selection of particular courses of action;
c. Institutions: for the rules created by them and used by participants to frame their relationship, attributive states of the world that determine the engagement in the arena, and the structure of the community at large within which the arena is placed.

The framework has been widely applied in policy analysis to understand governance systems, institutional design, and collective action problems across sectors. Some of the examples of its application include the designing of institutional responses to disaster, disaster management and risk reduction, along with climate related planning like Water Arena (A et al., 2025). Figure 3 is a flowchart showing the various layers within the IADF.

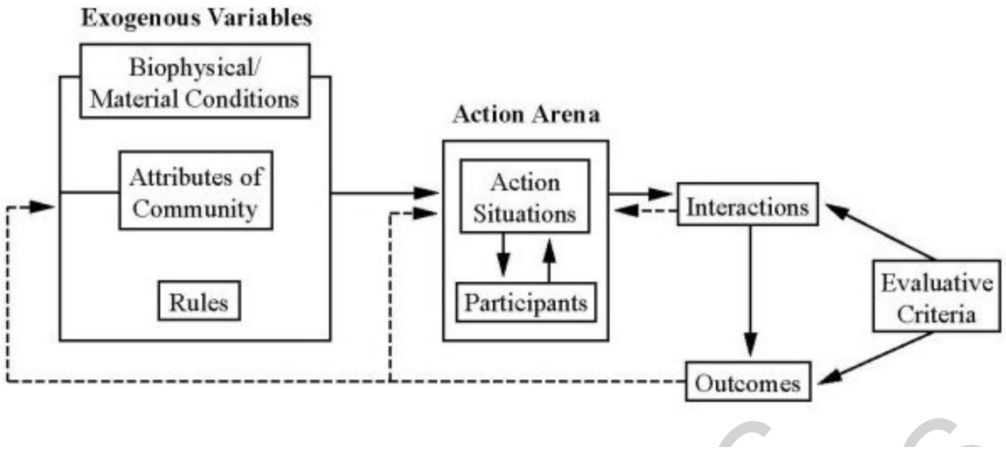

Figure 3: Framework for Institutional Analysis in the IADF

Source: Ostrom, E., Institutional and Analysis Development Framework, 2011

The second framework adopted is the Policy Analytical Capacity framework by Howlett, that builds on his previous theory on policy capacity being resource-oriented, and gives space to the role of policy research. Howlett finds its relevance in all levels, from organisational "to the system level and dealing with managerial and political skills and resources in addition to analytical ones." (p. 174, Howlett, 2015). He describes policy

analytical capacity as "the ability of individuals in [an] organisation to produce valuable policy-relevant research and analysis on topics asked of them or of their own choosing" (Howlett, 2009; 2015). The framework lays emphasis on the fact that this capacity comes as a function of the 'individual skills or competencies' of the research analyst, vis-à-vis the resources at their disposal.

Borrowing from Fellegi, the framework also lays the same capacity at an organisational level, wherein it is articulated through the communication of their "medium and long term priorities, test of its robustness…by building alternative scenarios [and] attach[ing] qualitative and quantitative assessments to different policy options" (Howlett, 2015; Fellegi, 1966). State Services Commission found that ceteris paribus, organisation with stronger policy analytical capacity perform better than the ones lacking it (Howlett, 2015; States Services Commission, 1999). Further, Howlett also recognises that this kind of a capacity tool would only work if there is demand for it. He quotes Riddell, who mentions the creation of a "culture in which openness is encouraged and risk-taking is acceptable" (Howlett, 2015; Riddell, 1998). Howlett emphasises on quality over quantity, and gives adequate space to research expertise of individuals, while also crediting quantitative and qualitative assessments as per situational requirements. He lays the foundational question of allowing for innovation at all levels within the organisational environment or be limited to few. He proposes to meet such doubts with accurate data and supportive environments for highly trained and qualified employees, recognising that not all actors of agencies meet those levels (Howlett, 2015). Figure 4 is the table of components of policy analytical capacity devised by Howlett.

Components
Ability to utilize environmental scanning, trends analysis and forecasting methods
Ability to undertake theoretical research
Ability to utilize statistics, applied research and modelling
Ability to undertake evaluation of the means of meeting targets/goals
Ability to undertake consultation and managing relations
Ability to undertake Program design, implementation monitoring and evaluation
Department's capacity to articulate its medium and long term priorities
Policy analytical resources - Quantity and quality of employees; budgets; access to external sources of expertise

Figure 4: Components of Policy Analytical Capacity

Source: Howlett, M., Policy Analytical Capacity (2015)

It is imperative that the two frameworks are not seen in isolation from each other. In order to fit the lens of CRs and cyber resilience of CII of India, and particularly the BFSI sector, they have been adapted as follows:

The BFSI sector may be conceptualised as an action arena. The actors, i.e., key participants, are the regulatory bodies, the RBI in this case, banking and research institutions, cybersecurity agencies and SOC specialists, CR providers, and other impacted and/or actors that hold influence on the structure. The outcomes that lead to cyber resilience- such as preparedness and recovery- will be determined by the interaction of these actors within the action arena, whether it be compliance, coordination and/or incident response and training. A CR situated within this framework is an institutional mechanism that influences and alters the structure and quality of interactions within the action area. They change the preparation process of actors responding to cyber incidents, which further impacts the behavioural patterns and system-level outcomes. The rules-in-use versus rules-in-form may be conceptualised as the RBI guidelines and mandates for banks to operationalise cyber security and crisis management plans, and the lacunas that get created when those are not followed. As a research participant would put it, “India is not as strict as the West” (P1). Therefore, the rules-in-use also get derived from the window of freedom that the lack of imposition brings.

However, existing literature also highlights how capacity constraints significantly limit the effectiveness of cybersecurity frameworks, particularly in the context of rapid digitisation (Abiona, 2024). Scholarships refer to this as a pacing problem (Leviäkangas et al., 2017). This becomes particularly relevant for India, where digital expansion has not been met with growth in correspondence to institutional and operational capacity (Panagariya, 2022). To move beyond a descriptive mapping of institutional arrangements, and arrive at an evaluative understanding of why gaps persist in operationalisation of cyber resilience, the policy analytical capacity framework comes in hand. The lack of CR creation and adoption for the BFSI sector of India, or a comprehensive approach establishing CR as a policy tool for building cyber resilience for the CII at large, can be seen as the manifestation of limited operational and analytical capacity of the existing institutional ecosystem.

The layering of the framework with IADF and policy analytical capacity provides for positioning the CR as an institutional and a capacity-building tool. It would further aid in accounting for the institutional complexity, capacity constraints, and sector-specificity. Additionally, it also supports the development of policy-relevant recommendations- the

broader CR framework for the CII- by linking the technical design considerations with governance structures and capacity-building needs.

Rules-in-form, in the context of the BFSI sector and for this paper, refer to the guidelines and SOPs established by the regulatory bodies such as the RBI, CERT-In, and the governing hierarchies of the institutions. Rules-in-use, on the other hand, refer to the level to which actors can push the boundaries of the set SOPs and guidelines while tackling a challenge. Rules-in-use, in a sense, then become the height to which bending the rule-in-form is permissible. For example, CR frameworks allowing individuals to use newer solutions and draw new threat vectors as per requirement. Or, the actors making a call to escalate matters to higher-ups/blocking a user from the platform as per the perceived urgency of the situation, which maybe unwarranted in the SOP that calls for a chain of command.

Positionality Statement

This study sits at the intersection of public policy and cybersecurity, addressing a wider question of operationalising cyber resiliency goals through the use of manufactured tools such CRs. It reflects my academic background of public policy, a keen interest in emerging technology governance, and the growing need of capacity building for resilience. While I am not a technical specialist, I tend to keep a policy-oriented lens that helps me examine the interaction between technological systems and institutional, regulatory and operational frameworks. It also helps me relate national objectives with individual initiatives.

This positioning has influenced both, the framing of the research question, and the interpretation of the findings- particularly of governance structures, institutional coordination, and policy designs rather than viewing technology in isolation. The engagement with technical literature and practitioners was to ensure that the analysis is grounded in the operational realities of CR design and cybersecurity practice.

I acknowledge that this perspective may privilege institutional and policy considerations over deeply technical dimensions. To mitigate this, the study employs a multimethod approach, incorporating expert interviews, comparative analysis of international frameworks, and secondary literature. This allows for triangulation of insights and reduces the risk of bias arising from a single disciplinary perspective.

Validity

The validity of this study stems from the use of a qualitative multimethod approach, which integrates primary data from expert interviews with secondary data procured from

global frameworks and existing literature. By combining them, I seek to create a comprehensive understanding of CR designs, and its application within the CII. Triangulation of the findings derived from interviews, which were cross-referenced with insights from global CR frameworks (Singapore, Malaysia and Estonia in this case), along with established cybersecurity standards, served as a key element in ensuring validity. This allowed for identification of recurring themes such as realism, institutional coordination, and performance-based evaluation- thereby reducing the likelihood of bias arising from a single source of data.

The use of expert interviews further aided in enhancing the credibility of the study. The participants were selected on the basis of their experience in cybersecurity, CR development, their involvement in the BFSI sector and LEAs, leading to inclusion of practitioner insights that could not have been, and were not, captured through literature. I could contextualise theoretical frameworks within real-world constrains and operational challenges with the additional lens of practicality.

While the findings concern the FSI. sector, they are not limited to it. They extend to similar sectors with interdependence and digital reliance. However, such an insight transferability would require contextual adaptation, and, as the paper argues repeatedly, sector-specificity.

Limitations

This study is not free of its limitations. The research is based on a relatively small sample- which, while providing depth, may limit the breadth pf perspectives captured. The findings, therefore, are indicative rather than fully representative of the ecosystem. Secondly, the findings could be interpretive and context-dependent. While the thematic analysis allows for rich insights, it may not provide quantitative validation of relationships- such as the direct impact of CR components on measurable improvement in cyber resilience. Thirdly, the scope of this research is limited to the BFSI sector alone, and therefore, its applicability within other sectors of the CII like healthcare and energy is not empirically tested- neither is it scoped for. Fourth, certain policy documents, such as India’s National Cyber Security Framework and Estonia’s CR14 mandate were not accessible, or kept classified. Further, the fiscal scope of the study is only an instrument to enable discussion and consideration, and does not intend to make the economic decision- that must remain with the decision-makers. However, since the financial data of CR implementation is elusive and highly context-

specific (and not subject to public knowledge), the depth of the economic modelling is limited in this study.

Lastly, while the study attempts to integrate legal and regulatory landscapes along with data protection and cybersecurity mandates, the dynamic nature of the cyberspace means that these frameworks require continuous updating and review.

Future Scope of Research

With this paper, I aim to ignite the possibility of CRs being used as a policy tool for cyber resilience, and importantly, for capacity building. I introduce it as a policy capacity tool. An important direction that emerges is the validation, review, and expansion of the proposed framework and CR blueprint. There also is the scope to study the actual dynamic of the relationship between cyber ranges and the improvement in cyber resilience using quantitative metrics or correlation analysis.

Further, future studies may study other sectors of the CI sectors such as energy, healthcare, and telecommunication. Given the interconnected nature of these sector, the potential for a cross-sectoral CR- at local or national level- could be also explored. Federated simulations may provide insights into systemic resilience. These would lead to the policy angle of CR standards, and their integration into regulatory frameworks. This would call for deeper engagement with emerging policies, institutional coordination mechanisms, and international collaboration models- hinting as synergised governance structures.

The role of human-facing emerging technology, such as artificial-intelligence, presents opportunities and risks. Future studies could explore automation of scenario generation, threat simulation, and evaluation, while also examining the governance challenges associated with deploying AI in such a system. Finally, research on workforce development and training could contribute to the broader capacity challenges identified in this study. This includes examining how CRs can be integrated into the academic curricula, certification systems, and national skill development initiatives.

Chapter 3 Summary

This chapter outlines the qualitative multimethod approach adopted in the study, laying the justification and the concept of triangulation. It explains the frameworks and the layered approach. Further, it addresses the positionality, validity, limitation and the future scope of study. In essence, the methodology aims to capture the conceptual and practical dimensions of CR development for a comprehensive and policy-relevant analysis.

Chapter 4 – Secondary Data Analysis

On the basis of the papers reviewed, certain baselines were made clear:

i. Digitisation of services and products is unavoidable;
ii. The shift to digitisation of critical sectors is creating new cyber threat vectors, making it a pacing problem;
iii. Globally, institutions are opting for ways to increase cyber resilience in the face of cyber threats;
iv. The BFSI sector of India has been digitised rapidly, but the gaps in practice remain with fragmented understanding of roles;
v. While the regulatory landscape of India is vast and encompassing of numerous bodies with delegated responsibilities, there is an overlap and lack of synergy in the policy landscape, creating lacunas in implementation and LEA-agency coordination;
vi. In light of these gaps, and smaller institutions like cooperative banks and small finance banks being particularly vulnerable, it becomes imperative for India to devise a policy tool that is technically sound to enhance its cyber resilience;
vii. Such a tool would be the creation of a CR, the basic blueprint of which should be publicly advisable, along with a CR framework, setting certain basic minimum requirements and components befitting the Indian context.

