A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions

SALEH MOHAMED ALHIDAIFI, The University of Glasgow, Glasgow, United Kingdom
MUHAMMAD RIZWAN ASGHAR, University of Surrey, Guildford, United Kingdom and The University of Auckland, Auckland, New Zealand
IMRAN SHAFIQUE ANSARI, The University of Glasgow, Glasgow, United Kingdom

Cyber resilience has become a major concern for both academia and industry due to the increasing number of data breaches caused by the expanding attack surface of existing IT infrastructure. Cyber resilience refers to an organisation's ability to prepare for, absorb, recover from, and adapt to adverse effects typically caused by cyber-attacks that affect business operations. In this survey, we aim to identify the significant domains of cyber resilience and measure their effectiveness. We have selected these domains based on a literature review of frameworks, strategies, applications, tools, and technologies. We have outlined the cyber resilience requirements for each domain and explored solutions related to each requirement in detail. We have also compared and analysed different studies in each domain to find other ways of enhancing cyber resilience. Furthermore, we have compared cyber resilience frameworks and strategies based on technical requirements for various applications. We have also elaborated on techniques for improving cyber resilience. In the supplementary section, we have presented applications that have implemented cyber resilience. This survey comprehensively compares various popular cyber resilience tools to help researchers, practitioners, and organisations choose the best practices for enhancing cyber resilience. Finally, we have shared key findings, limitations, problems, and future directions.

CCS Concepts: • **General and reference → Surveys and overviews;**

Additional Key Words and Phrases: Cyber resilience, cyber resilience engineering framework (CREF), cybersecurity, risk management, threat modelling, and cyber-attacks

ACM Reference Format:
Saleh Mohamed AlHidaifi, Muhammad Rizwan Asghar, and Imran Shafique Ansari. 2024. A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions. *ACM Comput. Surv.* 56, 8, Article 196 (April 2024), 48 pages. https://doi.org/10.1145/3649218

1 INTRODUCTION

Cyber resilience is receiving attention from **Information Technology (IT)** experts due to the surge in cyber-attacks compromising the existing infrastructure [81]. Cybersecurity mainly protects IT assets such as data. Still, cyber resilience is the ability of the system to defend against successful cyber-attacks and revert to a normal state when cybersecurity fails to protect the

Authors' addresses: S. M. AlHidaifi and I. S. Ansari, The University of Glasgow, Glasgow, Scotland, United Kingdom, G12 8QQ; e-mails: s.alhaudii@gmail.com, imran.ansari@glasgow.ac.uk; M. R. Asghar, University of Surrey, Guildford, United Kingdom and and The University of Auckland, Auckland, New Zealand; e-mail: r.asghar@surrey.ac.uk.

ACM 0360-0300/2024/04-ART196
https://doi.org/10.1145/3649218

system [71]. Cyber resilience enables organisations to return to running when cyber-attacks are missed by the deployed cybersecurity solutions [42]. Cyber resilience is not only about resisting potential breaches but rather about learning from those attempts and continuously adapting the system to changing conditions to dampen its impact on service survivability. In other words, it aims to sustain system operations while ensuring mission execution [14].

Let us consider cyber-attacks that happened in 2007 in Estonia, then in 2010 the Stuxnet attack on the Iranian nuclear program [65]. After the 2007 Estonian cyber-attack, many technologically advanced governments reinforced their national cyber resilience [134]. Cyber resilience has been implemented in many applications, such as Information Technology (IT) security research [6]. Even though it is widely now utilised among practitioners in many countries, understanding cyber resilience is critical, especially from the information security perspective within political, industrial, and business domains [145]. Cyber resilience is increasingly an explicit concern for programs, systems, and missions. Therefore, cyber resilience architects and system engineers investigate ways to implement cyber resilience concepts by integrating and enhancing technologies into designs and architectures of cyber resilience [23].

