Towards an AI-Powered Cyber Resilience Model: A Systematic Evaluation of Frameworks Against Emerging Threats

Chhaya Jahajeeah-Suntoo, Sheeba Armoogum
Department of Information and Communication Technologies, University of Mauritius, Reduit, Republic of Mauritius

***Abstract*—This study presents a Systematic Literature Review of cyber resilience frameworks against emerging threats, published between 2010 and 2025. While numerous frameworks exist, their ability to anticipate, withstand, and evolve in the face of sophisticated attacks remains uncertain. The study maps frameworks across nine resilience goals, namely Identify, Protect, Detect, Respond, Recover, Govern, Anticipate, Withstand, and Evolve, creating a goal-wise evidence matrix and quantification. Using the PRISMA methodology, 11,027 publications were identified, of which 55 studies met the inclusion criteria for critical analysis. The results indicate that most frameworks accentuate Protect and Detect functions at 87.72 per cent, whereas Govern at 17.54 per cent, Withstand at 28.07 per cent, and Evolve at 24.56 per cent remain under-represented. Only 45.61 per cent of frameworks explicitly address emerging threats such as Artificial Intelligence-driven or Internet of Things-based attacks. Strengths observed include situational awareness, Artificial Intelligence and Machine Learning integration, dynamic defence mechanism, Blockchain, and adoption of Zero Trust principles. The key weaknesses lie in the undervalued cyber resilience goals, namely Govern, Withstand, and Evolve, low empirical validation, and a narrow scope in addressing emerging threats, which highlight gaps that limit resilience against sophisticated attacks. Based on these findings, an evidence-informed Artificial Intelligence-powered cyber resilience model is proposed that privileges adaptability and future proofing. This review highlights the urgent need for cyber resilience frameworks to expand beyond reactive measures and to embed forward-looking resilience capabilities.**

Keywords*—Cyber resilience; cybersecurity framework; Artificial Intelligence; emerging threats; Zero Trust; systematic literature review

I. Introduction

The vision of a secure cyberspace without the least fear of cyber-attacks seems like a distant dream. The reality of the digital sphere is far more complex than can be imagined. While insecurity is inbred in cyberspace; cyber threat is the rule in the premise of cyber resilience [1]. The rise of the internet with high-speed digital communication networks have substantially reduced the limitation of physical distance and time. This has eased the way in which people communicate, work, and experience the world around themselves [2]. However, the development of adequate safeguards has often been left behind in the process of rapid expansion of connectivity, leaving systems vulnerable to cyber-attacks [1].

Cyber threats have become an intrinsic component of modern societies. Academicians, business leaders and practitioners are striving hard to dampen the challenges posed by evolving cyber-attacks. Researchers have diverse opinions on the current state of affairs, but so far have been unable to provide an appropriate solution. Various frameworks have been developed to guide organisations in implementing effective policies, procedures, and processes to protect digital assets and mitigate potential cyber threats. However, research still points out vulnerabilities in the current frameworks as they poorly address unknown and evolving cyber threats.

Although traditional cybersecurity approaches primarily emphasise prevention and incident response, these measures are increasingly insufficient in environments characterised by persistent, adaptive, and intelligent cyber threats. Modern adversaries exploit Artificial Intelligence (AI), automation, and interconnected infrastructures to circumvent static security controls, thus rendering perimeter-based defences inadequate. In this context, the concept of cyber resilience has gained prominence as a complementary paradigm. It emphasises the capacity of systems and organisations to anticipate, withstand, recover from, and adapt to adverse cyber events.

Despite the increasing recognition of cyber resilience, existing frameworks exhibit substantial variation in scope, conceptual foundations, and operational focus. Many of these frameworks prioritise technical controls, often neglecting aspects such as governance, adaptability, and long-term learning capabilities. This fragmentation complicates the process of selecting appropriate frameworks and restricts organisational preparedness against emerging threats. Consequently, a systematic and goal-oriented evaluation of cyber resilience frameworks is necessary. Such an evaluation can identify strengths, weaknesses, and unresolved gaps, thereby informing the development of resilience models that are capable of supporting future organisational needs.

Numerous systematic reviews and surveys have examined cybersecurity frameworks, maturity models, and resilience assessment methods. These studies often focus on compliance, risk management, or applications specific to particular sectors. Earlier research typically analyses resilience qualitatively or concentrate on a limited number of functional aspects, without providing a comprehensive quantitative comparison across different resilience objectives. Moreover, existing reviews rarely evaluate frameworks in the context of emerging threats such as those enabled by AI, autonomous adversaries, or Zero

Trust Architecture (ZTA). They also seldom translate identified gaps into a cohesive framework design.

This study addresses these limitations by making four distinct contributions. Firstly, it provides a goal-oriented, quantitative evaluation of cyber resilience frameworks across nine resilience objectives. This evaluation integrates both the functions outlined in NIST CSF 2.0 and the extended resilience dimensions. Secondly, it offers a longitudinal synthesis of evidence covering frameworks published between 2010 and 2025, thereby facilitating trend-based analysis. Thirdly, it explicitly assesses the extent to which existing frameworks address emerging threats and attack vectors driven by Artificial Intelligence. Fourthly, it highlights gaps in governance, adaptability, and empirical validation. Finally, it translates the identified gaps into an evidence-informed, AI-powered cyber resilience model. This approach effectively bridges findings from systematic reviews with framework design. To the authors' knowledge, no previous research has combined these elements within a single, structured analysis.

In light of the above, the objective of this review is to systematically assess CRFs to determine their alignment with resilience goals and their capacity to address emerging threats. Four research questions (RQs) guided this study:

- RQ1: Which goals are most commonly pursued in CRFs?
- RQ2: Do current CRFs address emerging cyber threats?
- RQ3: What are the strengths and weaknesses inherent in CRFs?
- RQ4: Which gaps can inform the design of future CRFs?

The remaining part of this study is organised into six sections: Section II provides a conceptual overview of CRFs, Section III presents the method used, Section IV highlights the main findings, Section V offers the final discussion, Section VI introduces the proposed conceptual model, and Section VII closes the study with recommendations for further research.

II. Conceptual Overview

This section outlines the conceptual foundation of cyber resilience frameworks. The nine goals, inclusive of NIST CSF 2.0 functions and cyber resilience goals (Identify, Protect, Detect, Respond, Recover, Govern, Anticipate, Withstand, Evolve), provide the analytical baseline for this review. Additionally, Zero Trust (ZT) and Artificial Intelligence /Machine Learning (AI/ML) are introduced as emerging enablers of resilience that influence the design of contemporary frameworks.

A. Emerging Cyber Threats

Cybercriminals act with malevolent intent to disrupt services and compromise critical data, resulting in financial losses [3]. As cyber-attacks evolve, they also contribute to broader economic impacts [4]. Furthermore, these attacks pose a range of operational and organisational risks [5]. Attackers even adapt their attack strategies to elude traditional defences [6]. Several authors review emerging cyber threats, including Advanced Persistent Threats [7], cybersecurity challenges such as phishing and social engineering exploits [8], and modern threats and defence strategies addressing operational risks from malware, data breaches, and network intrusions [9]. In addition, AI-powered attacks and cryptocurrency-based cybercrimes demonstrate the growing technological intricacies of contemporary cyber threats [10]. Other threats exploit vulnerabilities in new technologies like fifth-generation (5G) networks, Artificial Intelligence (AI), Internet of Things (IoT), and cloud computing [11]. Recent research shows a growing trend in cyber threats that evolve in quantity and complexity, with attackers using advanced techniques to exploit vulnerabilities in digital infrastructure [12]. The threats are mostly characterised by their dynamic and volatile nature, which emphasises the need for continually adapting and enhancing countermeasures [9, 13]. Although safeguards such as antivirus software, firewalls, and encryption are alleviating, they have limitations [14]. The adoption of cyber resilience capabilities in security mechanisms can bring proactiveness and a reliable solution [15]. In conjunction with the accelerating growth of unpredictable cyber threats, there must be a shift from merely defending against such attacks. There is a need to cultivate resilience through a system's capability to absorb the impact of attacks, regain functionality, and adjust effectively in response to cyber incidents. This accentuates the importance of cyber resilience, which, on top of preventing breaches, also minimises disruptions and promotes rapid recovery.