Upon reviewing globally followed practices, the following criteria to evaluate countries for comparative analysis was drawn up, ideal comparators satisfying at least three of them:

i. Comparable digitalisation trajectory with India, which, in its essence, would mean rapid, uneven or recently accelerated;
ii. A strong BFSI-sector, or sector-specificity in the approach to CRs;
iii. A federated or multi-agency governance model, which is, also, similar to the Indian regulatory landscape;
iv. An emerging economy or a middle-income country, which further provides fiscal realism for the implementation and budgeting stage;
v. A documented policy, regulated mandate or a national initiative towards the adoption of CRs.

The countries thus chosen for a comparative analysis were Singapore, Malaysia and Estonia. While the first two were one of the only Asian countries to have a mandated CR

approach, with Malaysia having one of the most detailed framework for the same, Estonia became one of the first countries in the world to have a consolidated national CR (that also caters to the rest of EU member states) for developing defence capacity. Similarly, Malaysia's cyber range framework's basics overlap with the European Cyber Security Organisation's guide on CRs[9].

Singapore:

While Singapore does not have an entire framework dedicated only to cyber ranges, its Technology Risk Management guidelines for the protection of the financial institutions (FIs) from cyber incidents include a comprehensive section on cyber ranges (Monetary Authority of Singapore, 2021). The country mandates FIs to have VAPT that highlights their systemic vulnerabilities and the actual position of their security. They give organisations to determine the frequency of these checks, while defining guardrails. Sectors digitising rapidly, such as FIs, must go through them annually, or as per the changes and advancements in the procedures. Singapore also recognises the role of bug bounty programmes[10] and white hackers[11] for organisations to hold such evaluations.

It also recognises sector-specificity of FIs, and therefore mandates them to include necessary stakeholders, including "senior management team, service providers and technical staff responsible for cyber threat detection, response and recovery". It lays emphasis on the simulation of attacks, and them taking place within the scope and rules of engagement- which must be communicated before such activities begin. They recognise that threat scenarios must be challenging and plausible, but also the environment for conducting the same must be safe. They lay emphasis on the global best practice of forensics to identify the tactics, technique and procedures (TTP) used in attacks.

The evaluation metric Singapore suggests is to include:

a. The severity of the assessment and classification of an issue;
b. The timeframe to remediate the issues of varying severity; and
c. Risk assessment and mitigation strategies managing deviations from the framework.

[9] The verbatim in these two documents was found to be the same, aligning their approach and knowledge
[10] Bug bounty programmers are the third-party organisations that can assess an entity's security positionality: https://www.hackerone.com/bug-bounty-programs
[11] White hackers are ethical hackers, who are essentially the cyber security professionals using their skills to identify the vulnerability and weakness in systems: https://www.hackerone.com/knowledge-center/white-hat-hacker

However, the framework does not mention the ways of creating the breach and attack simulation library, neither does it define the roles of various actors. The framework is brief and vague, however, it does signal the seriousness of cyber ranges being viewed as national priority for developing in-house capacity and capability.

Malaysia

The Cyber Range Framework, published jointly by Ministry of Communication and Multimedia Malaysia and CyberSecurity Malaysia[12] aims to establish an effective way to integrate people, process and technology within the CR framework (CyberSecurity Malaysia, 2022). It differs from the NIST framework in its understanding of the CR, viewing as a means to collect and store data while ensuring confidentiality and integrity logically and physically, while offering researchers a safe environment to work in. They find CRs to be of use for various stakeholders of the society as a whole, mentioning CR use case for competence building, competence assessment, security education, recruitment, development of cyber capabilities, development of cyber resilience, national and international cyber competitions, security testing, security research and digital dexterity. Their aim is to keep the CR as honest and close to reality as possible. The framework acknowledges that certain elements can increase the complexity of the CR, like the simulation of internet services on which the simulation environment may itself depend- however, such a layer, for Malaysia, is important to be included for the sake of realism.

They also give Global ACE framework[13] pedestal, proposing that the individuals who go through CR trainings could avail the Global ACE credits- making it an incentive tool for cybersecurity professionals and aspirants to integrate CR institutionally. They also establish the cycle of learning, practicing, applying and assessing during the CR simulations. The framework also lays that CRs complying with the Global ACE framework (which, in turn, would be the necessary conditions for CRs in Malaysia to fulfil) would include the following elements:

i. Building foundational elements of cybersecurity with theoretical labs
ii. Transforming knowledge into skills with practical labs
iii. Applying knowledge and skills in real-world attack scenarios
iv. Providing actionable feedback to optimise skill development.

[12] Malaysian government has a collaboration with CyberSecurity Malaysia to create a national-level CR
[13] Global ACE Certification is for cyber security professionals to gain accreditation, mutually recognized by global partners https://www.globalace.org/home

In doing so, they lay emphasis on theoretical understanding being an important step to develop practical skills that are sound and methodologically correct. The framework has a provision for smaller CR environments for individuals to practice in and improve their skills. Further, they map multiple technical skills together along with other teammates while mitigating scenarios. This is to ensure that there is a clear teamwork approach, and a mechanical way to increase the 'emotional IQ' required while handling real world cyber incidents with colleagues who may be distressed. They also aim to inbuild feedback mechanism to explain teams their progress right after they finish a task- to tap into the freshness and immediacy of actions.

Further, two more aspects that make the Malaysian framework the most distinct are its recognition of the global shortage of cybersecurity professionals and its proposal for having a cross-border security forces; and its sheer distinction from the NIST framework. It acknowledges that CRs can be resource intensive, and the creation being technically heavy. Therefore, it also suggests CRs as SaaS on a public cloud, an interesting take. It further advocates against blindly adopting the NIST framework and its work roles[14], given the fact that they may not translate aptly into the roles that are contextually different, both, in physical and logical dimensions. However, it also mentions that having globally accepted measures will work in favour of developing a specific workforce with established qualities. It also mentions that certain roles may overlap, while responsibilities could be completely different.

The basic evaluation metrics for the performance in CRs for Malaysia are:

a. Mean-Time-To-Detect (MTTD)
b. Mean-Time-To-Respond (MTTR)

The framework also gives the prerequisites of a CR within different simulations, and has specific guidelines for architectural components, scenarios and content development, MITRE ATT&CK framework, cloud CR functional and technical requirements, and those required for on-premise CRs. Overall, the framework is wholesome and gives enough space for sector-specific customisation, along with layer-level understanding of CRs.

Estonia

CR14, created by the Ministry of Defence of Estonia, is a national CR providing defence training through national and international cyber exercises (*CR14*, n.d.). The CR is also used by the NATO for research and development, serving as the basic infrastructure for NATO to

[14] NIST proposes a list of around fifty-two roles for cybersecurity https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/resources/occupations-jobs-and-work

base its defence upon. The CR is based on over ten years of operating experience, and is "arguably…one of the first establishments of its kind globally." They have various kinds of CRs to serve different purposes, including classified and unclassified CRs. CR14 connects governance and defence bodies, such as the military, the ministries and the private sector ranges, making it a federated governance model.

The need for such a robust platform was felt after the massive 2007 DDOS attack in Estonia that targeted the banking, government and media websites. The attack originated from Russia, and left Estonia digitally crippled for weeks. As a proactive step designing a policy tool to mitigate the possibility of such an event occurring again- that too, in an increasingly VUCA world[15]- Estonia established CR14, shaping its cybersecurity strategies. Its globally known Locked Shields model, a CR exercise that NATO engages with annually, evidences the possibility of a cross-institutional, realistic simulation at scale.

While Estonia does not have a public document for the CR framework, its cybersecurity strategy lays out how cyber resilience is not an isolated act, but requires cooperation and coordination with other "like-minded" countries. It also positions CRs right at the forefront of its training and capacity building strategies, emphasising on the need for having technical know-how. Along with a national mandate, CR14 has a harmonious relationship with other defence bodies, like Defence League[16]. However, CR14's operational framework is either classified or non-public, which raises questions on its transparency.

Takeaways-

Singapore, Malaysia and Estonia, all three recognise the need for cyber ranges as a national priority. There is also a distinction between rules-in-use and rules-in-form, wherein the face of a novel attack vector, defenders may need to go beyond the rules-in-form, and operate within the structures of rules-in-use, which is an extension of the stricter rules-in-form. They also recognise that CRs need to incorporate various, and sector-appropriate, actors. Further, the integration of CRs with ministries of communication, defence and finance only shows that CRs can also be institutionally designed for integration beyond the basic requirements, becoming another source for conducting R&D.

---

[15] VUCA stands for volatile, uncertain, complex and ambiguous- a term currently being used to describe the current geopolitical tensions across Europe, Russia, USA, Israel and West Asia.

[16] Kaitseliit is the Estonian Civilian Organisation working for state defence and population security https://ewspa.edu.pl/en/e-czasopismo/nr-1/kaitseliit-estonian-civilian-organization-working-for-state-defence-and-population-security/

These frameworks also ring a tale of caution as they suggest against blind adoption of foreign frameworks and initiatives, laying emphasis on contextual relevance. For the BFSI of India, these insights matter as they highlight the need for:

- Context-specific simulation environments, particularly replicating the core banking systems;
- Integration of people, process and technology rather than making CRs a purely technical training;
- Flexible frameworks avoiding over-standardisation, allowing for adoption at varying levels of institutional maturity;
- Mechanisms for shared infrastructure, enabling smaller institutions to access cyber range capabilities.

Taken together, the comparative analysis suggests that effective cyber range strategies operate at the intersection of institutional design, capacity-building, and technical architecture. While each country emphasises different elements, all recognise that cyber resilience cannot be achieved through static controls alone, but requires dynamic, simulation-based validation.

For India, and particularly the BFSI sector, this implies that the development of a cyber range framework must go beyond technical specifications to address questions of governance, capacity, and contextual relevance. Cyber ranges must be positioned not only as tools for training, but as mechanisms for aligning institutional behaviour, enhancing operational capacity, and supporting systemic resilience.

Chapter 4 Summary

The chapter analyses CR frameworks, focusing on Singapore, Malaysia and Estonia. It derives key insights and contextualises them for the BFSI sector of India, going from broader to concentrated area.

Chapter 5 - Primary Data Analysis

As part of qualitative research, eight participants were interviewed. The data analysis from the interview was driven and aided by the IADF and the Policy Capacity framework. The following table enlists the details:

Table 2: Participant Details

Participant	Affiliation	Remarks

P1	Academia	Aware of CRs
P2	Practitioner	Aware of CRs
P3	Banking professional	Unaware of CRs
P4	Academia	Aware of CRs
P5	LEA	Unaware of CRs
P6	Practitioner	Aware of CRs
P7	LEA/expert	Aware of CRs
P8	Expert/Academia	Aware of CRs

After interviewing the professionals from the domains of cyber and banking, it was clear that while not everyone was familiar with the concept of cyber ranges (two out of eight), all participants deemed it necessary and integral. Each participant was asked eight-ten questions. A total of 153 codes[17] with ten code groups emerged out of the responses. The ten code groups were further clustered into four major themes of technical dominance, institutional embedding, capacity logic and gaps[18]. They are elaborated upon in the section on Discussion.

Table 3: Sample Coding, Categorisation and Theme Distribution

Codes	Categories	Themes
Digital first*	Capacity Building	Capacity logic
people process and technology*		
Team-based exercises*		
Learning and development*	Gaps	Gaps
Incompatible decision making*		
Freedom (lack of)		
Indigenous attack scenarios	components	Technical dominance
Security top down*		
Proper signatures*		
Track all attacks*	elements	
Budget		

[17] *See Annexure for the codebook*
[18] *See table 2 for the categorisation*

identify		

5.1 Findings

Three points emerge from data analysis:

First, the interviews were dominated by components, followed by elements and governance, while actors, gaps, the types of cyber ranges and the West were the least talked about. Thus, the professionals were focused on what should exist, rather than what is missing, inclining towards a solution-oriented approach. The West was only spoken of when the question itself prompted the participants to think or compare. The focus on governance- decision making, makers of rules-in-use, control and command models, evaluation and maturity benchmarking, prescribing frameworks and audit mechanisms- may mean that it is seen as an embedded layer, and not external. It is not seen as secondary, making cyber range an issue requiring institutional and governance lenses. While actors and gaps have the least share, capacity building emerges as a significant category. This implies that actors (which consist of employees, decision-makers, attackers, and overall engagers within the action-arena of cyber range) are fundamental to a cyber range- with capacity building being central. Capacity building as a concept would not take dominance if there were no gaps. Another observation is that while gaps are less spoken of, they are rather wide in nature. Types and the West were the least talked of, which hints at the fact that experts and practitioners are not concerned with classification and theoretical typologies, neither do they believe that a western structure could fit Indian contexts. Their primary focus was on implementation, components that are driven by ground knowledge of the Indian cyber landscape, and the overall elemental essence of a cyber range.

The empirical distribution suggests a shift from conceptual classifications to operational and institutional design- with strong emphasis on tailoring approaches based on sector requirements. It further indicates that CRs are understood primarily as an applied infrastructure, rather than a theoretical construct. However, it is also seen to exist within the institutional rules and bylaws. Therefore, a techno-legal approach would determine the outcome-orientation and successful execution of CRs. Figure 5 represents a pie chart showing the share of the code groups in the interviews.