Cyber resilience combines best practices from business continuity, IT infrastructure security, and other disciplines to create a business strategy that addresses today's needs and goals. An enterprise can prepare efficiently and prevent, detect, respond to, and recover from cyber-attacks. If an enterprise can at least partially continue its business operations during a cyber-attack, it will be called a *cyber resilience enterprise* [68]. The relationship between cyber resilience and business is formed by enterprise connection, which becomes essential when assessing business resilience.

A cyber-attack that manages to breach the organisation's systems or networks could have a significant impact on its overall operation. That is why cyber resilience becomes paramount for those responsible for risk management, business continuity, and cybersecurity professionals [45]. Protecting against cyber-attacks has become more complex due to several vulnerabilities and sophisticated threats. Cyber resilience attempts to rebalance by designing systems to continue working under cyber-attacks [145].

Cyber resilience efforts and strategies have traditionally been considered enabling governments and businesses to deliver the intended outcome despite disruptions to information and communication systems [37]. Additionally, most professionals understand the importance of cybersecurity, but fewer IT security specialists understand the adequate significance of cyber resilience; unfortunately, the top management might not be fully aware of cyber resilience [54]. Cyber resilience recognises that cyber systems contain components across the physical, information, cognitive, and social environments in which they exist [38]. Recent efforts based on this idea have generated a set of cyber resilience metrics that organisations can integrate with decision-analytic frameworks to compare cyber system designs or prioritise cyber system upgrades and maintenance [90].

1.1 Contributions

This survey includes main contributions as follows: (1) focuses on cyber resilience and its critical domains, which have received more attention from researchers; (2) understands the significant domains of cyber resilience, including frameworks, strategies, applications, tools, and technologies and outlines the requirements for each domain; (3) discusses each of these domains in detail and groups them into five domains based on the critical area discussion, as shown in Figure 1; (4) explores solutions related to each domain and compares and analyses different studies to find ways of enhancing cyber resilience; (5) compares **Cyber Resilience Frameworks (CRFs)** and strategies based on technical requirements for various applications, helping researchers, practitioners, and organisations choose best practices for enhancing cyber resilience; and (6) presents key findings, limitations, problems, and future directions in the field of cyber resilience. Overall, it provides a

Fig. 1. Mind-Map of cyber resilience. The studies in this survey were grouped into five categories based on the critical area of cyber resilience. The five main categories are frameworks, strategies, recent advancements, applications, and tools.

comprehensive overview of cyber resilience, identifies key strategies and research challenges, and offers insights into future directions for enhancing cyber resilience.

1.2 Survey's Selected Domains

The selected domains of frameworks, strategies, recent advancements applications, and tools are all critical in contributing to the overall cyber resilience of organisations in many ways, which can be summarised as follows.

Frameworks. They offer a roadmap for organisations to assess their current cyber resilience, identify vulnerabilities, and prioritise actions. By adhering to established frameworks, organisations can ensure that they cover all critical aspects of cyber resilience, making their efforts systematic and consistent. Moreover, using common frameworks facilitates communication and collaboration among different organisations and sectors, enhancing overall cyber resilience at

a broader scale. Frameworks also provide a common language and set of standards for cyber resilience, which can help improve collaboration and information sharing between organisations.

Strategies. These help organisations define their objectives, allocate resources, and proactively protect against cyber threats. Strategies encompass both technical and non-technical aspects, emphasising the importance of employee training and awareness. Effective strategies ensure that organisations are prepared to efficiently prevent, detect, respond to, and recover from cyber incidents. Effective cyber resilience strategies are critical in mitigating the impact of cyber-attacks and ensuring that organisations can continue to operate in the face of cyber threats.

Recent Advancements. These recent advancements include today's digital age. Organisations need to stay up to date with the latest advancements in cyber resilience as well as threat intelligence and industry trends. Cyber-attacks are becoming increasingly sophisticated and frequent, and continuous integration of new advancements is crucial for organisations to proactively mitigate emerging risks and vulnerabilities. By keeping abreast of these advancements, organisations can better protect themselves from potential attacks.