B. Resilience to Cyber Threats

Cyber resilience has stimulated scholarly interest since the 2000s, alongside the growing maturity in cyber threats. It complements the traditional security approach to protect digital assets and systems. It is vital to highlight the distinction between cybersecurity and cyber resilience for a deeper understanding of the latter. Cybersecurity is defined as "the organisation and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" [16]. In simple terms, it is the operationalization of policies, procedures, and technical measures aimed at securing information and communication systems. Cybersecurity solutions alone cannot cope with the increasing impact of cyber-attacks on organisations. However, the relationship between cybersecurity and cyber resilience remains ambiguous, with some arguing that both goals should be pursued simultaneously rather than prioritising one over the other [1]. Cyber resilience distinguishes itself on the basis of its readiness to pull through cyberattacks, be adaptable, and learn from adversity [17]. It is about going beyond the traditional cybersecurity measure. Cyber resilience requires a mindset shift from reactiveness to proactiveness against known to unknown cyber incidents. Its aim is to incessantly deliver the expected outcome despite adverse conditions [18]. Traditional cybersecurity approaches are reactive and mostly founded on a perimeter-based model for securing organisations. They address certain and known cyber events and adopt a fail-safe strategy. However, cyber resilience acknowledges the inevitability of risks and promotes the strategy of safe to fail, where every system can fail in a controlled way with the ability to recover [18]. Hence, there is a pressing need to either supplement cybersecurity with cyber resilience or simply transcend cybersecurity while moving towards cyber resilience. Today, a number of frameworks are considering cyber resilience and entailing proactive measures to

prevent emerging cyber threats. Therefore, it is important to define cyber resilience.

The literature review shows that there are many definitions of cyber resilience. Researchers have yet to gain unanimity in accepting a unique scientific definition for it [19]. The lack of a universally agreed-upon definition is not only an academic concern but has real-world consequences. This has an impact on the design of CRFs and affects their practical applicability in organisations. Each definition influences the way an organisation or system conceptualise and implement resilience strategies. The different definitions emphasise resilience goals or characteristics in varying ways, depending on what needs to be resilient [20]. For instance, the focus might be on systems, organisations, or threat models. Consequently, five definitions of cyber resilience have been selected that can provide the material perspectives of cyber resilience. Since very often the essence of cyber resilience is misunderstood, Table I below summarises the main definitions.

TABLE I. OVERVIEW OF SELECTED DEFINITIONS

Definition of Cyber Resilience	Key Goals
"The ability to anticipate, withstand, recover from, and evolve to adverse conditions, stresses, attacks, or compromises on systems" [21,22]	Anticipate, Withstand, Recover, Evolve/Adapt
"The ability to prepare for, absorb, recover from, and adapt to adverse events in cyber systems" [23].	Prepare, Absorb, Recover, Adapt
"The ability to continuously deliver the intended outcome despite adverse cyber events" [18].	Business continuity during cyber disruption
"The capacity to withstand, recover from, and adapt to the external shocks caused by cyber risks" [24].	Withstand, Recover, Adapt
"The ability of systems to resist and recover from, or adapt to, a cyber compromise" [25].	Withstand, Recover, Adapt

It is observed from Table I above that the definitions of cyber resilience are mainly goal-oriented. The first definition has been used to ease discussion, and the goals are defined below:

- Anticipate (AP): to maintain an informed state of readiness against potential compromises arising from attacks by antagonists.
- Withstand (WT): to uphold critical operational continuity in spite of the successful occurrence of an attack by an antagonist.
- Recovery (RC): to recover operations in the aftermath of an attack by an antagonist.
- Evolve (EV): to adapt to anticipated changes in the operational, technical, or threat environments.

This definition offers a complementary approach to conventional measures undertaken in cybersecurity. Understanding and using this definition as a foundation to implement cyber resilience is not enough. Organisations need to be guided by CRFs to implement cyber resilience strategies. A well-defined one provides the methodologies and best practices to achieve cyber resilience goals. However, as evidenced by the literature, there is a dearth of studies that focus on CRF against emerging threats of unknown and evolving nature. This inquiry attempts to address this gap by examining the extent to which the current frameworks ensure resilience.

C. Cyber Resilience Frameworks (CRFs)

A CRF is a structured method for managing and responding to threats and incidents in cyberspace. It aids in minimising the disruption caused by such occurrences in an organisation. It is designed in a way to assist organisations anticipate, withstand, and recover from cyber threats [26]. Such a framework typically includes a set of policies, procedures, and technologies that work together to ensure that an organisational entity can survive and recover from attacks. An organisation can improve its capacity to sustain critical functions and swiftly rebound from the disruption of service by adopting a proper CRF [26]. CRFs are evolving and moving from prevention to detection, response, and recovery so as to confront the adaptive and shifting characteristics and challenges of cyber threats [27]. In general, the framework is structured to strengthen an organisation's proficiency in detecting, managing and bouncing back from cyber incidents. This further promotes risk mitigation strategies in the organisation. Recently, emphasis has been laid on situational awareness for effective crisis management and cybersecurity resilience [28].

D. Commonly Established Frameworks

Several well-established frameworks, including NIST, ENISA, ISO 27001, and ISO/IEC 27032, provide guidance for organisations seeking to strengthen their safeguards against cyber threats. Their contributions in enhancing business continuity and cyber resilience have been recognised [29]. The comparative analyses of NIST and ISO27001 offer practical guidance for minimising exposure to cybersecurity risk by selecting appropriate frameworks for organisations [30]. Reviews of framework methodologies and implementation challenges further support effective adoption and application into organisational cybersecurity strategies [31].

In particular, the NIST CSF 2.0 is an updated voluntary guideline to assist all types of organisations to manage and mitigate cybersecurity risks. The way organisations implement it will depend on their risk tolerances, missions, and objectives. It builds on the previous version's functions, highlighting the importance of governance and supply chains. Its core abilities are to:

- Govern the organisation's cybersecurity risk management strategy;
- Identify current cyber risks, to protect against those risks by using safeguards;
- Detect possible attacks and compromises, to respond to detected incidents; and
- Recover affected operations and assets from incidents.

HIPAA, CIS Controls, COBIT, PCI DSS, and CMMC are also prominent frameworks that organisations use to improve their security posture. The role of HIPAA is in securing patient health information and healthcare provider responsibilities [32], while comparative analyses of frameworks such as CIS Controls and COBIT provide guidance for selecting appropriate standards [33]. The PCI DSS framework is used in the context of payment card industry security requirements [34], and CMMC for supply chain management [35]. Additionally, GDPR and HIPAA compliance in IoT healthcare systems shows the importance of regulatory adherence in the digital environment [36]. Since these frameworks have distinct features and operational differences, organisations often align multiple frameworks to meet their needs. Nowadays, some frameworks are leveraging on Zero Trust Architecture to strengthen cyber resilience.

E. Zero Trust Security Frameworks

The Zero Trust (ZT) concept was initially meant to deal with insider threats within organisations. The ZT security model is defined as a network defence strategy that presumes that an adversary has penetrated inside the hardened perimeter of an organisation [37]. Enterprises like Google, Microsoft, and Gartner have implemented this framework after having understood that safeguarding only their network perimeters is fruitless [38]. ZT is an emerging paradigm supporting cyber resilience. Its strategic approach is to "Never trust, always verify". Users, devices, or transactions are not granted trust by default. Currently, there is a scarcity of research in this area [39]. In brief, ZT uses the de-perimeterisation concept. It departs from a perimeter-based security model to a perimeter-less one, where users and devices should not assume trustworthiness by default [37]. It aligns with the principles of cyber resilience as it focuses on measures on how to safeguard sensitive data [40]. This alignment is crucial as data breaches have alarming consequences. ZT should not be considered as a security model only, but a new way of thinking that should be indoctrinated in all security frameworks. Another important aspect is the incorporation of Artificial Intelligence in frameworks.

F. Contribution of Artificial Intelligence (AI) in CRF

Today, Artificial Intelligence is becoming an integral part of technology. However, AI-driven solutions in cybersecurity are used in paradoxical situations. It can either be used as an intelligent defence mechanism or a weapon, such as Advanced Persistent Threats [41]. AI is a powerful tool to rapidly analyse large datasets, detect patterns of a potential threat that may be partially hidden [42]. Cyber defence systems without AI are insufficient to fight against AI-driven cyberattacks, which applies fast decision logics. Furthermore, AI integration in cyber defence for automating threat detection, incident response, and threat analysis can reorient cybersecurity from responding to anticipating threats [42]. The use of AI in CRF is to ensure the system's protection and address the challenges associated with advanced cyber-attacks, including AI-powered attacks [41]. It aids in staying ahead of shape-shifting threats as it facilitates the development of adaptive defence tactics to counter emergent threats. AI is the game-changer in cyber resilience and the development of new frameworks.

As evidenced by various studies, research in the ambit of cyber resilience is gradually progressing. However, although many CRFs have been proposed since the year 2000, they have limitations. There is still a need for increased clarity on their scope, characteristics, and synergies [43]. In order to realise this outcome, a methodical approach is required. The subsequent section discusses the methodology applied to gather the information and analyse the frameworks.