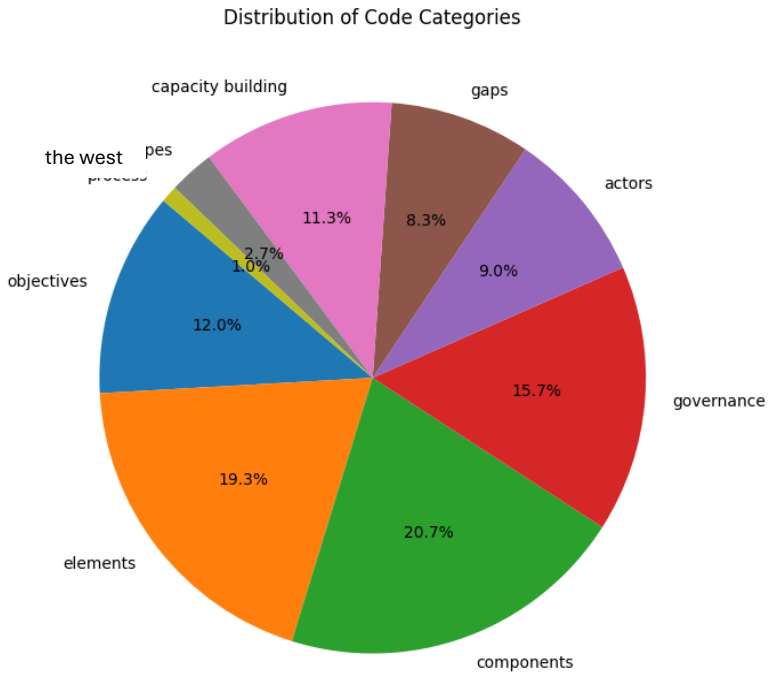

Figure 5: Distribution of Code Categories

Second, it was also seen that certain categories had instances of overlaps. Governance and elements overlapped eighteen times, capacity and elements overlapped ten times, and all three overlapped seven times. This implies the following:

i. Elements of a CR are not standalone with technological inputs. Its principles, essence, institutional design are all governance-driven. Thus, far from being neutral, the features and characteristics of a CR are shaped by the institutional rules, and the broader policy choices and compliances of the institute.

ii. Capacity building is not a separate function, but is in fact built into the system by design itself. It is embedded into the platform.

iii. Governance, capacity and the elements of a CR are interdependent, showcasing the characteristics of a triangular relationship.

On the other hand, it was seen that while components and actors overlapped twelve times, components and objectives only co-occurred four times, and all three, i.e., components, actors and objectives overlapped only a single time. This means that the current approaches toward CRs and capacity building remain fragmented. This is a counterfactual to

the guiding secondary data that suggests CRs to be driven by objectives. This implies the following:

i. The visible relationship between components and actors represents that components of a CR are actor-linked. The design depends on who is using them, where, and for which purpose. It was also acknowledged in the first point that actors are fundamental to a CR.

ii. The link between components and objectives is weak. This means that while there is a momentum to fulfil the objectives with the help of the design blueprints of current CRs, there is a significant gap arising. The systems are being designed devoid of their ties to objectives. This gap may not necessarily be in the CR design itself, but how it is adapted into institutions. This point will be discussed further in the section on gaps.

Thus, CR design is emerging as a socio-technical range with functions of governance priorities, capacity constraints and components reflecting institutional choices. However, there is a relative isolation of components, which indicates a lack of systemic integration of current CR thinking. While design is dominating the discourse, it seems not in line with outcomes. Interestingly, capacity sits tightly linked with outcomes, which highlights an underlying gap between component design, outcomes and the resulting fragmented capacity building. Conclusively, the insufficient integration of technical components with governance structures and understanding,- which would directly impact its institutional adaptability-capacity requirements and resilience outcomes altogether are fragmenting the existing approach to CRs. Figure 6 shows the overlaps of the categories in the form of a Venn Diagram.

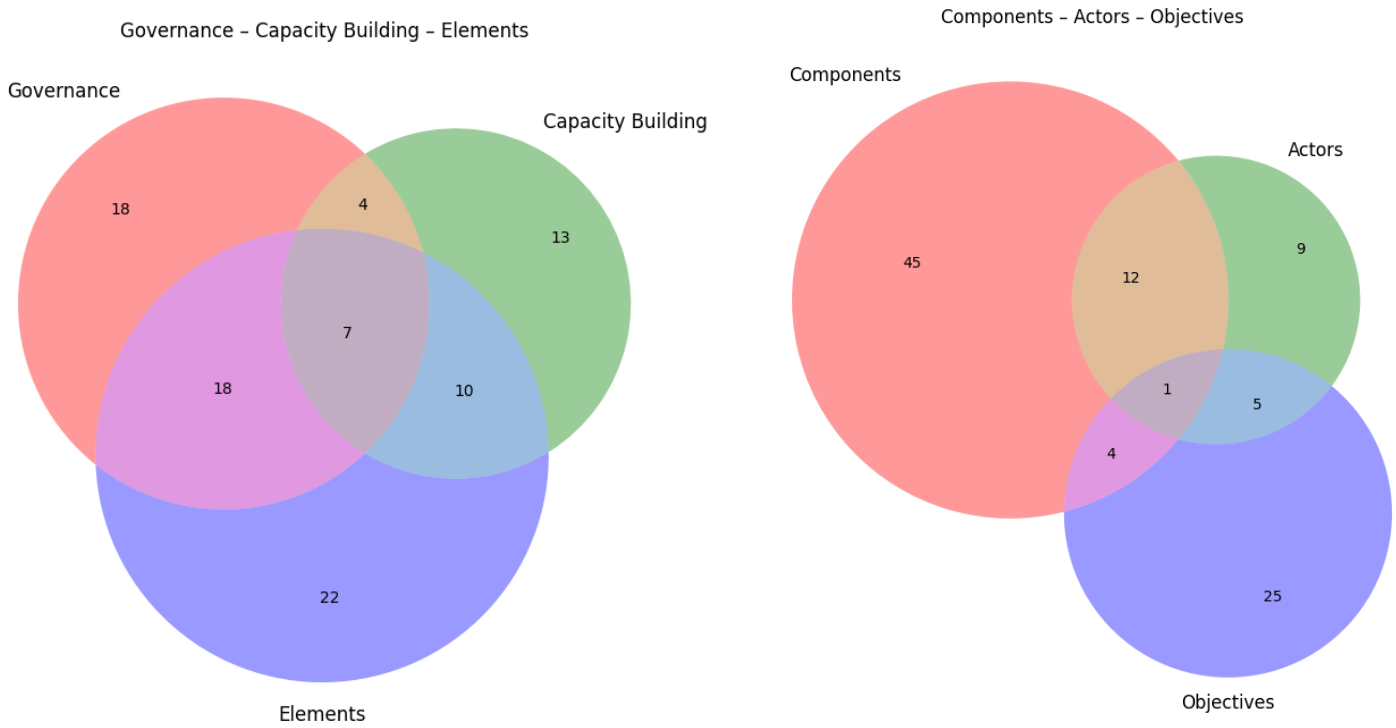

Figure 6: Category Co-Occurrences

5.2 Discussion: Categories and Themes

The following is a brief description of the categories, and code types included within each, in alphabetic order and no order of preference or value.

Actors: This category includes all the users of the CR, anyone with a role to play in the cyber range. Actors, while itself a category, is also a sub-category of Components, since it determines the range design, the procedures, the rules, etc. Participant 5 (P5) emphasised on the roles of various actors, defining and understanding which has a strong role to play within CRs, “role of the instructors,… cyber security experts,…forensic investigators,…attackers” (P5). Participant 2 (P2) reinstated that actors have the most common role, and that the existence and establishment of a CR is solely for them.

Participants 1 (P1), 4 (P4), along with P2 said that it was because of the various actors present in the real environment of the banking platforms that they needed to use social engineering to study the behavioural patterns to make the scenarios more realistic. Participant 6 (P6) spoke of the complexity that arises in scenario planning for a banking platform, because there is a “sense of vulnerability” in the users of a financial system.

Capacity Building: Both, points of capacity building-oriented approach, and points that exhibit the need for capacity building as solution are included within this category. For example, P1's description of cyber resilience being closely determined by "people, process and technology" highlights the needs of building institutional capacity to make processes more people-facing. P1and P8 speaking of the current workforce not being digitally savvy, whereas the upcoming generations being "digital first" highlight the need of capacity building in the older generations. Alongside, P7 spoke of building capacity to fight "malicious and vulnerable systems". This category is based on the underlying essence of capacity building, rather than an explicit mention of the same. However, there have few instances of it being explicitly mentioned by the participants, as in the case of P2 and P4. P2 uses the term 3C to denote "capacity, capability and compliance" as foundational to CRs.

Capacity building is also almost as fundamental as actors to a CR. The entire point of a CR being to create enough capacity and capability for businesses, in this case banks, to continue their operations amid facing cyber-attacks on their systems.

Components: All codes that would frame as blueprint, and/or guide the laying of the blueprint for the CR have been coded as components.

Elements: All codes that would help in the creation of the framework of the CR- the guiding points that translate into the features, qualities, principles, objectives and even operationality of the CR were included in this category. This was to ensure that components remain standalone their functions as purely a part within the CR, whereas elements are what would give shape to the CR. Because elements must be translated into implementation, many found integration into components. For example, "process-oriented exercises" (P1, P4, P8) were categorised as components and elements because while it must be a core function of a CR, it is also an important element of its guiding principles.

Gaps: Alongside the broad institutional and skills gaps like digital, communication, integration and learning, the category includes more implicit codes. When P2 shared that many "organisations do [not] think of guardrails to prevent cyber accident within cyber range", it implied a clear gap between institutional requirements and security guardrails that was not, or has not been yet, given enough deliberation. Gaps also emerge as an important theme that is discussed towards the end of this section.

Governance: This category includes all codes that reflect prevalence, the lack of, or the need of decision-making, control designs, command distribution, impact assessments,

evaluations, authority, monitoring and overseeing, or any role of leadership- even if technical. I acknowledge the technical components of CR systems, and therefore this category is in cognisance with an integrated, harmonised approach where a purely techno-legal, or a socio-legal governance lens has been adopted to review the process and set structures of CRs, and what could improve. Therefore, while governance is not made explicit in responses, institutional choices and control models of top-down vs bottom-up, along with the role of the sector authority (the RBI in this case) have all been included in this category.

This approach was adopted to ensure that the linear understanding toward governance and its functions of regulating and deregulating are broken out of. It gives space for the nuances of the category. For example, the in-vivo of the current CRs "sticking to traditions" (P2) is categorised as both gaps and governance, because this gap in the training arises from the institutional aversion to novelty. Similarly, the code "budget" has been categorised as an element and as governance, because a separate budget has to be part of the investment in the CR, however fund allocation still remains a fundamental governance choice. Thus, governance arises as an embedded layer to CRs and their implementation, which could potentially play a determining role in its success rate.

Objectives: The deliverables expected out of a CR, impact aimed to be generated by the CR, problems that should be solved, gaps that need to be filled- all codes hinting at these have been categorised under objectives. Therefore, this category also overlaps with others. For example, P1 and P4 recognised the role of policy for safety guardrails so CRs, in their attempts to reduce the systemic vulnerabilities, "do[not] end up amplifying [them]" (P1). Recognising the elemental security-first nature of a CR implicit in this statement, which also serves as one of the primary objectives of a CR- and could potentially turn into a systemic gap if not achieved or missed,- the code was categorised under elements, objectives, and gaps. Similarly, since there have been numerous cases of functional creep in case technological advancements and innovations in the past, to make "no creep" (P1; P4) an objective along with an element of the CR is a conscious policy angle. The approach to not view objectives solely from the "to-do" lens, but also from what to not cause has been adopted in order to ensure curtailing systemic neglect of potential mishaps. It increases accountability, traceability, and truly strengthens the system without adversely impacting units and parts of it.

The West: This category was created to clearly analyse the differences that the practitioners find between the Indian and Western structures, particularly on CR. The aim behind this was to establish exactly how the Indian cyberthreat landscape differs, and why Western frameworks cannot be adopted as replicas in India. P5 explicitly mentions the broader cyberthreat landscape of India being rather opportunistic due to the gullibility of the public in general. They give an example of an APK-based fraud luring people with "gas cylinder booking" in light of the 2026 West Asia was, and the succeeding tensions over gas unavailability.

Types: This category contains the different types of cyber ranges, which exist as an institutional choice and also becomes a vital part of the element and component level of a cyber range.

5.3 Themes

The nine categories were mapped on to four main themes, with seven umbrella takeaways.

Technical Dominance

The current discourse on CRs and even cyber resilience has a heavy focus on infrastructure and attack simulation layers, and are investing in the same (P2). Many organisations, as stated by P2 and P6, are basing their cyber ranges on the NIST framework entirely, running the risk of missing their local context altogether. The five-layer model of the framework, about which three out of eight participants talk, is a purely of technical components. Further, along with the training being more tools-centric and traditional (P2; P5), than context-specific, there is also over-reliance on the purchase of tools than building the capability to use them (P2).

The empirical data reveals that CR thinking is engineering-first. This implies that instead of more focus on continuing to update and rooting the CR into the real-world systems and scenarios by integrating workflows, defining roles, behavioural responses and the nuances of the sector, the focus gets pushed to more external aspects such as compliance for the sake of compliances. Not only does this create a gap between the expected performance and the actual performance levels, it also creates a false sense of security (P2).

Participants highlighted that after multiple instances of systemic failures, and with a stake as huge as India's, it is important to remember that there is a fundamental and societal difference between India and the West. The digital maturity in India remains extremely

uneven and fragmented, and the systems hybrid with no clear demarcation between the distribution. P5 revealed that while many banks have their operation on the intranet, the fraud detection chain, though powered by artificial intelligence and a human-in-loop, generally falls upon a non-technical employee with little practice, and many other deliverables (P5). P4 also shared that the cyberthreat actors are now organised cybercrime networks with designated teams delegated with different tasks to bypass systems.