Applications. These applications include software solutions like Security Information and Event Management (SIEM) systems, **Intrusion Detection Systems (IDS)**, and vulnerability scanners. They are critical in continuously monitoring the organisation's digital environment, detecting anomalies, and providing real-time alerts. Integrating these applications into the cybersecurity ecosystem enables proactive threat detection and incident response, reducing the potential impact of cyber-attacks. These tools can help organisations identify potential threats and vulnerabilities and respond quickly and effectively to cyber-attacks.

Tools and Technologies. These tools and technologies include firewalls, encryption technologies, backup and recovery systems, and other security measures. These tools act as defensive mechanisms, safeguarding an organisation's digital assets and data. They work with strategies and applications to create multiple layers of protection against evolving cyber threats. Practical cyber resilience tools and technologies are critical in protecting organisations from cyber threats and ensuring they can recover quickly during attacks.

These domains are interrelated and contribute to developing a comprehensive cyber resilience strategy. Frameworks provide a structured approach to identifying and prioritising cyber resilience efforts, whereas strategies, recent advancements, applications, tools and technologies provide the specific measures and tools needed to implement those efforts. By working together, these domains can help organisations build solid and effective cyber resilience to mitigate cyber-attack impact and ensure business continuity.

1.3 Requirements Classification

In this survey, we utilised cyber resilience requirements classification into the groups as shown in Table 1, which can be summarised as follows.

Framework Requirements. These requirements are related to CRFs and are used in Section 3, which support specific application domains such as security systems, network systems, and **Cyber-Physical Systems (CPS)**. It is similar to the **Cyber Resilience Engineering Framework (CREF)**, the most popular one. There are other framework requirements, such as development cost to design the CRF, deployment cost to implement the framework, and maintenance cost to continue utilising the framework. The other framework requirements, such as support by multi-data sources, will make the framework more flexible for incorporating data sources. Correspondingly, the framework should be open source to be easily modified, customised, and utilise metrics to quantify the framework.

Table 1. Cyber Resilience Requirements

Domains	Section	Requirements	Description	Evaluations
Frameworks	Section 3	Similar to Cyber Resilience Engineering Framework (CREF)	Similar to the popular CRF	👍 / 👎
		Development cost	The cost of a new framework	○/ ◐/ ●
		Deployment cost	The cost of developing a framework	○/ ◐/ ●
		Maintenance cost	The cost of maintenance and improvement a framework	○/ ◐/ ●
		Support multi-data sources	Competencies to support multi-data sources	👍 / 👎
		Open source	Available as open source	👍 / 👎
		Use metrics	Use a number of metrics	👍 / 👎
Strategies	Section 4	Effectiveness	Set the right goals and objectives consistently to achieve them	👍 / 👎
		Strategic acceptability	Concentrated and suitable for achieving the goals	👍 / 👎
		Cost	The cost of implementing the strategy	○/ ◐/ ●
		Quality	Fitness to productivity strategies with high significance	○/ ◐/ ●
		Flexibility	Capability to respond to major changes if needed	○/ ◐/ ●
Advancements	Section 5	Organisational management	The whole thing with organisational management	👍 / 👎
		Operational management	Machinery with operational management	👍 / 👎
		Gives recommendations	Competency to provide recommendations for improvement	👍 / 👎
		Uses standards	Supports and uses some international standards	👍 / 👎
		Uses technologies	Using some technologies for improvement	👍 / 👎
		Improvement cost	The cost of improving the cyber resilience	○/ ◐/ ●
		Performance after improvement	Capability to continue performance after improvement	○/ ◐/ ●
Applications	Appendix A	Application	Suitable for a specific application	Exegesis
		Domains	Effective for a specific domain	Exegesis
Tools	Section 6	Organisational management	Working with organisational management	👍 / 👎
		Operational management	Mechanism with operational management	👍 / 👎
		Easy to use	Ability to be friendly and easy to use	👍 / 👎
		Web based	Available as a web-based tool	👍 / 👎
		Efficient	Efficient working	👍 / 👎
		Software based	Presented as software based	👍 / 👎
		Open source	Available as open source	👍 / 👎
		Cost	The license cost of the tool	○/ ◐/ ●
		Performance	Proficiency in working with good performance	○/ ◐/ ●
		Uses database	Supports database	○/ ◐/ ●
		Paths to improvements	Provides the report of paths for improvement	👍 / 👎
👍=Yes, 👎=No, ○=Low, ◐=Medium, and ●=High				