III. METHODS

This section outlines the procedure used to conduct a systematic literature review on CRFs by focusing on their goals, strengths, and weaknesses. The concepts of repeatability [44, 45], along with the PRISMA framework for systematic reviews and meta-analyses [46], were applied. This approach was selected to enhance the review process, making it more transparent, rigorous, and reproducible. Since systematic review can be prone to selection bias by unintentionally favouring certain studies, this methodology helped in reducing that risk. The PRISMA checklist in conjunction with the flow diagram supported the systematic organisation and presentation of the findings, to reflect recent advances in systematic review methodology and terminology. This framework also substantiates the rationale behind the methodological decisions on search strategy, data sources, eligibility criteria, study selection and examination procedures. PRISMA is also a robust protocol commonly used in cybersecurity research [47, 48].

A. Eligibility Criteria

The eligibility criteria were established to confirm the relevance and rigor of the evaluation. Studies were included if they:

- Proposed or evaluated a CRF between 2010 and 2025;
- Addressed resilience goals or emerging threats, and
- Were published in peer-reviewed venues. Non-English, non-peer-reviewed, and duplicate studies were excluded.

B. Databases and Search Strategy

Primary studies were systematically identified and pulled out using carefully selected keywords across multiple databases. IEEE Xplore, ScienceDirect, Scopus, Emerald Insight, and Google Scholar were searched using Boolean query: (“cyber resilience framework” OR “CRF”) AND (“emerging threats” OR “AI” OR “Zero Trust”).

C. Screening and Selection

As illustrated in Fig. 1, a total of 11,027 records were retrieved. After duplicate removal and two-stage screening, 55 studies were included. Fig. 2 illustrates the annual number of research publications in CRFs from 2010 to 2025. It shows that publications in cyber resilience were unstable in the early years, while recently it has been trending upwards. The highest number of publications was recorded in the year 2025.

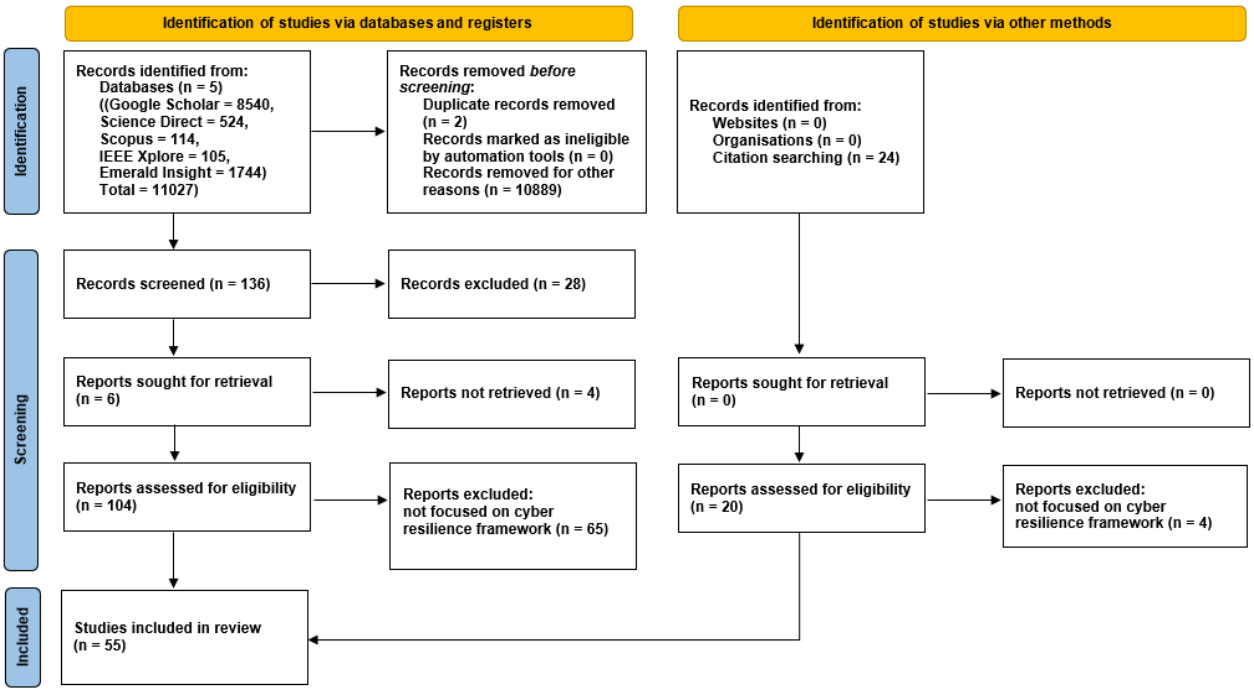

Fig. 1. PRISMA 2020 flow diagram for systematic review.

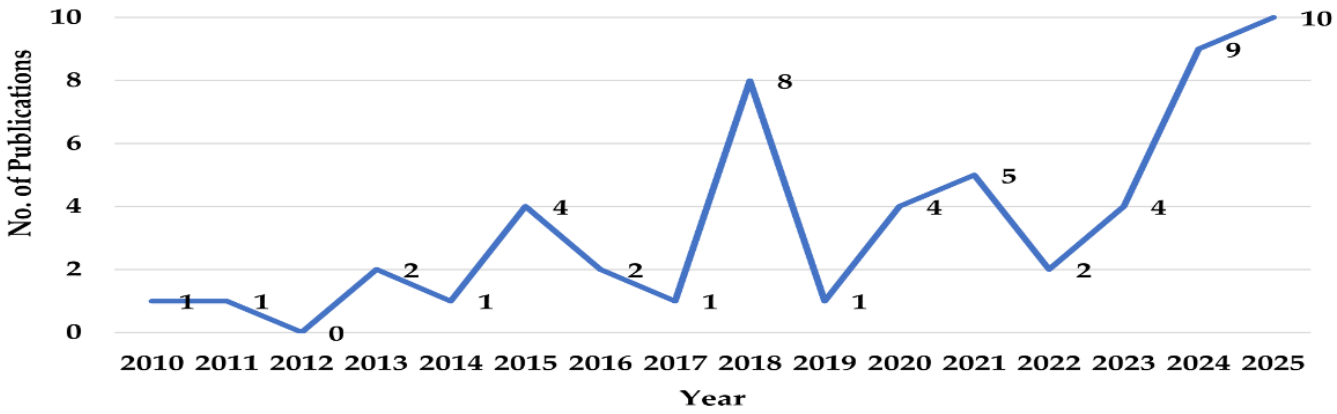

Fig. 2. Annual number of research publications in cyber resilience framework from 2010 to 2025.

TABLE II. PICO FRAMEWORKS

Element	Definition	Application in this Review
Population	Cyber resilience frameworks	All CRFs published 2010–2025
Intervention	Features/ capabilities	AI/ML integration, Situational Awareness, Zero Trust, Blockchain, dynamic defence mechanisms, Comprehensive scope
Comparator	Established frameworks/goals	9 goals of (NIST CSF 2.0 functions + cyber resilience goals)
Outcome	Evaluation metrics	Goal coverage %, strengths/ weaknesses, emerging threat coverage

Table II outlines the PICO framework applied in this study, specifying the population, intervention, comparison, and outcomes that guided the research design.

D. Data Extraction and Synthesis

Data was extracted using a coding sheet capturing year, framework, domain, goals addressed, emerging threats, and validation status. In synthesis, Table III and Table IV, the presence of a feature or goal was indicated with a tick symbol (√), while absence was left blank. Percentages were calculated to quantify coverage, as shown in Tables V and VI. Thematic synthesis was then applied to interpret patterns, supported by visualisations (radar/pie charts). Based on the structured extraction and synthesis, the following section summarises the main outcomes:

TABLE III. CYBER RESILIENCE FRAMEWORKS FROM 2010 TO 2025

Citation	Publication Year.	Cyber Resilience Framework (CRF)	Goals									Comprehensive scope	Situational Awareness	AI/ML Integration	Dynamic Defence	Caters for emerging threats	Lacks Empirical Validation
			Identify	Protect	Detect	Respond	Recover	Govern	Anticipate	Withstand	Evolve						
[49]	2010	"CERT Resilience Management Model"	√	√	√	√	√	√				√					
[20]	2011	"Cyber Resiliency Engineering framework"		√	√	√	√		√	√	√	√			√	√	
[23]	2013	"Resilience matrix framework"					√		√	√	√						
[50]	2013	"Offensive Cyber Counterintelligence (CCI) framework"	√	√	√	√			√				√			√	
[51]	2014	"Cyber Resiliency Engineering framework"	√	√	√	√	√		√	√		√			√	√	
[52]	2015	"Proactive crisis management"	√	√	√	√	√		√			√			√		√
[53]	2015	"Updated Cyber Resiliency Engineering Framework (CR Eng. Aid)"	√	√	√	√	√		√	√	√	√			√	√	
[54]	2015	"Cyber Resilience Engineering Framework (CREF)"		√	√	√											
[55]	2015	"Cyber Resiliency Framework"	√	√	√	√	√		√				√			√	
[56]	2016	"ISP 10x10M Framework"		√	√	√	√										
[57]	2016	"Resilience Metric Framework"					√			√							
[58]	2017	"SDN-based security risk assessment"	√	√	√	√											√
[59]	2018	"Process Reference Model (PRM)"	√	√	√	√	√	√									
[60]	2018	"Universal System Model"		√		√	√										
[61]	2018	"Siemens Cybersecurity Model"			√				√			√					
[61]	2018	"Frost & Sullivan's Security Maturity Model"		√	√	√	√		√	√	√	√					
[62]	2018	"Cyber resilience Assessment model (industrial Control Systems)"	√	√	√	√	√		√			√					
[63]	2018	"Start Secure, Stay Secure, & Return Secure"	√	√	√	√	√		√	√	√	√			√	√	
[64]	2018	"Wicked Problem Conceptual framework"	√	√	√	√	√										
[65]	2018	"Proactive Resilience Educational Framework (Prosilience EF)"	√	√	√	√	√				√						
[66]	2019	"Novel cyber resilience framework"			√	√			√								
[67]	2020	"Holistic Cybersecurity Maturity Assessment Framework (HCYMAF)"	√	√	√	√	√										
[68]	2020	"Managerial CRF"		√	√	√	√			√	√						
[69]	2020	"CRF for SMEs"	√	√	√	√	√	√									
[70]	2020	"IWA framework"		√	√								√			√	√
[29]	2021	"New Cyber Resilience framework"	√	√	√	√	√							√		√	
[71]	2021	"CR-SAT cyber resilience framework"	√	√	√	√	√	√									
[72]	2021	"New AI-led framework"	√	√	√	√	√		√	√	√		√	√		√	
[73]	2021	"MTD Strategy Design Framework"		√	√								√			√	
[74]	2021	"SME Cyber Situational Awareness model"		√									√				
[75]	2022	"Cybersecurity Service System Model"	√	√	√	√	√									√	
[76]	2022	"Network Defense Training Game (NDTG) framework"	√	√	√	√	√										

TABLE IV. CYBER RESILIENCE FRAMEWORKS FROM 2023 TO 2025

Citation	Publication Year.	Cyber Resilience Framework (CRF)	Goals									Comprehensive scope	Situational Awareness	AI/ML Integration	Dynamic Defence	Caters for emerging threats	Zero Trust	Blockchain	Lacks Empirical Validation
			Identify	Protect	Detect	Respond	Recover	Govern	Anticipate	Withstand	Evolve								
[77]	2023	"Smart Cities Cybersecure framework - Blockchain-based architecture"		√	√	√			√	√			√	√	√	√		√	
[28]	2023	"PHOENI2X CRF AI-assisted orchestration, automation & response"	√	√	√	√	√		√	√			√	√		√			
[78]	2023	"NIST organization's cybersecurity maturity"	√	√	√	√	√						√						
[41]	2023	"AI4CYBER framework"	√	√	√	√	√		√	√	√	√	√	√	√	√			
[79]	2024	"New Cyber resilience metric including Zero Trust & MITRE ATT&CK)"		√	√	√	√					√	√	√	√	√	√		
[27]	2024	"Next-Generation CRF"	√	√	√	√					√			√	√	√			
[26]	2024	"New Cyber Resilience Framework"	√	√	√	√	√	√				√				√			
[80]	2024	"NIST CSF v2.0 aligned with maritime challenges"	√	√	√	√	√	√	√										
[81]	2024	"Framework for Cyber Security & vulnerability management"	√	√	√	√			√					√		√			
[82]	2024	"Agile Cybersecurity Framework"		√	√	√	√	√											
[83]	2024	"Supply Chain CR (SCCR)"		√	√	√			√										
[84]	2024	"Novel ML-based HCT modeling & analysis framework"		√	√	√			√			√	√	√		√			
[85]	2024	"New three-layer architecture - Cyber-biosecurity"		√	√	√			√				√						
[86]	2025	"Fraud detection & data protection cybersecurity framework-financials"	√	√	√	√			√		√			√		√			
[87]	2025	"Multi-layered AI-enhanced cyber resilience framework to safeguard smart city infrastructures"	√	√	√		√		√	√	√			√	√	√	√	√	
[88]	2025	"KPI-Based Evaluation CRF - Ships"	√	√	√	√	√	√	√	√	√								√
[89]	2025	"A Conceptual framework for SME"	√											√					
[90]	2025	"AI-Powered Cybersecurity Framework for Remote Work"	√	√	√	√								√		√			
[91]	2025	"NIST CSF aligned with Evaluation Framework for Cybersecurity Maturity"	√	√	√	√	√	√											
[92]	2025	"Optimal cybersecurity framework - Smart Water System Detection"	√	√	√									√		√			
[93]	2025	"Cybersecurity Framework for Protecting Critical Infrastructure in Organization"	√	√	√	√	√	√		√				√		√	√	√	
[94]	2025	"Cognitive Zero-Trust Resilience Framework (CZTRF)"	√	√	√	√	√		√	√	√	√		√		√	√		
[95]	2025	"CR-V2XR, cross-layer, federated, & trust-aware coordinated framework"	√	√	√				√					√		√			

TABLE V. SUMMARY OF CRFS STRENGTHS AND WEAKNESSES

Years	CRFs from 2010 to 2025							
	Strengths							Weakness
	Comprehensive Scope	Situational Awareness	AI/ML Integration	Dynamic Defence Mechanism	Caters for emerging threats	Zero Trust	Blockchain	Lacks Empirical Validation
Total No. of CRF	14	13	17	10	26	4	3	4
Percentage of CRF	24.56	22.81	29.82	17.54	45.61	7.02	5.26	7.02

TABLE VI. SUMMARY OF GOAL-WISE CRFS FROM 2010 TO 2025

Goals	Identify	Protect	Detect	Respond	Recover	Govern	Anticipate	Withstand	Evolve
Total No. of CRF	36	50	50	45	36	10	26	16	14
Percentage of CRF	63.16	87.72	87.72	78.95	63.16	17.54	45.61	28.07	24.56

IV. RESULTS

The review syntheses the result of 55 studies, as presented in Table III, Table IV, Table V, and Table VI, with respect to the Research Questions that guided this study. The findings uncovered notable trends and important insights on the prevailing research trends in CRFs. The main results are as follows:

- RQ1 (Goals pursued): Most CRFs emphasise Protect (87.72%) and Detect (87.72%), with limited focus on Govern (17.54%), Withstand (28.07%), and Evolve (24.56%).
- RQ2 (Emerging threats): Only 45.61% of CRFs explicitly address emerging threats such as AI-driven or IoT-based attacks.
- RQ3 (Strengths & weaknesses): Strengths include AI/ML integration (29.82%), comprehensive scope (24.56%), Situational Awareness (22.81%), Dynamic Defence mechanism (17.54%), Zero Trust (7.02%) and Blockchain (5.26%). Weakness includes lack of empirical validation (7.02%).
- RQ4 (Gaps): Under-represented goals (Govern, Withstand, Evolve) and low empirical validation highlight gaps that limit resilience against sophisticated threats.

The radar chart in Fig. 3 is based on the summarised CRFs' goals calculated from Table VI. This chart has been used to visualise the multivariate goals in a way that highlights comparisons across the CRFs. The general trend shows that there are significant variations across the different categories with peaks in areas like Protect, Detect, and Respond while sharp declines in Govern, Withstand and Evolve. There is an overall asymmetrical distribution, indicating that some CRFs have focused more on certain specific goals (Protect, Detect, Respond, Identify, Recover) than others.

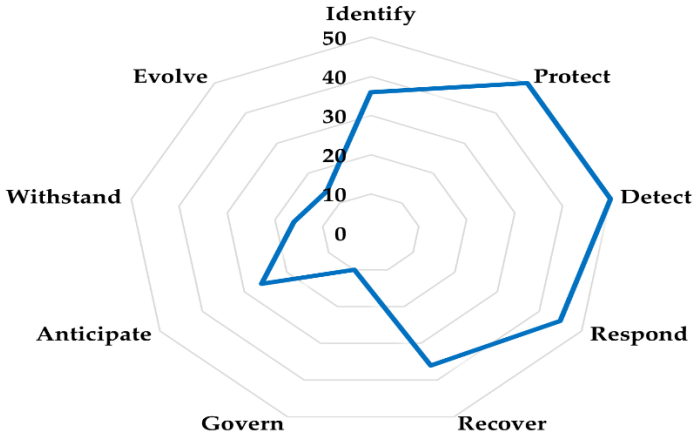

Fig. 3. Radar chart showing goal-wise total of CRFs (2010 to 2025).