Conclusively, P8 said that the BFSI sector needs a replication of the core banking system,- which now includes Immediate Payment Service (IMPS), National Electronic Funds Transfer (NEFT), and the communication channels with the Unified Payment Interface (UPI), among others,- transaction continuity, and fraud detection adapting to newer and arising vectors.

Institutional and Governance Embedding

CRs can essentially be understood as sandboxes (P; P3), and by virtue of being a sandbox, they must sit isolated and with clear audit mechanisms. At the same time, they run the risk of malware leakage (P1, P2, P3), i.e., the spillage of malware to the outside of the CR, exposing to other systems, resulting in unauthorised access or data theft (Fortinet, n.d.). Apart from external threats, there also exist internal threats like misuse by the insiders or vulnerability replication in the actual environment. Therefore, it falls upon governance to "catalogue vulnerabilities" (P1, P2, P3). An important risk highlighted was function creep, one that India has had a history of dealing with. Function creep occurs when a system, or a technology, starts getting used for purposes above and beyond it was created for. Instances that gathered national prominence were that of Aadhaar card being used for SIM card activation and PAN card registration, when to begin with, it was a voluntary system for welfare subsidies- to curb systemic leakages. Another one is the use of facial technology for surveillance and making police arrests, when the primary purpose the judiciaries allowed it to serve was for tracing missing persons and human trafficking. Thus, it also falls incumbent upon the governance structures to ensure that there is "no [function] creep" occurring (P1). Further, in order to truly make the CR serving the Indian contexts and banking landscape, it is imperative for the components to reflect the real-time platform environment- equipped with emerging threats and evolving modus operandi (MO) (P2, P5, P8). Thus, alongside R&D, maintaining control datasets that store use cases across the various organisations of the same sector is also the responsibility of the governance.

P1, P2 and P4 shared that while the regulators, in this case the RBI, need to standardise approaches, they also run the risk of over-standardisation. This may give the threat actors to explore newer areas and MOs accordingly. They believe that the role of the RBI should be to enable, and not prescription. P2 shared the structure of their organisation, wherein the freedom to conduct R&D on new threat vectors and tools, and the subsequent choice of working on mitigating the threat lies with the team, while the overall bigger decisions like budget allocations and guardrail audits remain with higher-ups. P5 and P6 echoed similar thoughts as they suggested for developing anti-forensics for forensics and integrating them into the training. This seconds the paper's proposition to make the elements of the CR top-down, but the CR design itself a bottom-up process. P2 and P7 state that many failures in achieving the desired outcome through CRs occur due to incompatible decision-making.

Therefore, borrowing the action arena consisting of actors and institutional rules (Ostrom, 2011), as a socio-technical system, a CR must simulate infrastructure, behaviour and organisational response. It must include employees, customers, vendors and establish meaningful SOPs, the intent of which must be emulated into the workflows. Institutional governance must also study the roles of decision-making, human behaviour and interest levels- all of which make the performance vary. Doing so, a CR establishes itself as a technical, human and institutional system.

Capacity Logic

Cyber ranges were compared to mock drills (P1, P2). This substantiates the likeness of cyber ranges to a digital shooting range for cyber soldiers gathered from secondary data. All participants agree that such a platform would result in preparation for attacks- known and unknown. However, a key gap that remains is that people have a tendency of not recalling SOPs in real situations. P2 and P5 shared their experiences of seeing people get 'completely blank' (P2) in face of a real attack. This occurs not just because the threat is more real and therefore evoking fear, but also that they did not really learn how to practically use it. This, in turn, means that the SOP's intent went amiss- which in fact plays a role in building capacity. P5 explains how it is important to understand what things mean, than just blindly following orders. Research also shows that when people understand the meaning of something, particularly of something taught, they instinctively perform better at it. This also overlaps with P1 describing the essence of a CR as 'people, process and technology' (P1).

P2 shares that many organisations invest in the development of CRs, but do not acquire the knowledge to actually use it (P2). This would directly impact the training, the outcomes and the overall use of the CR. Capacity building is not solely dependent on training, it reflects in preparedness of the workforce under pressure. As found during secondary research and substantiated by six participants, India lacks adequate number of cyber security experts. Therefore, it becomes important to train the non-technical workforce engaged in the banking sector to deal with the cyberthreats. However, this capacity will only build if the employees are themselves confident and trusting of the SOPs, there is clearer communication between the organisation, and appropriate delegation of work. While P2 suggests that organisations should take training by CR experts on how to use the CR optimally, P4 and P7 say that the current work delegation in banks in uneven, and the addition of the technical layer to their work has compromised quality of work. According to them, apart from the main SOC team, each branch requires a technical team to handle the daily threat detection within the cyber threat landscape. Their response hints at the hesitation with digitisation that P1 and P8 identified in the workforce bracket that grew up not being digital-first.

Gaps

Despite the country's surmountable growth, India continues to struggle with fundamental gaps. These include learning and development, the fundamental digital gap, digital exposure and comfort with technology at large- also feeding into the trust deficit. Standard gaps within the CR design remain the lack of mark of maturity- and the understanding of it; capability gap of using the CR; integration gap with the system.

The data shows that maturity cannot be measured by the number of simulations run and the tools used, simply because training does not equate to capacity. As P1, P2, P3 and P8 state, the mark of maturity should come by the reduced number of incidents and better response outcomes to cyberthreats, if faced any. However, some participants are also of the belief that organisations have an illusion of resilience (P2, P5, P7). They "think they are resilient, but [they are] actually not [as] protected" (P2). This implies that the training outcomes are not linked to real-world outcomes, and therefore not resulting into systemic resilience. This further establishes that there is no such causal link between training and resilience.

The paper has attempted to establish that governance is built and embedded with the architecture of CRs, and is also crucial for necessitating the safety guardrails. The bridging of the gaps also is the inherent responsibility of the governance structures. However, they cannot be rigid or prescriptive, or else they run the systemic risks of failure. Another important institutional concern arises is that of ecosystem fragmentation. P5 and P7 speak of the lack of coordination between banks and LEAs. The synergy gap results into a mismatch between policy formulation, intent and implementation. The institutional gap widens when departmental hierarchies cause a slowdown in response. This gap is also a result of regulatory dependencies of the institutions themselves. Since there is no unified cybersecurity framework in India in public knowledge yet[19], responsibilities remain undisclosed. All eight participants are of the belief that India, and particularly the BFSI sector, is not truly cyber-resilient. This institutional setback is not a single-actor problem, but a coordination failure at large.

5.4 Consolidated Findings- Secondary and Primary

When the secondary and primary data are read together, ten major insights emerge:

i. Cyber resilience is operational and systemic, not merely technical: NIST framework emphasises on detect, respond and recover. Singapore and Malaysia lay down performance metrics. The participants during the interviews emphasised upon the inability of the organisations to respond in real time, and the gap between the possession of tools and the actual, appropriate execution of the same.

ii. Persistent gap between perceived and actual preparedness: cybersecurity, in many organisations, is generally compliance-driven. Many organisations also approach cybersecurity, overly relying on preventive controls. At the same time, organisations, due to the compliance-orientation, assume their own safety, while they fail to validate the performance through simulation.

iii. CRs are underdeveloped as a policy instrument in India: Globally, several frameworks exist, such as the ECSO, NICE, TRM and Malaysia's CR Framework. While many guidelines in India mention the need for conducting red and blue teaming exercises, it lacks a consolidated, structured CR policy that could serve as

[19] A National Cybersecurity Reference Framework (NCRF) was drafted and circulated to select few institutions in 2023, but has not been brought to public access yet, and so remains largely unimplemented. Read more: https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2078093&reg=3&lang=2

a base for any and all entities willing to develop cyber capabilities. The primary data also reveals that adoption remains fragmented, lacking standardisation.

iv. Realism, Cyber Resilience, Components, Simulation- While there is technical heaviness in the dialogue of CRs, scenario-realism, components that determine cyber resilience are also necessitated to be positioned close to the impact they have in the real-world. However, interviews reveal that there is a gap in R&D, that fails to translate the components into real-world capabilities.

v. Training does not equal to capacity: This insight emerging from the primary data that runs parallel to the secondary data, points to a fundamental institutional problem. Drawing from Howlett's framework, capacity is not simply a function of exposure to knowledge or tools, but is also a function of demand for that knowledge within the institutional environment. If organisations approach cyber resilience as a mere compliance and not as an operational necessity, the demand for genuine learning outcomes could be absent. The illusion of resilience is an institutional incentive failure. The rules-in-form mandate training, the rules-in-use reward compliance.

vi. Cyber resilience in India's cores: cyber resiliency, particularly in cyber crisis management and response plan, is of central focus. CERT-In lays down four core principles of anticipate, withstand, respond, and evolve. Each stage is dependent on step-wise procedures. The first step comes as understanding a problem, preparing against it and successfully preventing it from occurring. The next step, of withstanding, requires a business to continue its operations even if it is attacked, while also constraining the impact the attack would potentially cause. The recovery stage requires the entity to understand and evaluate its position, continue its operations, while simultaneously constituting its shaken foundations. The last stage of what can be understood as a cycle, is evolving, in which the local platform environment is transformed and re-architected. Figure 7 represents the diagram from the CERT-In's CCMP guideline.

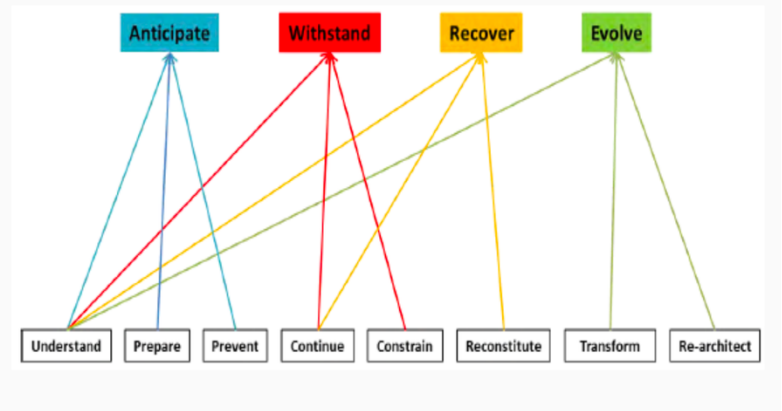

Figure 7: Cyber Resiliency Goals of CERT-In

Source: CERT-In (2017), Cyber Crisis Management Plan

A CR design framework for cybersecurity education and training introduced a topic map including the characteristics of a CR (Katsantonis et al., 2023), reproduced as Figure --. On the basis of this, the particular characteristics of operationalisation of the proposed CR are in table – below the image.

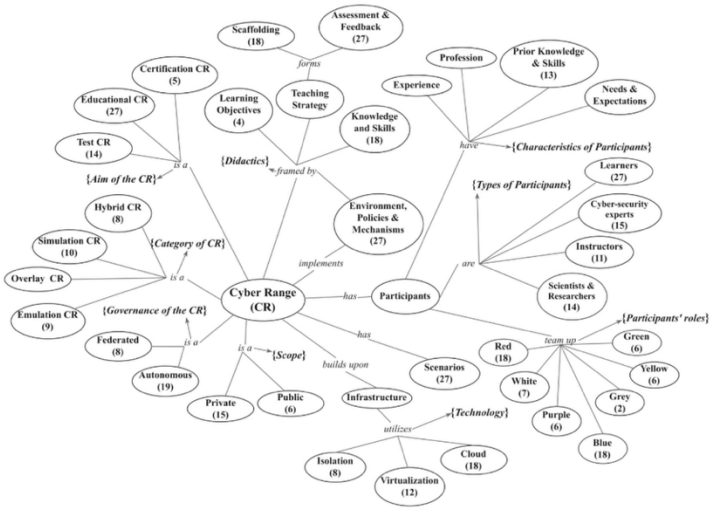

Figure 8: Topic Map of CR Characteristics

Characteristic Type	**BFSI Actors / Components**
Participants	Bank IT teams, SOC analysts, cybersecurity professionals, regulators (RBI, CERT-In, NCIIPC), auditors, academic researchers
Participant Roles	Incident responders, risk managers, compliance officers, red teamers, trainers, regulators

Characteristic Type	BFSI Actors / Components
Teams (Operational Structure)	Red Team (attackers), Blue Team (bank defenders), White Team (controllers), Purple Team (collaborative testing), Green Team (infrastructure), Yellow Team (scenario designers), Grey Team (regulators/auditors)
Purpose	Training (incident response), testing (system vulnerabilities), certification (skill validation), simulation (financial crises), research (threat analysis)
Types of Cyber Range	Hybrid CR (primary), Simulation CR (banking operations), Test CR (system validation), Educational CR (training), Certification CR (skills assessment)
Scenarios	Ransomware attacks on banking systems, UPI/payment failures, insider threats, fraud detection, phishing/social engineering, supply chain compromise
Infrastructure	Cloud environments, virtualised banking systems, sandboxed environments, secure isolated networks, partial physical emulation (critical systems)
Technologies	Virtualisation, containerisation, cloud platforms, orchestration tools, threat modelling frameworks (e.g., ATT&CK), data analytics tools
Orchestration	Scenario automation systems, access control mechanisms, workflow coordination engines
Capabilities	Attack simulation, user behaviour simulation, internet service simulation, scenario design, data collection and analysis, scoring and reporting
Governance	RBI oversight, CERT-In reporting compliance, NCIIPC coordination, DPDP-aligned data governance, audit and logging systems
Data Management	Synthetic/anonymised financial data, controlled datasets, secure storage, compliance with data protection laws
Learning & Evaluation	Competency tracking, performance metrics (MTTD, MTTR), feedback systems, structured training modules
Teaching & Training Strategy	Scenario-based learning, adversarial simulations, guided exercises, role-based training
Policy & Regulatory Integration	RBI cyber resilience framework, business continuity guidelines, CERT-In directives, sectoral compliance requirements

Characteristic Type	BFSI Actors / Components
Environment	Multi-institutional ecosystem involving banks, regulators, vendors, and infrastructure providers
Interdependencies	Interbank systems, payment networks (UPI, RTGS), telecom and power dependencies, vendor ecosystems
Access & Control	Role-based access systems, secure authentication, controlled simulation permissions
Audit & Reporting	Incident logging, breach reporting simulation (6-hour rule), compliance tracking
Deployment Model	Centralised (national range), decentralised (bank-level), shared (RaaS model), federated (cross-sector integration)
Cost Structure	Tiered model (large banks vs small banks), shared infrastructure, cloud-based cost optimisation
Capacity Building	Workforce training (NASSCOM, DSCI), institutional training programmes, continuous skill development
Risk Management	Controlled simulation environments, misuse prevention, scenario approval mechanisms

Table Mapping CR Characteristics to BFSI

Chapter 5 Summary

The chapter presents findings from expert interviews, organised through thematic analysis. It identifies key themes and triangulates these insights with secondary data and frameworks. Further, it bridges the gap between theory and practice by underlining actionable recommendations for strengthening cyber resilience in CII through operational CRs.