Strategy Requirements. These requirements are related to cyber resilience strategies used in Section 4, which are support specific application domains, should be effective, should be strategically acceptable, cost of the strategy, quality of the strategy, and flexibility of the strategy. These requirements will help select the best strategy for cyber resilience in a specific application. For example, the flexibility of the strategy requirement will show the ability to change the strategy to improve cyber resilience quickly.

Recent Advancement Requirements. These requirements are related to improving cyber resilience and are considered in Section 5. They refer to supporting a specific area or application domain, such as in the supply chain, organisation, or cyber defence. They cover whether there is an enhancement to the organisational management level or an improvement at the operational management level. Another one is to utilise international standards and technologies to improve cyber resilience, cost improvement, and performance after advancement.

Applications Requirements. These requirements are related to cyber resilience applications and are used in Appendix A. Those are compatible with specific applications and valid for a particular domain. These requirements will help researchers understand the applications that already implemented cyber resilience. However, these requirements will compare applications implementing cyber resilience. The main applications and sectors using these requirements are transportation, financial, power system, supply chain, **Supervisory Control And Data Acquisition (SCADA)** systems, smart grid, communications network, healthcare, and **Industrial Control Systems (ICS)**.

Tools Requirements. These requirements are related to cyber resilience tools used in Section 6. They refer to work in organisational management, conducting into operational management, easy to use and more friendly for users, web-based too fast access, efficient, software based, open source if available, cost-effective, performing exemplary, monitoring and tracking cyber resilience as a predictive measure for future via use of a database, and showing the improvement path of cyber resilience.

1.4 Survey Outline

The survey is divided into several sections. In Section 2, we define the term *cyber resilience* and discuss the concept in detail. In Section 3, we review and compare existing CRFs. Then, in Section 4, we look at existing cyber resilience strategies and highlight their differences. Section 5 covers the recent techniques used to advance cyber resilience. In Section 6, we compare the tools and technologies used to evaluate and improve cyber resilience. In Section 7, we explore research studies on threat modelling related to cyber resilience. Section 8 discusses the key findings, limitations, and open problems related to cyber resilience. Finally, in Section 9, we focus on future research directions for cyber resilience. The survey concludes in Section 10. Due to strict page limits, we discuss implemented cyber resilience applications in Appendix A[1] and list acronyms in Appendix B.

2 DEFINING CYBER RESILIENCE

This section presents different definitions of cyber resilience and its meaning in various domains, as illustrated in Table 2. Subsequently, we discuss the conceptualisation of cyber resilience and make it more apparent relative to the existing works. Moreover, we demonstrate cyber resilience and how it works diagrammatically. Cyber resilience has many definitions depending on its implemented application. For instance, a small business can explain cyber resilience to defend against cyber-attacks and roll back to a healthy functioning state. It can also be defined as ensuring devices operate under any threat environment and are not affected by malicious activities such as phishing e-mails and distributing spam [143]. Similarly, it is also defined as the ability to maintain the operation of a system when it is under cyber-attacks [9]. Cyber resilience encompasses the capacity to withstand cyber-attacks and involves multiple dimensions for assessment [138].

Most definitions of cyber resilience focus on an organisational level without considering the system level. However, there are some fundamental differences between those definitions. Studies have been conducted on cyber resilience at the organisation level [6, 17, 111, 115]. Aoyama et al. [6] described cyber resilience as the capability of organisations to defend against cyber-attacks based on three factors of cyber resilience: prevention, detection, and response. These factors have a specific resilience factor: prevention for anticipating, detection for monitoring, and learning and incident reporting response. The main limitation of this definition is describing cyber resilience as based on cyber-attacks without mentioning what happens after the successful attack.