The pie chart, in Fig. 4, illustrates the same results from Table VI, in the form of percentages. The majority of frameworks focus on cybersecurity capabilities, namely, "Protect" (87.72%), "Detect" (87.72%), "Respond" (78.95%), "Identify" (63.16%), and "Recover" (63.16%). The "Govern" function (17.54%) has been overlooked. This is perhaps because it focuses on organisational cybersecurity rather than technical implementation, which is often the primary concern of security teams. Some attention has been dedicated to "Anticipate" (45.61%) capabilities. However, not much consideration has been devoted to "Withstand" (28.07%) and "Evolve" (24.56%) goals.

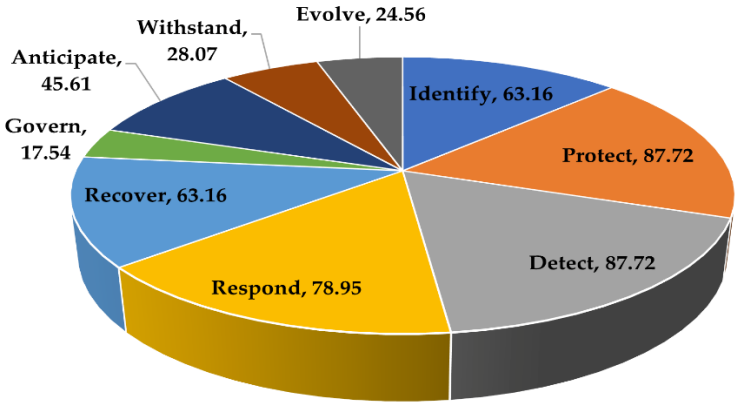

Fig. 4. Pie chart showing goal-wise percentage of CRFs (2010 to 2025).

A noteworthy observation from this review is that the CRFs are still heavily dependent on reactive measures. They fail to fully embrace the proactive and adaptive principles of cyber resilience in terms of withstanding and evolving to ever-changing cyber threats. The exposed gap has several implications for organisations or systems adopting frameworks without resilience capabilities. Should a threat arise, for instance, an AI-based cyber-attack, the organisations might face the following challenges:

- Adaptation failure to emerging threats and become an easy target to cyber incidents;
- Safe-to-fail strategy of cyber resilience will be jeopardised, as systems will not be able to fail in a controlled manner;
- Recovery time delay and lengthening of operational downtime;
- Major financial/reputational loss or legal implication issues; and
- Business closure.

In view of addressing this major gap, there is a necessity to develop a comprehensive framework. This framework should integrate resilience capabilities to adverse conditions with special focus on govern, withstand, and evolve goals. Consequently, a structured visual representation of a model can provide a systematic approach to designing such a framework. The following sections discuss the results and present a proposed conceptual cyber resilience model.

V. Discussion

This review reveals that CRFs prioritise reactive capabilities (Protect, Detect, Respond), while governance and adaptive goals (Withstand, Evolve) remain neglected. The overemphasis on technical safeguards reflects a short-term posture, leaving organisations under-prepared for evolving threats.

Comparisons with previous surveys show that while situational awareness and AI/ML integration are increasing, empirical testing of frameworks is rare, raising concerns over practical deployment.

- Implications for Practice: Policymakers should encourage frameworks to institutionalise governance and adaptive mechanisms. Practitioners should prioritise frameworks with empirical validation before adoption.
- Limitations: This review only included English language sources and excluded grey literature. Binary coding (ticks) may oversimplify framework capabilities.
- Future Research: There is a need for measurable resilience indicators for Withstand/Evolve, digital twin validation of CRFs, and AI-driven resilience metrics.

VI. Proposed Framework

The proposed AI-powered CRF directly addresses the identified gaps. Specifically, it enhances the neglected "Govern", "Withstand", and "Evolve" goals, integrates Zero Trust and situational awareness, and introduces AI/ML for adaptive defence. This ensures continuity between the evidence synthesis and framework design.

The framework focuses on the ability to offer real-time protection, recovery, and operational continuity based on the four dimensions of cyber resilience, i.e., competence in predicting threats, resisting shocks, recuperating from, and evolving from adverse conditions. Fig. 5 illustrates the model, which integrates multiple layers of defence with situational awareness and Zero Trust Architecture to create a complete, adaptive, scalable, cyber resilient, and dynamic defence mechanism to counteract cyber threats.

This model has three layers with a core, whereby each layer is finely coupled and supports one another. It ensures a structured and adaptive cyber resilience coverage. It incorporates the protection of data in terms of confidentiality, integrity, and availability throughout its lifecycle.

The top layer, Situational Awareness, emphasises continuous monitoring and vigilance to stay aware of potential threats. This layer consists of Risk Assessment, AI-driven Threat Intelligence with continuous monitoring, and Decision Support.

Fig. 5. AI-powered cyber resilience model (Source: authors' creation).

The second layer is the Zero Trust Architecture (ZTA). It helps eliminate implicit trust and promotes continuous authentication and authorisation of users, devices, and network traffic to access network resources. Furthermore, it uses the principle of least privilege access, micro-segmentation, dynamic security policies, and encryption. Implementing ZTA enhances the cybersecurity posture of an organisation by reducing the attack surface and preventing lateral movement across networks.

The third layer of the model consists of the four pillars of cyber resilience functions, ensuring resilience spanning the pre-incident, during the incident, and post-incident stages of a cyber-attack. Their functions are:

- To anticipate with proactive threat hunting capabilities. AI-driven threat intelligence with Artificial Intelligence algorithms for anomaly and threat detection, and real-time monitoring of cyber threats with early warning. In this phase, prioritisation of assets is important, suggesting a prioritised approach to asset security;
- To withstand with dynamic defence, deceptive mechanisms to mislead attackers, air-gapped protection as a fail-safe, data immutability, as well as Zero Trust mechanisms;
- To recover with automated response, swift recovery, self-healing capabilities, redundancy, failover Systems, minimum downtime, and business impact; and
- To evolve with a feedback mechanism, learning, acknowledging policies and cyber laws with compliance to regulations, adaptation, and a continuous improvement process.

The core of the model consists of governance and humans as key factors. On one hand, good governance in line with organisational goals and policies guides security decisions, on the other, humans through their cybersecure awareness and skills bring these policies to life. Together, they create a resilient cyber resilience-aware culture where leadership, policy, and vigilance jointly safeguard the organisation.

A. Technical Specificity of the AI Model

The AI-powered components of the proposed framework support specific goals related to cyber resilience. Machine learning-based anomaly detection models analyse network traffic and system logs in order to enhance the anticipation of emerging threats. Automated response mechanisms, which are integrated with security orchestration platforms, facilitate rapid containment and recovery following security incidents. Reinforcement learning techniques enable continuous adaptation by updating defensive policies based on observed attack patterns and response outcomes. Collectively, these AI mechanisms operationalize the goals of anticipation, withstanding, recovering, and evolving capabilities. Thus, they strengthen resilience against adaptive adversaries.

B. Framework Validation and Evaluation Strategy

Although the proposed AI-powered cyber resilience framework is conceptual in nature, its effectiveness can be systematically evaluated using established validation methodologies. Scenario-based simulations may be employed to assess the framework's behaviour under representative attack conditions. These conditions include AI-driven phishing, ransomware propagation, and IoT-based intrusions. Digital twin or cyber-range environments can further support controlled experimentation. Such environments enable the measurement of recovery time, operational continuity, and the effectiveness of adaptive responses.

Furthermore, key performance indicators such as mean time to detect, mean time to recover, resilience maturity progression, and governance effectiveness may be employed to quantify outcomes of the framework. These validation strategies establish a robust foundation for future empirical testing. They also ensure that the proposed framework is grounded in practical feasibility rather than in purely theoretical abstraction.

VII. Conclusion

Improper implementation of cyber resilience leaves organisations susceptible to cyber-attacks. Although a number of CRFs have been conceived to date, they still have some shortcomings. Most of the frameworks are still using traditional cybersecurity approaches with reactive strategies and insufficient focus on cyber resilience. They are unable to deal with unknown and evolving cyber threats, requiring a comprehensive coverage of technologies like AI/ML, ZTA, blockchain, IoT, and automation. Consequently, the limitations in the frameworks lie mostly in their adaptability to handle

evolving threats, and cyber resilience does make a difference. Although cyber resilience is not a panacea, it does provide a distinctive strength through proactive security management. The conceptual model proposed in this research is a stride towards this aim, harnessing the speed and accuracy of Artificial Intelligence and the "Never Trust Always Verify" paradigm to advance Cybersecurity.