6. Component Blueprint for a BFSI-specific Cyber Range in India

Based on the multi-method approach adopted for this paper, a basic component blueprint for the creation of a BFSI-specific CR has been created, laying some minimum-standards for reference of banks, specially cooperative and small finance banks. It acknowledges that cyber incidents do not just disrupt systems, they also adversely impact the decision-making pathways. The structure of the CR contains eight main layers:

i. Contextual Infrastructure and Realism Layer: To ensure that the CR does not remain a technical system, but is in fact a socio-digital ecosystem simulation reflecting the people-process workflows of the real world, the layer will include the following components:

   a. The core banking system replica, including the transition from legacy, monolith architectures to modular, cloud-native and AI-enabled platforms;
   b. Payment ecosystem simulation, including the UPI, IMPS< NEFT, SWIFT flows;
   c. Customer interfaces of mobile banking and automated teller machine (ATM) networks;
   d. Hybrid infrastructure simulation that integrates manual and digital workflows. The following are the methods to simulate manual workflows into the CR:
      i. Manual workflows would include instances of manual approval of high-value transactions; phone and email-based verifications; physical escalation chains; paper-based fallback processes; human-led fraud verification; and crisis decision-making by senior management. It would simulate human-triggered processes and non-automated decision points.
      ii. Decision injection points where systems flag anomalies, or the simulation pauses/escalates- therein the participants must choose between approving or rejecting the flagging, escalating the anomaly, or delaying the response.
      iii. Role-based human simulation which would include roles of branch managers, compliance officers, fraud analysts and senior management, wherein the participants must communicate/escalate/coordinate.
      iv. Tabletop and live hybrid simulations which combine cyber attacks and decision making, such as ransomware attacks and system degradation.
      v. Communication simulation which would entail emails, phone calls and internal messaging pathways.
      vi. SOP execution tracking which checks the adherence to protocol, correct escalation paths and the time-limit abidance.

vii. Fallback mode simulating system downtime, wherein participants must switch to conducting operations manually, ensuring transaction continuity.

ii. Adversarial and Threat Evolution Engine Layer- The purpose of this engine is to create attack scenarios that are organised, evolving and cross-border in nature. To ensure that the attack library is not static, and a rather continuous R&D-driven scenario engine, it will include the following components:

a. MITRE ATT&CK-aligned attack library
b. APT simulation engine
c. Fraud and insider threat simulation
d. Attack modules based on social engineering and behavioural pattern recognition
e. AI-enabled attack scenarios.

iii. People-Process-Decision Simulation Layer- To bridge the gap of SOP adoption and understanding, being cognisant of the fact that performance level vary individual to individual, and even decision-making of an individual may differ in the scenario under different contexts, this layer includes:

a. Role-based simulation, which includes red teams (attackers); blue teamers (SOC teams/defenders/responders); and the purple team of regulators and the management
b. SOP execution engine which remains similar to layer 1
c. Decision-making simulation evaluating crisis response and leadership intervention, similar to layer 1
d. Behavioural simulation which tests stress conditions and the actors functioning with incomplete information.

iv. Systemic Interdependency and Ecosystem Layer- The BFSI is a highly interconnected system, and yet no synergy exists in the parallel systems. This layer is to replicate the external dependencies of the system that cause disruptions, delays and failures. Instead of simulating the entire systems, it simulates attacks that leads to a system failure, cueing in cascading effects. The components include:

a. Bank, fintech, NPCI and telecom simulations (from the bank's local environment)
b. SCADA linked disruption simulation

c. Interbank transaction flows
d. LEA interaction simulation

v. Orchestration, Control and Governance Layer- CRs run various inherent risks, and are unsafe environments. The attempt of this layer is to embed governance in design, and not just external regulation, through the following components:
   a. Scenario orchestration engine which ensures that tasks run in the correct sequence, at the right time and with proper error handling and retries
   b. Automated environment resets in order to avoid unintended data accumulation, and provide the CR clean, new environments under each new simulation.
   c. Sandbox isolation, air-gapped or controlled to completely isolate the workspace from public internet and untrusted networks.
   d. Malware and vulnerability control systems that prevent leakages
   e. Audit trails and activity logs to enhance traceability.

vi. Analytics, Evaluation and Outcome Layer- Since the mark of maturity should be outcome-based, a link needs to be established between training and measurable resilience. The blueprint suggests the following components to do so:
   a. Performance tracking, which notes response time and detection accuracy
   b. Behavioural analytics that include decision quality and protocol adherence
   c. Outcome metrics that evaluate incident containment, recovery efficiency and coordination effectiveness.

vii. Capacity Building and Learning Layer- This layer is introduced because capacity building must be intentional, and not an outcome aimed for. The training pathway for a participant would be of three stages, beginner, intermediate, and advance, along with the following components:
   a. Certification modules
   b. Feedback loops
   c. Scenario replaying and key insights for learning.

viii. Adaptive Layer- The CR must avoid being prescriptive in order to come at par with, and perhaps be a step ahead of, the cyberthreat actors. This layer tries to help systems evolve through:
   a. Dynamic scenario generation

b. Modular architecture, allowing the subparts to be developed, replaces or upgraded even at individual levels.

This component blueprint attempts to couple cyber resilience with cyber range as a direct feature. It aims to move beyond the technical-heaviness of CR thinking, to a more adaptive, outcome-oriented and institutionally embedded system that operationalises cyber resilience. However, one limitation of this kind of a CR is that it requires active reviewing, and does not encourage CR to be an isolated function of tech teams only.

6.1 Cyber Range Framework for the CII of India

The digitalisation of critical sectors has transformed the nature of risks associated with ecosystems today (Pricopoaia et al., 2025). The increasing dependence of CII on the ICT, and interconnected digital systems, has made cyber resilience a systemic and national concern, rather than just a technical one- particularly for the BFSI sector (George et al., 2024). Financial systems, especially for India, are beyond a repository of the economy- they are a crucial tool and pathway for public service delivery (Sood et al., 2024). With real-time transactions, resource allocation, and monetary banking, BFSI are the harbours of public trust and macroeconomic stability. Described as the 'heart of all' (P2) systems, by the virtue of being a fundamental structure of the CII, any disruption in the banking sector can cause cascading effects across multiple domains, affecting institutional functioning and societal confidence[20].

Existing approaches to cybersecurity in India have focused on retrospective measures which are technically heavy, remaining largely compliance-based and prevention-focused. The regulatory frameworks, including the guidelines by the Reserve Bank of India, have emphasised on cyber hygiene, risk management, and business continuity (Rao, 2011). CERT-In also introduced strict reporting requirements, and data retention (CERT-In et al., n.d.). Primary research suggests that even though there have been mandates for cyber crisis response management policies, many stakeholders of an organisation, after a particular designation, remain elusive of them, in spite of them being a system operator. While the measures seem necessary, they are not sufficient to address the simulation-based validation of cyber resilience under real-world circumstances. Thus, there arises a gap between theoretical preparedness and operational readiness.

[20] The CIA triad holds true

Global literature and best practices hint that such a gap can be fulfilled by the establishment of cyber ranges. Estonia's globally acclaimed CR14 cyber range ecosystem demonstrates how simulation environments can be institutionalised as national cyber defence strategy, harnessing large-scale sector coordination (*CR14*, n.d.). Singapore and Malaysia also have integrated adversarial simulations, structure evaluation metrics, and capacity building frameworks into their cybersecurity approaches (Monetary Authority of Singapore, 2021; (CyberSecurity Malaysia, 2022).

In order to enable the sectors within the CII to have a consolidated cyber range, and particularly to allow the BFSI have a CR such as the CR component blueprint, the present framework aims to propose a structured, contextually sensitive approach to the design and governance of CRs for the Indian CII.

6.1.1 Guiding Principles- Cyber Resilience

The framework is anchored in the core functions of cyber resilience, using them as the principles to base the framework on: prevention, detection, response and recovery. These dimensions frame a lens that can align both design and policy considerations.

Prevention extends beyond traditional perimetric defence, and includes proactive identification of vulnerabilities through simulation-based testing. Detection, on the other hand, emphasises on the real-time monitoring and anomaly detection, especially in complex and distributed systems. Response becomes the ability of the organisation to coordinate actions, reduce reaction time, smoothen the process of cooperation and communication, and bring together multiple stakeholders together under the conditions of uncertainty. Lastly, recovery, refers to the need of continuity of business operations, minimising systemic disruptions and mitigating cascading effects.

The shift towards resilience is evident in countries' framing of issues. Singapore's structured remediation cycles and adversarial attack simulations determine the importance of testing organisational (or collective) response to realistic threat scenarios. The CR framework of Malaysia reinforces making organisations resilient by creating indicators which are measurable, such as the MTTD and MTTR, which further links training and simulation to operational performances and readiness. These approaches taken together highlight how CRs cannot be viewed as technical tools alone, but they must be recognised as infrastructures for operationalising resilience across systems, institutions and processes.

6.1.2 Institutional Design: Multiple Actors

Institutional design of CRs is a fundamental and central feature of this proposed framework. Like Estonia, for CRs to be functional and accurately adopted, they must be conceptualised as platforms that facilitate interaction among multiple stakeholders, than just isolated environments confined to individual organisations.

The Indian regulatory and operational ecosystem involves a diverse and a vast range of actors, such as the RBI, CERT-In, NCIIPC, various financial institutions which actively communicate and facilitate the transactions with each other, LEAs, private sector technology providers, and the system end users at large. These actors operate within he action arena of a cyber range, within which, during exercises, they interact, communication, make decisions and coordinate for various tasks.

While in theory, such a platform seems complicated and nuanced to be reproduced, in practice, it already has been established by Estonia. The CR14 ecosystem integrates military, civilians, and private actors into a unified national framework, which also enables internation exercises and capacity building, furthering the culture of continuous preparedness.

While Estonia created such a model which fits its hybrid governance structure, India would require a comprehensive approach with central and sectoral regulators. The framework proposes an open-source dummy cyber range, which would require central oversight provided by sectoral regulators and national agencies, implemented in a decentralised manner across institutions- sharing the infrastructure which enables further participation of smaller entities. This could also help address the fragmentation currently observed in the Indian regulatory landscape, minimising institutional resistance and responsibility delegation.

6.1.3 Technical and Operational Design

The effectiveness of CRs depends significantly on their technical and operational designs. Drawing from global practices and ecosystem insights, this framework proposes some minimum baseline components that should be incorporated and adapted according to sector-specific requirements.

a. Realistic Simulation Environments

   Realism plays a critical role in the effectiveness of CRs. Globally, countries base attack simulations based on plausible threat scenarios, derived from structured threat intelligence. Dependencies also reflect the complexity of modern attack environments. Therefore, rather than replicating the entire system, more focus should

be laid on modelling impact pathways and dependencies, allowing participants experience cascading effects of a single faultline.

b. Threat Modelling and Scenario Design

CR exercises demand a well-defined scenario that is realistic and challenging. Global practices and professionals highlight that there is a need to clearly define the objectives, scope, and rules of engagement, prior to conducting simulations. Usage of MITRE ATT&CK is also recommended to standardise threat modelling. However, that should not be the expanse of the attacks. Scenarios must also incorporate

- advanced persistent threats (APTs),
- insider threats,
- social engineering, and
- AI-enabled attacks.

Additionally, the scenario designs must be dynamic, allowing for continuous updates and knowledge integration based on the evolving threat landscape.

c. Orchestration and Automation

It has been established that CRs are a complex environment, therefore, for scalability and efficiency, automation plays a critical role. To deliver this, infrastructure as code [21](IaC), and orchestration tools enable rapid deployment of scenarios, reducing manual effort and allowing for consistent execution across multiple environments. Globally, there has been emphasis on cloud-based CRs, including RaaS models[22], showing the importance of scalability in enabling wider adoption.

d. Analytics and Performance Measurement

A distinctive feature of advanced cyber range frameworks is their focus on measurable outcomes, as a direct mirror to the notional concept of resilience. Countries use metrics of duration taken to solve tasks, the severity of the tasks, and the number of tasks solved to evaluate the simulation performance while looking at the overall annual performance of an organisation in the real world as the outcome of CR program. In the Indian context, performance metric would include

- response time,
- decision accuracy,

[21] Infrastructure as code is a methodology for managing and provisioning computing infrastructure, providing machine-readable definition files for configuration: https://cloud.google.com/discover/what-is-infrastructure-as-code

[22] Malaysia's and Europe's emphasis on range-as-a-service models

- coordination effectiveness, and
- recovery time.

This basic metrics could help organisations to navigate evidence-based resilience assessments, beyond mere compliances.

6.1.4 Governance, Legal and Risk Considerations

While CRs operate as a controlled environments, they also simulate real-world attacks using real data of breaching and threat acting, which raises important legal and governance considerations.

a. Data Protection and Privacy

   CRs involve data that can be sensitive or representative of real-world systems and incidents. The establishment of a national CR for India would require compliance with the Digital Personal Data Protection Act, 2023. Thus, the following implications:

   - The use of synthetic or anonymised datasets,
   - Restrictions on data storage and sharing,
   - Safeguards to prevent the misuse of the CR and its learnings

   A caveat in the regulation is that a government body may use the data for national purposes. This decision-making lies with the governing bodies.

b. Regulatory Alignment

   CRs must also align themselves with existing regulatory mandates. The RBI's guidelines on cyber resilience and business continuity provide a foundation for resilience-focused practices, while CERT-In's reporting requirements necessitate the inclusion of audit and logging capabilities within simulation environments.

   This further suggests that a CR, along with attack simulations, should also:

   - Simulate compliance processes;
   - Test reporting mechanisms;
   - Evaluate adherence to regulatory timelines.

6.1.5 Risk Management

The potential risks associated with CR operation includes misuse of the environment and the unintended system impact. Strong mechanisms are required to mitigate these risks, including controlled execution of simulation; embedded layer of governance and oversight; strict granular control and access; and continuous monitoring. For an open-source national CR,

these layers are unavoidable. However, it must be maintained that the CR has to be secure, yet flexible for the environment to facilitate experimentation.

6.1.6 Capacity Building and Workforce Development

A CR function also lies in its ability to address the growing shortage of cybersecurity professionals, who are updated and capable enough to help curb the impacts of the currently increasing threat landscape. Best practices include capacity building, theoretical learning, practical exercises, real-world simulations and feedback mechanisms.

A CR must align with existing institutions such as NASSCOM and Data Security Council of India, along with the academic and training programmes. Capacity building must extend beyond technical skills, including:

- Decision-making during pressure
- Communication and coordination- inter and intra agency
- Understanding of the organisational SOPs

This also establishes CRs as a learning ecosystem than a mere technical platform.

6.1.7 Implementation and Fiscal Feasibility

The implementation of CRs within the CII requires a clearly defined institutional ownership structure, particularly given th emulti-actor nature f the Indian cybersecurity ecosystem. While resilience is often framed at the organisational elevel, the operationalisation of the same required coordinated involvement of regulators, national agencies and private stakeholders. Thus, a distributed yet coordinated model may befit the Indian context. The RBI would have a central role to play in mandating the adoption and defining minimum standards for CR implementation within the BFSI sector. National coordination and cross-sectoral integration within the CII could be overseen by the NCIIPC, whereas the CERT-In would contribute to maintaining threat intelligence inputs and supporting scenario design.

` Operationally, individual financial institutions would be responsible for customisation of the CR environment for their context. Industry bodies like the DSCI and NASSCOM would play a role in certification, training and workforce development. Integration of private organisations that provide RaaS like Bhumi iTech could help in understanding and optimising CRs.

This distributed model attempts to address the coordination challenges identified in both, literature and interviews, while carefully avoiding over-centralisation that may limit flexibility.

i. Cost Architecture

The BFSI sector has heterogeneous institutions. Therefore, having a uniformed budget model may not be feasible. A tiered approach, instead, would help in better adoption, aligning with differences in institutional capacity, scale, and resource availability.

The framework proposes three broad tiers:

a. Tier 1: Large Scheduled Commercial Banks
   Major public and private sector banks possess the financial and technical capacity to develop in-house or hybrid CR environments. For these institutions, investments may focus on advanced simulation capabilities, integration with existing security operations centres, and custom scenario development.
b. Tier 2: Mid-sized Institutions
   These include cooperative and regional banks. These institutions may benefit from shared infrastructure models, including sector-level CRs or centrally supported platforms. RaaS model may be particularly of use here, which allows access to advanced simulation environments without requiring significant capital investment.
c. Tier 3: Small Finance and Payment Banks
   For smaller institutions, an open-source or centrally provisioned CR model could be appropriate. The use of lightweight simulation environments, standardised scenarios, and shared training modules, along with teams that can facilitate adoption or customisation of the open source CR- would all be included. The provision of the CR blueprint and the creation of a supporting framework particularly cater to this tier.

Tiered approach for the framework accommodates varying levels of digital maturity, ann ensures that CR access is not limited to large institutions alone.

ii. Capital and Operational Expenditure

The economic feasibility of CRs depends on clear distinction between cap expenditure (CapEx), and operation expenditure (OpEx), having different implications for plicy design and institutional adoption.

CapEx includes the following costs:

- Infrastructure setup- such as cloud or on-premise environments;
- Platform development or licensing;
- Creation of initial scenario libraries;
- Network architecture and sandbox environments.

OpEx would include:

- Continuous scenario updates and threat modelling;
- Staffing- which includes red team and blue team facilitators;
- Maintenance and vendor support;
- Training and certification programmes;
- Coordination across institutions

If the CR is open-source or shared, the Capex reduces significantly. However, OpEx costs cannot be ignored, and would be accompanied by higher OpEx requirements, particularly in relation to maintaining and updating scenario libraries and ensuring relevance to evolving threat landscapes.

6.1.8 Justification

CR development is not a standalone expenditure. It is a risk-adjusted investment, aligned with existing cybersecurity and operational risk management frameworks. Availale estimates suggest that data breach costs in India exceed two million in US dollars. A ransomware incident would cost slightly higher, and would have detrimental cascading effects in the CI. In the BFSI sector, such incidents would cause reputational damage and feed into the trust factor. Thus, an investment in CR would contribute to reduced incident response time; improved coordination during crises; minimised operational disruption; and enhanced regulatory compliance.

Financial sector regulations already exist, which this framework aims to align with. They view investments in risk mitigation in relation to potential losses, rather than as isolated costs.

6.1.9 Phased Implementation

A three-phased model, usually used for large-scale implementation, could be deployed as a structured pathway for framework adoption.

a. Phase 1: Foundational Stage- Years 1 and 2
    - Pilot implementation across a limited number of institutions representing different tiers.

- Development of baseline cyber range infrastructure
- Establishment of governance mechanisms and technical standards
- Initial integration with national agencies

Phase 2: Scaling Stage - Years 3 and 4

- Expansion to additional institutions within the BFSI sector
- Operationalisation of shared infrastructure models (RaaS)
- Conduction of inter-institutional simulation exercises
- Development of certification and training frameworks

Phase 3: Maturation Stage - Year5 and Beyond

- Development of federated cyber range networks
- Integration with national and sectoral exercises
- Adoption of outcome-based evaluation mechanisms
- Exploration of international interoperability

This phase approach allows for gradual scaling while incorporating feedback and lessons learned from earlier stages, along with scope for amendments as per sectoral developments.

Open-Source Cyber Range Model and Indigenisation

The potential role of open-source CR platforms is an important consideration for the Indian context. Developing systems from scratch run the risk of failure, double effort, and resource intensity. Existing frameworks like OpenCyberRange[23] and KYPO[24] could provide the foundation for implementation. These platforms can be adapted and indigenised by:

- Incorporating BFSI-specific scenarios
- Aligning with Indian regulatory requirements
- Integrating with local threat intelligence

An open-source approach may also offer several other advantages, such as:

- Reduced initial costs
- Flexible customising

[23] View https://opencyberrange.com/
[24] Visit https://crp.kypo.muni.cz/

- Avoidance of vendor lock-in

However, the trade-off is not free of the challenges:

- Maintenance and updates
- Quality assurance
- Long-term sustainability

PPP Consideration

The development and operation CRs, in order to be accurately updated and remain technical competent, would require contribution of public institutions and private technology providers, including academic institutes. This raises certain policy considerations:

- Procurement models and contracting structures;
- Intellectual property ownership;
- Data sovereignty and localisation requirements

A well-defined PPP framework may be necessary to ensure that the said challenges are addressed while enabling innovation and efficiency.

6.2 Adaptive and Context-Sensitive Framework

Global lessons highlight the dire requirement and accommodation of flexibility. Frameworks allow organisations to determine the frequency and scope of simulations based on their specific risk profiles, while providing structured guidelines without excessive rigidity. Similarly, the proposed framework advocates for:

- Minimum baseline standards;
- Flexibility in implementation;
- Continuous adaptation to evolving threats.

6.3 Policy Gaps in India

The absence of a publicly accessible national cyber range framework represents a significant gap in India's cybersecurity ecosystem. While various institutions and guidelines exist, there is limited integration across sectors, without a standardised approach to simulation-based resilience testing. To address this gap, this framework aims to:

- Provide a structured design for CRs
- Integrate institutional and technical dimensions

- Align with existing regulatory mandates.

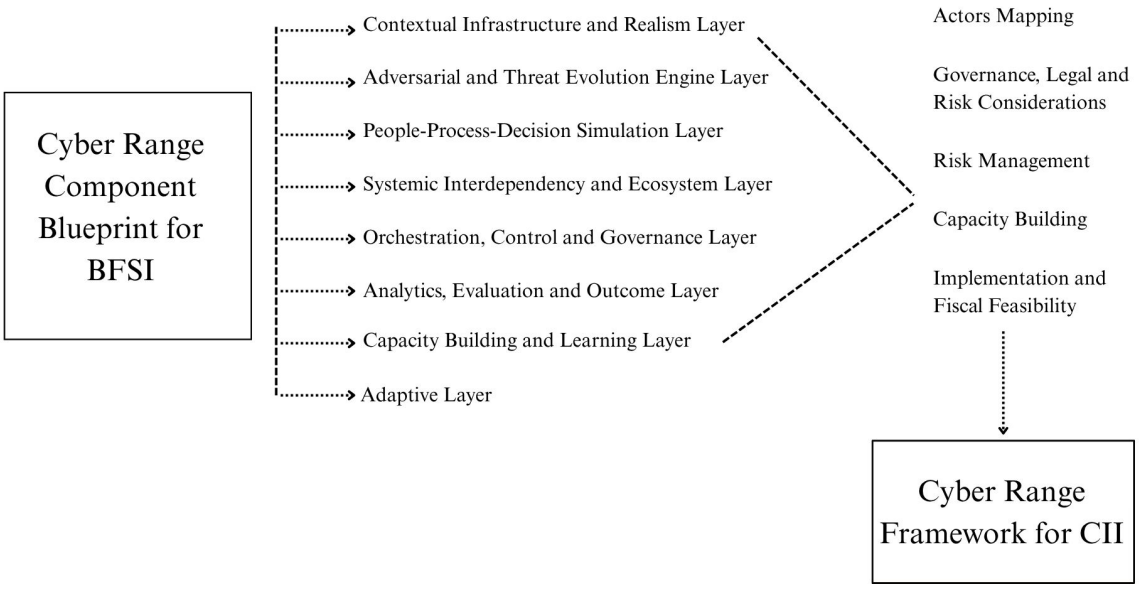

Figure 9: Cyber Range Component and Framework Map

7. Concluding Remarks

At its core, the framework aims to emphasise that cyber resilience is not merely a technical capability, but also an institutional and operational outcome, which calls for coordinated action across sectors, rules, actors, systems and processes. The development of CRs for CII represents an important step toward strengthening cyber resilience in India. By drawing on global best practices and adapting to local conditions, the proposed framework provides a foundation to move beyond reactive cybersecurity and toward proactive, system-wide resilience.

Digitisation acts as a boon, but also injects systemic vulnerabilities that can have a multi-fold impact. While technological advancement is a policy conversation, cybersecurity and guardrails, with alternative methods than relying on LEAs and compliance, need to be made part of the broader dialogue. CRs present an optimal solution to operationalise cyber resiliency goals and can situates well within the regulatory mandates of India.

The study's contribution attempt to be two-fold. First as an eight-layer CR design moving beyond technical heaviness and embedding governance, behavioural simulation, systemic interdependency and outcome-based evaluation in the CR architecture itself. Second, the CR framework for the CII of India, proposing a structured, contextualised and

institutionally grounded approach to the design, governance and phased-implementation of CRs. It aims to be a reference point for regulators and researchers, and an angle to start the dialogue from.

It must be acknowledged that the study is purely exploratory and indicative, and not exhaustive. The sample of eight interviews, while rich in expertise, may limit the representativeness. The fiscal modelling is directional than definitive, and is mostly a starting point. The classified nature of certain government frameworks limits the depths of comparative analysis possible. However, the central of the argument remains that India's current approach to cyber resilience is structurally insufficient, and requires a policy tool, such as a cyber range. Cybersecurity has been treated as a technical problem for long, ignoring its other dimensions of institutional learning and functioning within adversity. There is a need for genuine preparedness than performative compliance, with a multi-actor, socio-technical design, securing systems in practice, and not paper (or firewalls).