The proposed framework is applicable to a broad range of organisational contexts, including small and medium-sized enterprises, critical infrastructure operators, and public sector organisations. By integrating governance, adaptive learning, and emerging-threat awareness, the framework supports informed decision-making concerning cybersecurity investment, policy formulation, and resilience planning. Consequently, it offers both a theoretical contribution to cyber resilience research and practical guidance for organisations operating within increasingly dynamic cyber risk environments.

Although this study advances scholarly understanding in cyber resilience, it is not free from limitations. The authors recognise that there might be some potential biases or subjectivities introduced by their own perspectives in evaluating the CRFs. Furthermore, the authors acknowledge that the issue of the AI aspect would be in the training of the AI model, which requires large and accurate datasets, which are often limited. Instead, AI-generated synthetic cybersecurity datasets that maintain realistic attack patterns and vulnerabilities can be used. In addition, adversarial AI-training can be utilised to improve the model's resilience against emerging threats. There is also a need to build a prototype CRF from this model and assess its practical feasibility in organisations within risk management practices. It is also critical to evaluate the CRF to ensure its effectiveness against evolving threats.

Some potential improvements for future research are to explore the possibility of using an AI-driven security framework evaluation, using machine learning techniques to assess the framework's efficiency and predictive accuracy. Also, the use of cybersecurity digital twins to empirically test the CRF through real case studies or simulations could be envisaged. Another option could be the use of AI-Augmented Penetration Testing tools to evaluate CRF dynamically against new and evolving threats. Lastly, a promising avenue for future research is on self-healing systems within a framework, which is critical to enhance resilience. These techniques and research areas will address the current limitations and applicability of CRFs.

Some practical implications of the proposed model in real-world scenarios would be proactive threat detection before they cause damage, as the AI capability in the model would identify patterns and anomalies in network traffic and user behaviours. Enhanced response to cyber incidents in real-time by isolating compromised systems and mitigating attacks without human intervention. Overall, its benefit would be to strengthen cybersecurity posture, reduce system downtime, sustain business continuity, and protect sensitive data from cyber incidents.

In conclusion, while CRFs have advanced in integrating AI and Zero Trust, their limited attention to governance and adaptive resilience weakens their effectiveness. Addressing these gaps is crucial for organisations facing dynamic cyber threats. The proposed framework provides a blueprint for strengthening future CRFs through adaptability, validation, and evidence-based design.

REFERENCES

[1] L. A. Bygrave, 'Cyber Resilience versus Cybersecurity as Legal Aspiration', in 2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon), Tallinn, Estonia: IEEE, May 2022, pp. 27–43. doi: 10.23919/CyCon55549.2022.9811084.

[2] D. Stokols and M. Montero, 'Towards an Environmental Psychology of the Internet', in Handbook of Environmental Psychology (661-675) New York: John Wiley & Sons, R. Bechtel&A. Churchman (Eds)., vol. Chapter 41, 2002.

[3] D. Kaushik, 'The Impacts of Cybersecurity and AI on Businesses and Individuals', J Stud Res, vol. 12, no. 4, Nov. 2023, doi: 10.47611/jsr.v12i4.2282.

[4] P. Kelley, 'Evolution of Cyber Attacks and Their Economic Impact', Dec. 11, 2022. doi: 10.36227/techrxiv.21670718.v1.

[5] S. Vaddadi, R. Vallabhaneni, and A. Maroju, 'A Comprehensive Review Study of Cyber-Attacks and Cyber Security', IJRITCC, vol. 11, no. 9s, pp. 844–848, Aug. 2023, doi: 10.17762/ijritcc.v11i9s.9492.

[6] R. Montasari, A. Hosseinian-Far, and R. Hill, 'Policies, Innovative Self-Adaptive Techniques and Understanding Psychology of Cybersecurity to Counter Adversarial Attacks in Network and Cyber Environments', in Cyber Criminology, H. Jahankhani, Ed., in Advanced Sciences and Technologies for Security Applications. , Cham: Springer International Publishing, 2018, pp. 71–93. doi: 10.1007/978-3-319-97181-0_4.

[7] M. Siddiqi and N. Ghani, 'Critical Analysis on Advanced Persistent Threats', IJCA, vol. 141, no. 13, pp. 46–50, May 2016, doi: 10.5120/ijca2016909784.

[8] C. V. S. Babu, P. Andrew Simon, and S. Barath Kumar, 'The Future of Cyber Security Starts Today, Not Tomorrow':, in Advances in Information Security, Privacy, and Ethics, S. L. Shiva Darshan, M. V. Manoj Kumar, B. S. Prashanth, and Y. Vishnu Srinivasa Murthy, Eds, IGI Global, 2023, pp. 348–375. doi: 10.4018/978-1-6684-8666-5.ch016.

[9] O. C. Obi, S. O. Dawodu, A. C. Anyanwu, S. Onwusinkwue, and I. A. I. Ahmad, 'COMPREHENSIVE REVIEW ON CYBERSECURITY: MODERN THREATS AND ADVANCED DEFENSE STRATEGIES', Comput. sci. IT res. j., vol. 5, no. 2, pp. 293–310, Feb. 2024, doi: 10.51594/csitrj.v5i2.758.

[10] M. Alanezi and R. M. A. AL-Azzawi, 'AI-Powered Cyber Threats: A Systematic Review', Mesopotamian Journal of CyberSecurity, vol. 4, no. 3, pp. 166–188, Dec. 2024, doi: 10.58496/MJCS/2024/021.

[11] T. H. Woldemichael, 'Emerging Cyber Security Threats in Organization', IJICS, vol. 5, no. 2, p. 19, 2020, doi: 10.11648/j.ijics.20200502.12.

[12] O. M. Ijiga, P. I. Idoko, T. I. Olatunde, I. E. Godslove, T. I. Olatunde, and C. Ukaegbu, 'Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention', Open Access Res. J. Sci. Technol., vol. 11, no. 1, pp. 001–004, May 2024, doi: 10.53022/oarjst.2024.11.1.0060.

[13] A. I. Mallick and R. Nath, 'Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments', 2024.

[14] A. Tamrakar and B. Patra, 'CYBERSECURITY THREATS AND COUNTERMEASURES: A REVIEW', TURCOMAT, vol. 9, no. 3, pp. 1400–1404, Dec. 2018, doi: 10.61841/turcomat.v9i3.14598.

[15] M. F. Safitra, M. Lubis, and H. Fakhrurroja, 'The State of Cyber Resilience: Advancements and Future Directions', in Intelligent Sustainable Systems, vol. 817, A. K. Nagar, D. S. Jat, D. K. Mishra, and A. Joshi, Eds, in Lecture Notes in Networks and Systems, vol. 817. , Singapore: Springer Nature Singapore, 2024, pp. 353–363. doi: 10.1007/978-981-99-7886-1_30.

[16] D. Craigen, N. Diakun-Thibault, and R. Purse, 'Defining Cybersecurity', Technology Innovation Management Review, vol. 4, no. 10, pp. 13–21, Oct. 2014, doi: 10.22215/timreview/835.

[17] T. Munusamy and T. Khodadi, 'Building Cyber Resilience: Key Factors for Enhancing Organizational Cyber Security', JIWE, vol. 2, no. 2, pp. 59–71, Sept. 2023, doi: 10.33093/jiwe.2023.2.2.5.

[18] F. Björck, M. Henkel, J. Stirna, and J. Zdravkovic, 'Cyber Resilience Fundamentals for a Definition', 2015, doi: 10.1007/978-3-319-16486-1_31.

[19] S. C. Smith, 'Towards a Scientific Definition of Cyber Resilience', 2023.

[20] D. J. Bodeau and R. Graubart, 'Cyber Resiliency Engineering Framework', 2011.

[21] D. Bodeau, R. Graubart, J. Picciotto, and R. McQuaid, 'Cyber Resiliency Engineering Framework', 2011.

[22] D. J. Bodeau, R. D. Graubart, R. M. McQuaid, and J. Woodill, 'Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring', 2018.

[23] I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and A. Kott, 'Resilience metrics for cyber systems', Springer Science+Business Media New York, 2013, doi: 10.1007/s10669-013-9485-y.

[24] B. Dupont, 'The cyber-resilience of financial institutions: significance and applicability', Journal of Cybersecurity, vol. 5, no. 1, p. tyz013, Jan. 2019, doi: 10.1093/cybsec/tyz013.

[25] A. Kott, M. S. Golan, B. D. Trump, and I. Linkov, 'Cyber Resilience: by Design or by Intervention?', Computer, vol. 54, no. 8, pp. 112–117, Aug. 2021, doi: 10.1109/MC.2021.3082836.