References

A, P. A., Seyedi, S., Komendantova, N., Yazdanpanah, M., & Mannocchi, M. (2025). The institutional analysis and development framework: A mathematical representation in water arena. *Current Research in Environmental Sustainability*, *10*, 100307. https://doi.org/10.1016/j.crsust.2025.100307

Abiona, O. S. (2024). *Cybersecurity policy frameworks in the public sector* [Journal-article].

Adelusi, J. B. (2023). Third-Party and Supply Chain Risks in Financial Services: An Analytical Exploration. *Research Gate*. https://www.researchgate.net/publication/387787302_Third-Party_and_Supply_Chain_Risks_in_Financial_Services_An_Analytical_Exploration

Alnajim, A., Habib, S., Islam, M., Thwin, S., & Alotaibi, F. (2023). A comprehensive survey of cybersecurity threats, attacks, and effective countermeasures in industrial internet of things. *Technologies*, *11*(6), 161. https://doi.org/10.3390/technologies11060161

Alzide, S. (2024). Cloud Computing: evolution, challenges, and future prospects. *Journal of Information Technology, Cybersecurity, and Artificial Intelligence.*, *1*(1), 52–63. https://doi.org/10.70715/jitcai.2024.v1.i1.007

Andrew, J. (2023). THE EVOLVING CYBER THREAT LANDSCAPE AND THE POWER OF ARTIFICIAL INTELLIGENCE IN DEFENSE. *Researchgate*.

Antonopoulos, M., Drainakis, G., Ouzounoglou, E., Papavassiliou, G., & Amditis, A. (2022). Design and proof of concept of a prediction engine for decision support during cyber range attack simulations in the maritime domain. *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, 305–310. https://doi.org/10.1109/csr54599.2022.9850280

Bharat NCX 2024 Concludes with Unprecedented Success: Over 600 Participants Trained, Key Initiatives Launched, and Innovations Showcased. (n.d.). https://www.pib.gov.in/PressReleasePage.aspx?PRID=2079609®=3&lang=2

Brissett, A., & Wall, J. (2025). Machine learning and watermarking for accurate detection of AI-Generated phishing emails. *Electronics*, *14*(13), 2611. https://doi.org/10.3390/electronics14132611

Cedergren, A., & Hassel, H. (2023). Building organizational adaptive capacity in the face of crisis: Lessons from a public sector case study. *International Journal of Disaster Risk Reduction*, *100*, 104235. https://doi.org/10.1016/j.ijdrr.2023.104235

Ciso, E. (2026, February 16). India faces over 3,100 weekly cyber-attacks as AI drives new security shift. *ETCISO.in*. https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/india-faces-surge-in-cyber-attacks-as-ai-revolutionizes-cybersecurity/128419177

CR14. (n.d.). CR14. https://www.cr14.ee/

Critical Information Infrastructure (CII) | Department of Financial Services | Ministry of Finance | Government of India. (n.d.). https://financialservices.gov.in/beta/en/page/cii

Cyber Range Project Team & NICE Community Coordinating Council. (2023). *CYBER RANGE GUIDE* [Report]. https://www.nist.gov/system/files/documents/2023/09/29/The%20Cyber%20Range_A%20Guide.pdf

CyberSecurity Malaysia. (n.d.). CYBER RANGE FRAMEWORK: A REVIEW FOR GLOBAL ACE CERTIFICATION. In *CYBER RANGE FRAMEWORK: A REVIEW FOR GLOBAL ACE CERTIFICATION* (p. 1).

Cyberwarfare simulations between nations: Training in the modern cyber range. (2025, June). Medium. https://medium.com/@aditrizky052/cyberwarfare-simulations-between-nations-training-in-the-modern-cyber-range-2f6174e34dee

Data Security Council of India (DSCI), SEQRITE, Godse, V., & Katkar, S. (2023). *INDIA CYBER THREAT REPORT 2023* (By Data Security Council of India (DSCI) & SEQRITE). https://www.dsci.in/files/content/knowledge-centre/2023/India-Cyber-Threat-Report-2023_0.pdf

Dervishaj, B., Dervishaj, N., & Mucaj, E. (2025). Cybersecurity in fintech: challenges and strategies. *The Proceedings of the International Conference on New Ideas in Management, Economics and Accounting.*, *2*(1), 10–23. https://doi.org/10.33422/imeaconf.v2i1.1005

Director, D. M. (n.d.). *DBT Schemes | (DBT) Direct Benefit transfer*. DBT | Direct Benefit Transfer. https://dbtbharat.gov.in/central-scheme/list

ECSO WG5. (2025). *CYBER RANGE FEATURES CHECKLIST & LIST OF EUROPEAN PROVIDERS*. https://ecs-org.eu/ecso-

uploads/2025/02/Cyber_Range_Features_Checklist__List_of_European_Providers_2025.pdf

Elia, G., Solazzo, G., Lerro, A., Pigni, F., & Tucci, C. L. (2024). The digital transformation canvas: A conceptual framework for leading the digital transformation process. *Business Horizons*, *67*(4), 381–398. https://doi.org/10.1016/j.bushor.2024.03.007

EU defence initiatives. (n.d.). Default. https://eda.europa.eu/what-we-do/EU-defence-initiatives

European Cyber Security Organisation (ECSO). (2020). *Understanding Cyber ranges: From hype to reality*.

Finio, M., & Downie, A. (2026, January 23). Cyber range. *IBM*. https://www.ibm.com/think/topics/cyber-range#:~:text=A%20cyber%20range%20is%20a,various%20cybersecurity%20tools%20and%20functionality.

Gaidosch, T., Adelmann, F., Morozova, A., & Wilson, C. (2019). Cybersecurity Risk Supervision. *Departmental Paper*, *19*(15). https://doi.org/10.5089/9781513507545.087

Gallo, L., Gentile, D., Ruggiero, S., Botta, A., & Ventre, G. (2023). The human factor in phishing: Collecting and analyzing user behavior when reading emails. *Computers & Security*, *139*, 103671. https://doi.org/10.1016/j.cose.2023.103671

George, D., Dr.T.Baskar, & Srikaanth, D. (2024a). Cyber Threats to critical Infrastructure: Assessing vulnerabilities across key sectors. *Zenodo (CERN European Organization for Nuclear Research)*. https://doi.org/10.5281/zenodo.10639463

George, D., Dr.T.Baskar, & Srikaanth, D. (2024b). Cyber Threats to critical Infrastructure: Assessing vulnerabilities across key sectors. *Zenodo (CERN European Organization for Nuclear Research)*. https://doi.org/10.5281/zenodo.10639463

Guo, Y. (2022). A review of Machine Learning-based zero-day attack detection: Challenges and future directions. *Computer Communications*, *198*, 175–185. https://doi.org/10.1016/j.comcom.2022.11.001

Hossain, M. A., Raza, M. A., Mahjabeen, F., & Rahman, J. Y. (2025). Assessing the vulnerabilities of mobile banking applications and developing strategies to improve their security. *Jurnal Ekonomi Dan Bisnis Digital*, *4*(1), 1–18. https://doi.org/10.55927/ministal.v4i1.13371

Howlett, M. (2015). Policy analytical capacity: The supply and demand for policy analysis in government. *Policy and Society*, *34*(3–4), 173–182. https://doi.org/10.1016/j.polsoc.2015.09.002

Hypr. (2025, April 28). *What is NotPetya? 5 Fast Facts | Security Encyclopedia*. https://www.hypr.com/security-encyclopedia/notpetya#:~:text=NotPetya%20was%20a%20modified%20version,fully%20infected%20in%2016%20seconds.

Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. *PeerJ Computer Science*, *10*, e1772. https://doi.org/10.7717/peerj-cs.1772

Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, & Government of India. (n.d.). Guidelines on Information Security Practices for Government Entities. In *Guidelines on Information Security Practices for Government Entities* (pp. 1–7). https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf

India's DBT: Boosting Welfare Efficiency. (n.d.). https://www.pib.gov.in/PressReleasePage.aspx?PRID=2123192®=3&lang=2

India's digital revolution: transforming infrastructure, governance, and public services. (n.d.). https://www.pib.gov.in/PressReleasePage.aspx?PRID=2082144®=3&lang=2

ISAC in a box | ENISA. (n.d.). https://www.enisa.europa.eu/tools/isac-in-a-box

ISO / IEC 27032-2012. (2013). National Cyber Security Policy -2013. In *National Cyber Security Policy -2013* (pp. 1–3). https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf

John, C., & John, C. (2019, January 31). SBI leaked sensitive financial data of millions of customers. *TheQuint*. https://www.thequint.com/tech-and-auto/tech-news/sbi-leaks-financial-data-of-millions-of-customers-server-insecure

Karjalainen, M., & Kokkonen, T. (2020). Comprehensive Cyber Arena; The Next Generation Cyber Range. *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 11–16. https://doi.org/10.1109/eurospw51379.2020.00011

Katsantonis, M. N., Manikas, A., Mavridis, I., & Gritzalis, D. (2023). Cyber range design framework for cyber security education and training. *International Journal of Information Security*, *22*(4), 1005–1027. https://doi.org/10.1007/s10207-023-00680-4

Khiaonarong, T., Zheng, S., Tanai Khiaonarong, Shanyuan Zheng, Tohid Atashbar, Tobias Lindqvist, Majid Malaika, Garth Nicholls, Anca Paduraru, Marco Reuter, Puja Singh, Frankosiligi Solomon, Jay Surti, Tomohiro Tsuruga, Ying Xu, & Marie-Bernadette Amand de Mendieta. (2026). The rise of cyber events and digital fraud in the financial sector. *IMF Working Papers*.

Kovács, T. A., Nyikes, Z., & Fürstner, I. (2022). Security-Related advanced technologies in critical infrastructure protection. In *NATO science for peace and security series. C, Environmental security*. https://doi.org/10.1007/978-94-024-2174-3

Kumar, A., Shukla, P., Sharan, A., Mahindru, T., NITI Aayog, Sarkar, A., Nayan, A., Asthana, K., Wadhwani Institute for AI, Gupta, M., Raskar, R., nVIDIA, Intel, IBM, NASSCOM, McKinsey, Accenture, Roy, A., & Kant, A. (n.d.). National Strategy for Artificial Intelligence. In *National Strategy for Artificial Intelligence* [Report]. https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf

Kumar, S. V. (2026). Impact of US and Israel War with Iran On Global Economy With Special Reference to India -A Critical Analysis. *Research Gate*. https://doi.org/10.13140/rg.2.2.30191.80806

Lazarov, W., Schafeitel-Tähtinen, T., Squillace, J., Martinasek, Z., Coufalikova, A., Helenius, M., Gallus, P., & Fujdiak, R. (2025). Lessons Learned from Using Cyber Range to Teach Cybersecurity at Different Levels of Education. *Technology, Knowledge and Learning*. https://doi.org/10.1007/s10758-025-09840-y

Leviäkangas, P., Paik, S. M., & Moon, S. (2017). Keeping up with the pace of digitization: The case of the Australian construction industry. *Technology in Society*, *50*, 33–43. https://doi.org/10.1016/j.techsoc.2017.04.003

Linkov, I., & Kott, A. (2018). Fundamental Concepts of Cyber Resilience: Introduction and Overview. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1806.02852

Mallick, P. K., VSM (Retd) & Vivekananda International Foundation. (2024). *Protection of critical information infrastructure*. Vivekananda International Foundation. https://www.vifindia.org/sites/default/files/Protection-of-Critical-Information-Infrastructure.pdf

Management Alliance. (2022). Cyber-attack timelines: Educational guides to understanding attacks & enhancing resilience. In *Cyber-attack Timelines: Educational Guides to Understanding Attacks & Enhancing Resilience*.

Maurer, T., Nelson, A., GLOBAL, & European Systemic Risk Board. (2021). Cyber threats to the financial system are growing, and the global community must cooperate to protect it. *FINANCE & DEVELOPMENT*, 24–26. http://www.usasurvival.org/uploads/1/2/6/3/126369300/global-cyber-threat-to-financial-systems-maurer__1_.pdf

Mersinas, K., Bada, M., & Furnell, S. (2024). Cybersecurity behavior change: A conceptualization of ethical principles for behavioral interventions. *Computers & Security*, *148*, 104025. https://doi.org/10.1016/j.cose.2024.104025

Mohammed, I. A., Priya, A. C. D. M. S., & Thirupathi, V. a. D. M. (2020). *Global dimensions of Multidisciplinary Research*. https://doi.org/10.25215/9371837764

Monetary Authority of Singapore. (2021). *Technology Risk Management Guidelines*.

Morgan, J. (2022). Public-Private partnerships and collective cyber defence. In *2022 14th International Conference on Cyber Conflict* [Conference-proceeding]. NATO CCDCOE Publications, Tallinn.

Morrás, M. (2024, December 16). *What Is Phygital? Meaning, definition, and examples*. Veridas. https://veridas.com/en/what-is-phygital/

Nadeau, J. (2025, November 18). 2024 roundup top data breach stories and industry trends. *IBM*. https://www.ibm.com/think/insights/2024-roundup-top-data-breach-stories-and-industry-trends

Ostrom, E. & UNESCO – EOLSS. (2002a). INSTITUTIONAL ANALYSIS AND DEVELOPMENT: ELEMENTS OF THE FRAMEWORK IN HISTORICAL PERSPECTIVE. In *Encyclopedia of Life Support Systems (EOLSS)* [Book-chapter]. http://www.eolss.net/sample-chapters/c04/e6-99a-34.pdf

Ostrom, E. & UNESCO – EOLSS. (2002b). INSTITUTIONAL ANALYSIS AND DEVELOPMENT: ELEMENTS OF THE FRAMEWORK IN HISTORICAL

PERSPECTIVE. In *Encyclopedia of Life Support Systems (EOLSS)* [Book-chapter]. http://www.eolss.net/sample-chapters/c04/e6-99a-34.pdf

Panagariya, A. (2022). Digital revolution, financial infrastructure and entrepreneurship: The case of India. *Asia and the Global Economy*, *2*(2), 100027. https://doi.org/10.1016/j.aglobe.2022.100027

Patrick, D., Gilbert, D. P., Jr, Johns Hopkins University, Applied Physics Lab, & Booz Allen Hamilton. (n.d.). The Information Sphere Domain. In *The Information Sphere Domain Increasing Understanding and Cooperation*. https://ccdcoe.org/uploads/2018/10/09_GILBERT-InfoSphere.pdf#:~:text=The%20following%20examples%20show%20how%20the%20four,are%20required%20to%20operate%20in%20that%20Domain.

Pricopoaia, O., Cristache, N., Lupașc, A., & Iancu, D. (2025). The implications of digital transformation and environmental innovation for sustainability. *Journal of Innovation & Knowledge*, *10*(3), 100713. https://doi.org/10.1016/j.jik.2025.100713

Rao, G. J. M. (2011). Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds. In *Reserve Bank of India*.

Reis, J., & Melão, N. (2023). Digital transformation: A meta-review and guidelines for future research. *Heliyon*, *9*(1), e12834. https://doi.org/10.1016/j.heliyon.2023.e12834

Role of regulator in governance: Case study of Reserve Bank of India in safeguarding Consumer interest. (n.d.). https://www.iipa.org.in/GyanKOSH/posts/role-of-regulator-in-governance-case-study-of-reserve-bank-of-india-in-safeguarding-consumer-interest

Ross, R., & Pillitteri, V. (2024). *Protecting controlled unclassified information in nonfederal systems and organizations*. https://doi.org/10.6028/nist.sp.800-171r3

Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, *2*, 100034. https://doi.org/10.1016/j.jeconc.2023.100034

Sarker, I. H., Janicke, H., Ferrag, M. A., & Abuadbba, A. (2024). Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions towards automation, intelligence and transparent cybersecurity modeling for critical infrastructures. *Internet of Things*, *25*, 101110. https://doi.org/10.1016/j.iot.2024.101110

Sharma, R. (2022, November 4). Why policies fail: An institutional perspective. *The India Forum*. https://www.theindiaforum.in/society/why-policies-fail-institutional-perspective#:~:text=Coordinated%20action%20was%20difficult%20because,there%20were%20two%20coordinating%20agencies.

Sharma, S., Ahuja, M., State Bank of India, & State Bank of India. (2025). MITIGATING CYBER THREATS IN THE BFSI SECTOR: AI-DRIVEN RISK MANAGEMENT AND RESILIENCE STRATEGIES. In *The Journal of Indian Institute of Banking & Finance*.

Shin, Y., Kwon, H., Jeong, J., & Shin, D. (2024). A study on designing cyber training and cyber range to Effectively respond to cyber threats. *Electronics*, *13*(19), 3867. https://doi.org/10.3390/electronics13193867

Sinha, S., Singh, A., Nayar, S., Sood, D., Agarwal, V., Hiranandani, N., Goenka, B. K., Bali, Cmdr. N., & Malhotra, P. (2023). India leading the global digital transformation journey. *ASSOCHAM*, 1–23. https://www.assocham.org/uploads/files/Digital%20Transformation.pdf

SISA, CERT-IN, CSIRT-FIN, & KRISHNAN, S. (n.d.). DIGITAL THREAT REPORT 2024. In *DIGITAL THREAT REPORT 2024*.

Sood, D., Gandhi, M., & Patil, V. (2024). Role of financial services in the making of Viksit Bharat – Vision 2047. In ASSOCHAM & PwC, *ASSOCHAM*.

Statista. (2026, January 9). *Number of IoT connections worldwide 2022-2034*. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/?srsltid=AfmBOoqTyV0Qb06lCHbif9eTmsfydI73SB_tXUh8qUpABhwNMzJKy7Pv

Steininger, C. (2025). Creating a Framework for Platform-Independent Cyber Range Scenarios. *IEEE/IFIP Network Operations and Management Symposium*, 1–4. https://doi.org/10.1109/noms57970.2025.11073733

Susnjara, S., & Smalley, I. (2026, January 9). Cyber Resilience. *IBM*. https://www.ibm.com/think/topics/cyber-resilience

Tang, J., Saade, T., Kelly, S., & The Institute for Security and Technology. (2024). The Implications of Artificial intelligence in Cybersecurity: Shifting the Offense-Defense Balance. In *The Implications of Artificial Intelligence in Cybersecurity: Shifting the Offense-Defense Balance*. The Institute for Security and Technology. https://securityandtechnology.org/wp-content/uploads/2024/10/The-Implications-of-Artificial-Intelligence-in-Cybersecurity.pdf

Tella, S., & Raju, P. (2020). IoT Enabled smart banking system. *Journal of Information Technology, Cybersecurity, and Artificial Intelligence*. https://doi.org/10.13140/rg.2.2.25610.08644

The Global Hues. (2023, December 2). Cyber Security for banking and finance | The Global Hues. *The Global Hues | World Meet Media*. https://theglobalhues.com/cyber-security-for-banking-and-finance/

The Fourth Industrial Revolution: What it means, how to respond. (2016, January). World Economic Forum.

The Hindu Bureau. (2022, December 16). *1.3 TB data encrypted and five servers affected in AIIMS ransomware attack: Centre*. The Hindu. https://www.thehindu.com/news/national/13-tb-data-encrypted-in-ransomware-attack-on-aiims-by-unknown-threat-actors-centre/article66271226.ece

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: a historical and conceptual review. *International Journal of Information Security*, *23*(3), 1695–1719. https://doi.org/10.1007/s10207-023-00811-x

Uberoi, A. (n.d.). *AIIMS ransomware attack*. https://www.cm-alliance.com/cybersecurity-blog/aiims-ransomware-attack

Ukwandu, E., Farah, M. a. B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., Tachtatzis, C., Bures, M., Andonovic, I., & Bellekens, X. (2020). A review of Cyber-Ranges and Test-Beds: Current and future trends. *Sensors*, *20*(24), 7148. https://doi.org/10.3390/s20247148

Viksit Bharat: Unshackling job creators and empowering growth drivers. (2024). https://www.niti.gov.in/sites/default/files/2024-07/WP_Viksit_Bharat_2024-July-19.pdf

Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2503.22710

What is a data leak? 6 common causes for data leak | Fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/data-leak

Yeboah-Ofori, A., & Opoku-Boateng, F. A. (2023). Mitigating cybercrimes in an evolving organizational landscape. *Continuity & Resilience Review*, *5*(1), 53–78. https://doi.org/10.1108/crr-09-2022-0017

Appendix

name	codegroup 1	codegroup 2	codegroup 3	codegroup 4
people process and technology.	capacity building	elements	actors	governance
west is more sophisticated	the west			
digital gaps	gaps			
mature western society	the west			
systems are inflexible	the west			
digital first	objectives	gaps	capacity building	
following the process.	components	capacity building		
team-based exercises	components	types		
solo exercises	components			
process oriented exercises	elements	components		
baseline	components			

scenarios	components			
level of control	governance	elements	components	
ideal evaluation	objectives	gaps	components	elements
lesser incidents	objectives	elements	capacity building	
minimising the incidents	objectives	elements	governance	
better outcomes	objectives			
post-incident management	objectives	components	actors	capacity building
malicious or vulnerable systems	capacity building	elements		
red teaming	actors			
dirty environment	elements	components		
security guardrails	governance	components	elements	
cyber accident within cr	components	gaps		
sandbox environment	elements	governance		
isolated	elements	components		
physical isolation	components	elements		
auditing the platform	governance			
cataloguing the vulnerabilities	elements	objectives		
no creep	governance	components	objectives	
proper signatures	components			
learning and development	elements	gaps	objectives	capacity building
don't end up amplifying	elements	actors	objectives	governance
architectural elements	components	elements		

security top down	elements	governance		
competing engagement	components			
bottom up	components	governance		
control structures	governance	elements		
encourage their usage	actors	objectives	capacity building	governance
no prescription	elements	capacity building		
proactive	objectives	governance	actors	
screening of staff	actors	elements	governance	
retraining the staff	elements	capacity building	actors	
capacity and capability and compliances	objectives	elements	capacity building	governance
3C	objectives	elements		
anticipate	elements			
recover	components			
sticking to the traditional	gaps	governance		
attackers are advanced	actors	elements	components	
AI-based attacks	components			
budget	elements	governance		
track all the attacks.	elements			
false security	gaps			
investment	gaps	objectives	elements	governance
will and seriousness	governance			
separate budget	governance			

security compliances	governance	components		
personal data	components	governance		
separate team	governance	capacity building		
incompatible decision making	gaps	governance		
freedom	objectives	gaps	capacity building	elements
independent	elements	governance		
sector specificity	elements	actors		
core banking system	elements			
heart of all	components	elements		
sensitive information	components			
top down	elements	governance		
R&D	capacity building	governance	components	
indigenous attack scenarios	components			
flag-based evaluation				
mapping to list	components			
incident	components			
identify	elements			
protect response	components			
replicating	components			
hands-on	objectives	elements		
trainings from the vendor	elements			
good network	gaps	components		
VM-based approach	components			

how to use	gaps			
decision making	objectives	elements	governance	
identify, detect, protect, respond	elements	capacity building		
flexibility	governance			
not be custom	elements			
SOPs	components	capacity building	governance	elements
uninterested	governance	gaps		
employees	components	actors		
social engineering	components			
our role playing	capacity building	actors		
completely blank	gaps	capacity building		
drills	objectives	elements	capacity building	
prepare in advance	objectives			
natural disaster	elements			
No one is safe	gaps	capacity building	elements	
small SMEs	actors			
creating a bridge	objectives	elements	capacity building	governance
platform	components			
user behaviour	components	elements	actors	capacity building
organisational responses	elements	governance	actors	capacity building
simulating transaction	components			
trust system	elements	governance		
regulatory dependencies	governance	gaps	components	
5 layers	components			

infrastructure simulation	components			
APT style campaigns	components			
MITRE	components			
APT	components			
quality level	governance	components		
tend to fail	governance	gaps		
simulate continuity under attack	elements	objectives	capacity building	
cannot just shut down	components			
trust	capacity building	objectives		
evaluation	components	governance		
remain adaptive	objectives	capacity building		
range as a service	types			
hybrid model	types			
enable	objectives	capacity building		
overstandardization	gaps			
mark of maturity	components	elements	objectives	gaps
capability gap	gaps	capacity building		
integration gap	gaps			
lack of cs rules	gaps			
uneven digital maturity	gaps			
manually	gaps			
compromise and interbank coordination	objectives	capacity building		

similar methodology				
aims and objectives	elements			
char- acteristics of the participants	actors	elements	governance	
roles participants adopt	components			
Educational CRs	types			
organized learn- ing environment	objectives	elements		
hands-on practice				
Certification CR	types			
cybersecurity knowledge	objectives	capacity building		
competitions	components	elements		
Test CRs	types			
monitor the learners	actors	components		
role of the instructors	actors	components		
role of the cyber security experts	actors	components		
perform technical tasks	components	actors	capacity building	
most com- mon roles	actors	components		
blue	components			
red team	actors	capacity building		
defenders	components	actors		
role of forensics investigators	actors	components		

perform cyber-attacks	actors	components	capacity building	
role of attackers	actors	components		
gover- nance	elements	objectives	actors	governance
Autonomous CRs,	types			
Federated CRs	elements	types		
reduced costs	governance	objectives		
organizers share	objectives	governance		
specific oper- ating standards	elements	objectives	governance	

Annexure A: Institutions considered as the CII of India

Organisation	Date of Notification
1	Reserve Bank of India (RBI)
2	National Payments Corporation of India (NPCI)
3	ICICI Bank
4	HDFC Bank
5	LIC of India
6	Bank of Baroda
7	Punjab National Bank
8	Union Bank of India
9	State Bank of India
10	Axis Bank
11	Canara Bank
12	Kotak Mahindra Bank
13	HDFC Bank (additional)

14	ICICI Bank (additional)
15	Bank of India
16	Central Bank of India
17	IDBI Bank Ltd
18	Indian Bank
19	Paytm Payments Bank Ltd
20	Yes Bank Ltd
21	Bank of Maharashtra
22	Federal Bank
23	Indian Overseas Bank
24	IndusInd Bank Ltd
25	RBL Bank Ltd
26	UCO Bank Ltd
27	Karur Vysya Bank
28	City Union Bank
29	Karnataka Bank
30	IDFC First Bank Limited
31	Bandhan Bank
32	Jammu and Kashmir Bank Limited
33	South Indian Bank
34	Tamilnad Mercantile Bank Limited
35	Punjab & Sind Bank