[26] A. AL-Hawamleh, 'Cyber Resilience Framework: Strengthening Defenses and Enhancing Continuity in Business Security', International Journal of Computing and Digital Systems, vol. 15, no. 1, pp. 1315–1331, Mar. 2024, doi: 10.12785/ijcds/150193.

[27] M. Akinsanya, 'Next-Generation Cyber Resilience Frameworks: Enhancing Security, Recovery, and Continuity in Modern Networked Systems', IJSTI, vol. 3, no. 1, pp. 1–14, Feb. 2024, doi: 10.70560/h9r3vs24.

[28] K. Fysarakis et al., 'PHOENI2X A European Cyber Resilience Framework with Artificial-Intelligence', 2023.

[29] M. H. Bejarano, R. J. Rodriguez, and J. Merseguer, 'A Vision for Improving Business Continuity through Cyber-resilience Mechanisms and Frameworks', in 2021 16th Iberian Conference on Information Systems and Technologies (CISTI), Chaves, Portugal: IEEE, June 2021, pp. 1–5. doi: 10.23919/CISTI52073.2021.9476324.

[30] M. Alshar'e, 'CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001', ACJ, pp. 245–255, Feb. 2023, doi: 10.52098/acj.202364.

[31] A. D. Khaleefah and H. M. Al-Mashhadi, 'Methodologies, Requirements and Challenges of Cybersecurity Frameworks: A Review', IJWMT, vol. 13, no. 1, pp. 1–13, Feb. 2023, doi: 10.5815/ijwmt.2023.01.01.

[32] N. Abbasi and D. A. Smith, 'Cybersecurity in Healthcare: Securing Patient Health Information (PHI), HIPPA compliance framework and the responsibilities of healthcare providers.', J. Knowl. Learn. Sci. Technol., vol. 3, no. 3, pp. 278–287, Sept. 2024, doi: 10.60087/jklst.vol3.n3.p.278-287.

[33] V. Božić, 'Compare cybersecurity framework in NIST, ISO 27001, CIS Control and COBIT', 2024, doi: 10.13140/RG.2.2.24546.75201.

[34] E. A. Morse and V. Raval, 'PCI DSS: Payment card industry data security standards in context', Computer Law & Security Review, vol. 24, no. 6, pp. 540–554, Jan. 2008, doi: 10.1016/j.clsr.2008.07.001.

[35] S. R. Muller, 'An Analysis of the Design of the Cybersecurity Maturity Model Certification (CMMC) and Its Direct Effect on Supply Chain Management':, in Advances in Human Resources Management and Organizational Development, D. N. Burrell, Ed., IGI Global, 2023, pp. 220–243. doi: 10.4018/978-1-6684-8691-7.ch014.

[36] A. Said, A. Yahyaoui, and T. Abdellatif, 'HIPAA and GDPR Compliance in IoT Healthcare Systems', in Advances in Model and Data Engineering in the Digitalization Era, vol. 2071, M. Mosbah, T. Kechadi, L. Bellatreche, F. Gargouri, C. G. Guegan, H. Badir, A. Beheshti, and M. M. Gammoudi, Eds, in Communications in Computer and Information Science, vol. 2071., Cham: Springer Nature Switzerland, 2024, pp. 198–209. doi: 10.1007/978-3-031-55729-3_16.

[37] J. Kindervag, 'No More Chewy Centers: Introducing The Zero Trust Model Of Information Security', 2010.

[38] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, 'Theory and Application of Zero Trust Security: A Brief Survey', Entropy, vol. 25, no. 12, p. 1595, Nov. 2023, doi: 10.3390/e25121595.

[39] T. Tam, A. Rao, and J. Hall, 'The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses', Computers & Security, vol. 109, p. 102385, Oct. 2021, doi: 10.1016/j.cose.2021.102385.

[40] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, 'Zero Trust Architecture', National Institute of Standards and Technology, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

[41] E. Iturbe, E. Rios, A. Rego, and N. Toledo, 'Artificial Intelligence for next generation cybersecurity: The AI4CYBER framework', in Proceedings of the 18th International Conference on Availability, Reliability and Security, Benevento Italy: ACM, Aug. 2023, pp. 1–8. doi: 10.1145/3600160.3605051.

[42] Y. Al-Alwan, 'Introduction to AI and Cybersecurity', 2024.

[43] D. A. S. Estay, R. Sahay, M. B. Barfod, and C. D. Jensen, 'A systematic review of cyber-resilience assessment frameworks', Computers &security, 2020, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404820302698

[44] B. Kitchenham and S. M. Charters, 'Guidelines for performing systematic literature reviews in software engineering', 2007.

[45] B. Kitchenham, R. Pretorius, and D. Budgen, 'Systematic literature reviews in software engineering – A tertiary study', 2010, doi: 10.1016/j.infsof.2010.03.006.

[46] M. J. Page, J. E. McKenzie, and P. M. Bossuyt, 'The PRISMA 2020 statement: An updated guideline for reporting systematic reviews', 2021, doi: 10.1016/j.jclinepi.202103.001.

[47] R. Knight and J. R. C. Nurse, 'A framework for effective corporate communication after cyber security incidents', Computers & Security, vol. 99, p. 102036, Dec. 2020, doi: 10.1016/j.cose.2020.102036.

[48] C. M. Patterson, J. R. C. Nurse, and V. N. L. Franqueira, 'Learning from cyber security incidents: A systematic review and future research agenda', Computers & Security, vol. 132, p. 103309, Sept. 2023, doi: 10.1016/j.cose.2023.103309.

[49] R. A. Caralli, J. H. Allen, P. D. Curtis, D. W. White, and L. R. Young, 'CERT Resilience Management Model, Version 1.0', 2010. [Online]. Available: www.cert.org/resilience/

[50] J. Sigholm and M. Bang, 'Towards Offensive Cyber Counterintelligence: Adopting a Target-Centric View on Advanced Persistent Threats', in 2013 European Intelligence and Security Informatics Conference, Uppsala, Sweden: IEEE, Aug. 2013, pp. 166–171. doi: 10.1109/EISIC.2013.37.

[51] D. J. Bodeau, R. D. Graubart, and E. R. Laderman, 'Cyber resiliency engineering overview of the architectural assessment process', in Procedia Computer Science, Elsevier B.V., 2014, pp. 838–847. doi: 10.1016/j.procs.2014.03.100.

[52] T. Aoyama, H. Naruoka, and I. Koshijima, 'Studying Resilient Cyber Incident Management From Large-scale Cyber Security Training', Proceedings of the 10th Asian Control Conference 2015 (ASCC 2015), 2015, doi: 10.1109/ASCC.2015.7244713.

[53] D. Bodeau, R. Graubart, W. Heinbockel, E. Laderman, and M. A. Bedford, 'Cyber Resiliency Engineering Aid-The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques', 2015.

[54] Y. I. Khan and E. AI-Shaer, 'Cyber Resilience-by-Construction: Modeling, Measuring & Verifying', 2015, doi: 10.1145/2809826.2809836.

[55] E. T. Yano, W. de Abreu, P. M. Gustavsson, C. Sweden, and R.-M. Åhlfeldt, 'A framework to support the development of Cyber Resiliency with Situational Awareness Capability', 2015.

[56] I. Bernik and K. Prislan, 'Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation', PLoS ONE, vol. 11, no. 9, p. e0163050, Sept. 2016, doi: 10.1371/journal.pone.0163050.

[57] I. Friedberg, K. McLaughlin, P. Smith, and M. Wurzenberger, 'Towards a Resilience Metric Framework for Cyber-Physical Systems', presented at the 4th International Symposium for ICS & SCADA Cyber Security Research 2016, Oct. 2016. doi: 10.14236/ewic/ICS2016.3.

[58] H. Maziku and S. Shetty., 'Software Defined Networking enabled Resilience for IEC 61850-based Substation Communication Systems', 2017, doi: 10.1109/ICCNC.2017.7876213.

[59] G. Cadete, B. Rød, and M. M. Da Silva, 'Implementation guidance for resilience management of critical infrastructure', in Safety and Reliability – Safe Societies in a Changing World, 1st edn, London: CRC Press, 2018, pp. 1923–1931. doi: 10.1201/9781351174664-241.

[60] F. M. Isiaka, S. A. Audu, and M. A. Umar, 'Developing a fail-safe culture in a cyber environment using MySQL replication technique', IJCS, vol. 4, no. 2, pp. 149–170, 2018, doi: 10.1108/IJCS-04-2018-0008.

[61] Frost and Sullivan, 'Protecting Business Continuity Against Cyber Threats A Siemens Building Technologies Whitepaper'. Siemens Switzerland Ltd, 2018.

[62] M. A. Haque, G. K. De Teyou, S. Shetty, and B. Krishnappa, 'Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights', in 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL: IEEE, Nov. 2018, pp. 25–30. doi: 10.1109/ISI.2018.8587398.

[63] A. Kott et al., 'Approaches to Enhancing Cyber Resilience: Report of the North Atlantic Treaty Organization (NATO) Workshop IST-153', 2018.

[64] J. Mileski, C. Clott, and C. B. Galvao, 'Cyberattacks on ships: a wicked problem approach', MABR, vol. 3, no. 4, pp. 414–430, Dec. 2018, doi: 10.1108/MABR-08-2018-0026.

[65] J. Rajamaki, J. Nevmerzhitskaya, and C. Virag, 'Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF)', in 2018 IEEE Global Engineering Education Conference (EDUCON), Tenerife: IEEE, Apr. 2018, pp. 2042–2046. doi: 10.1109/EDUCON.2018.8363488.

[66] R. Van der Kleij and R. Leukfeldt, 'Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security', 2019, doi: 10.1007/978-3-030-20488-4_2.

[67] A. Aliyu, L. Maglaras, Y. He, and I. Yevseyeva, 'A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom'. 2020.

[68] A. Annarelli, F. Nonino, and G. Palombi, 'Understanding the management of cyber resilient systems', Computers & Industrial Engineering, vol. 149, p. 106829, Nov. 2020, doi: 10.1016/j.cie.2020.106829.

[69] J. F. Carias, M. R. S. Borges, L. Labaka, S. Arrizabalaga, and J. Hernantes, 'Systematic Approach to Cyber Resilience Operationalization in SMEs', 2020, doi: 10.1109/ACCESS.2020.3026063.

[70] J. Osborn, 'Comparison of the Impact-Wave Analogy to Published Cyber Resilience Models', 2020.

[71] J. F. Carias, S. Arrizabalaga, L. Labaka, and J. Hernantes, 'Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs', IEEE Access, vol. 9, pp. 80741–80762, 2021, doi: 10.1109/ACCESS.2021.3085530.

[72] E. Hammad, A. K. Nag, A. Chennamaneni, M. Aghashahi, and E. Dogdu, 'A Deep-Defense Approach for Next -Gen Cyber - Resilient Inter-Dependent Critical Infrastructure Systems', in 2021 Resilience Week (RWS), Salt Lake City, UT, USA: IEEE, Oct. 2021, pp. 1–7. doi: 10.1109/RWS52686.2021.9611790.

[73] A. A. Mercado-Velazquez, P. J. Escamilla-Ambrosio, and F. Ortiz-Rodriguez, 'A Moving Target Defense Strategy for Internet of Things Cybersecurity', IEEE Access, vol. 9, pp. 118406–118418, 2021, doi: 10.1109/ACCESS.2021.3107403.

[74] K. Renaud and J. Ophoff, 'A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs', OCJ, vol. 1, no. 1, pp. 24–46, Oct. 2021, doi: 10.1108/OCJ-03-2021-0004.

[75] G. Thomas and M.-J. Sule, 'A service lens on cybersecurity continuity and management for organizations' subsistence and growth', OCJ, vol. 3, no. 1, pp. 18–40, 2022, doi: 10.1108/OCJ-09-2021-0025.

[76] T. D. Ashley, R. Kwon, S. N. G. Gourisetti, C. Katsis, C. A. Bonebrake, and P. A. Boyd, 'Gamification of Cybersecurity for Workforce Development in Critical Infrastructure', IEEE Access, vol. 10, pp. 112487–112501, 2022, doi: 10.1109/ACCESS.2022.3216711.

[77] A. E. Bekkali, M. Essaaidi, and M. Boulmalf, 'A Blockchain-Based Architecture and Framework for Cybersecure Smart Cities', IEEE Access, vol. 11, pp. 76359–76370, 2023, doi: 10.1109/ACCESS.2023.3296482.

[78] V. K. Hidayat and G. Wang, 'A Comprehensive Cybersecurity Maturity Study for Nonbank Financial Institution', Journal of System and Management Sciences, vol. 13, no. 5, pp. 525–543, 2023, doi: 10.33168/JSMS.2023.0534.

[79] G. Ahn, J. Jang, S. Choi, and D. Shin, 'Research on Improving Cyber Resilience by Integrating the Zero Trust Security Model With the MITRE ATT&CK Matrix', IEEE Access, vol. 12, pp. 89291–89309, 2024, doi: 10.1109/ACCESS.2024.3417182.

[80] A. Dimakopoulou and K. Rantos, 'Comprehensive Analysis of maritime Cybersecurity Landscape Based on the NIST CSF v2.0', 2024, doi: 10.3390/jmse12060919.

[81] E. Egho-Promise, E. Lyada, G. Asante, and F. Aina, 'Towards Improved Vulnerability Management in Digital Environments: A Comprehensive Framework for Cyber Security Enhancement', IRJCS: International Research Journal of Computer Science, vol. 11, no. 05, pp. 441–449, 2024, doi: 10.26562/irjcs.

[82] E. Y. Handri, D. Indra Sensuse, and A. Tarigan, 'Developing an Agile Cybersecurity Framework With Organizational Culture Approach Using Q Methodology', IEEE Access, vol. 12, pp. 108835–108850, 2024, doi: 10.1109/ACCESS.2024.3432160.

[83] M. Herburger, A. Wieland, and C. Hochstrasser, 'Building supply chain resilience to cyber risks: a dynamic capabilities perspective', Supply Chain Management, vol. 29, no. 7, pp. 28–50, 2024, doi: 10.1108/SCM-01-2023-0016.

[84] Y. Liu, S. Li, X. Wang, and L. Xu, 'A Review of Hybrid Cyber Threats Modelling and Detection Using Artificial Intelligence in IIoT', CMES - Computer Modeling in Engineering and Sciences, vol. 140, no. 2, pp. 1233–1261, 2024, doi: 10.32604/cmes.2024.046473.

[85] D. D. Shankar, A. S. Azhakath, N. Khalil, S. J. , M. T. , and S. K. , 'Data mining for cyber biosecurity risk management – A comprehensive review', Computers & Security, vol. 137, p. 103627, Feb. 2024, doi: 10.1016/j.cose.2023.103627.

[86] E. Kokogho, P. E. Odio, O. Y. Ogunsola, and M. O. Nwaozomudoh, 'A Cybersecurity framework for fraud detection in financial systems using AI and Microservices', GJABR, vol. 3, no. 2, pp. 410–424, Feb. 2025, doi: 10.51594/gjabr.v3i2.90.

[87] A. Grace, 'AI-Enhanced Cyber Resilience in Smart Cities: A Multi-Layered Defense Framework Against Emerging Threats', 2025.

[88] A. Ko, J. Hyeon Lee, and J. T. Seo, 'KPI-Based Evaluation Framework for Cyber Resilience of Ships', IEEE Access, vol. 13, pp. 64226–64245, 2025, doi: 10.1109/ACCESS.2025.3550501.

[89] H. M. T. N. Jayathilaka and J. Wijayanayake, 'Systematic Literature Review on Developing an AI Framework for SME Cybersecurity Identification and Personalized Recommendations', sljo-j-jdrra, vol. 2, no. 2, pp. 249–250, Jan. 2025, doi: 10.4038/jdrra.v2i2.53.

[90] G. Areo, 'The Role of AI in Addressing Remote Work Cybersecurity Challenges: Emerging Trends and Tools', 2025.

[91] L. Bernardo, S. Malta, and J. Magalhães, 'An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF', Electronics, vol. 14, no. 7, p. 1364, Mar. 2025, doi: 10.3390/electronics14071364.

[92] N. Raza and F. Moazeni, 'Optimal cybersecurity framework for smart water system: Detection, localization and severity assessment', Water Research, vol. 281, p. 123517, Aug. 2025, doi: 10.1016/j.watres.2025.123517.

[93] C. E. Alozie and E. E. Chinwe, 'Developing a Cybersecurity Framework for Protecting Critical Infrastructure in Organizations', Jan. 2025, doi: 10.5281/ZENODO.14740463.

[94] J. Nsoh, 'Cognitive Zero-Trust Resilience: An Adaptive Cybersecurity Framework for Dynamic Connected Systems', PriMera Scientific Engineering 7.1 (2025): 17-37., June 2025, doi: 10.56831/PSEN-07-209.

[95] W. Abbass, N. Abbas, U. Majeed, W. Nawaz, Q. Abbas, and A. Hussain Farooqi, 'A Cyber Resilient Framework for V2X Enabled Roundabouts in Intelligent Transportation Systems', IEEE Access, vol. 13, pp. 154775–154802, 2025, doi: 10.1109/ACCESS.2025.3604095.