[1] https://github.com/SecurityResearchs/Cyber-Resileince-Research/blob/main/Survey_Appendix.pdf

Table 2. Summary of Cyber Resilience Definitions from 2010 to 2023

Proposals	Year	Level of Definition	Defined Cyber Resilience as . . .
Williams and Manheke [143]	2010	Organisational management	the ability to defend against cyber-attack and rollback to a healthy functioning state
Vugrin and Turgeon [50]	2014	System	the ability to reduce successfully the duration and importance of the targeted machine ranges for overall performance
Aoyama et al. [6]	2015	Organisational management	the capability of organisations to address cyber-attacks
Björck et al. [17]	2015	Organisational management	the ability to continuously monitor the intended outcome and adverse cyber events
Bodeau and Graubart [22]	2016	Organisational management and system	the ability to anticipate, withstand, and recover from cyber-attack and adapt to adverse attacks using cyber resources
Todorovic et al. [136]	2016	System	the ability to quickly recover from disruptive events caused by humans or nature by adapting, anticipating, and absorbing
Ayoub et al. [115]	2017	Organisational management	the capability to react, resist, and sense adapting events, and reshaping and adapting operations in risk environments
The Ponemon Institute and IBM Resilient [111]	2018	Organisational management	the prevention alignment, capabilities of detection, and response to manage and mitigate from cyber-attacks
Onwubiko [108]	2020	Organisational management and system	the ability to anticipate, withstand, recover from cyber-attack, and adapt to adverse attacks, stresses, conditions, and/or compromises on cyber resources
Hausken [64]	2020	Organisational management and system	the ability of an actor to resist, respond, and recover from cyber-attacks to ensure the actor's operational continuity.
Asante et al. [9]	2021	System	the ability to maintain the operation of a system when it is under cyber-attacks
Keleba et al. [74]	2022	Organisational management and system	the capacity of the organisation or system to withstand and recover quickly from cyber-attacks
Ur-Rehman et al. [138]	2022	System	the ability to resist cyber-attacks and has several dimensions to evaluate
Smith [128]	2023	Organisational management and system	the ability of an organisation or system to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources

Some authors define cyber resilience at the organisation level as the capacity to consider different groups, such as methods, challenges, and reasonable controls for cyber resilience. Björck et al. [17] defined cyber resilience as the ability to achieve the intended outcome and overcome adverse cyber events continuously. They consistently imply the ability to deliver change tools or make modifications if needed while facing risks. The intended outcome refers to achieving different goals through online services.

Likewise, Ayoub et al. [115] prescribed cyber resilience at the organisation level as the capability to react, resist, and sense to adapting events and reshaping and adapting operations in environments with foreseeable and unforeseeable risks. These risks emerge when technological change is so rapid that it becomes more challenging to predict many risks arising in the digital space. In other words, cyber resilience encompasses both organisational and cybersecurity and aims to defend against potential cyber-attacks to make survival possible after an attack. Therefore, an essential issue with this definition is that it does not include the main cyber resilience stages, absorbing and recovering.

The Ponemon Institute [111] determined cyber resilience as an organisation's prevention alignment and capabilities to detect, respond to, manage, and mitigate cyber-attacks. That refers to an enterprise's capacity to maintain its core of both purpose and integrity in the face of cyber resilience. A cyber resilience enterprise can have the ability to prevent, detect, contain, and recover from myriad severe threats against data, applications, and IT infrastructure. As per the definition provided by Keleba et al. [74], cyber resilience is characterised by the capability to effectively endure and swiftly recuperate from unanticipated and substantial interruptions caused by cyber-attacks. It pertains to an entity's capacity to adjust to recognised and unrecognised emergencies, risks, obstacles, and adversities, ultimately ensuring the continuation of services or business operations despite cyber threats.

Several researchers have only outlined cyber resilience as system level without considering the organisational level. Vugrin and Turgeon [50] defined the resilience of a system as the occurrence of a particular disruptive event or set of circumstances with the ability to reduce efficiently the targeted system levels affecting the performance. The central gap of this study is to consider only technical issues without considering human errors. To fill this gap, Todorovic et al. [136] defined cyber resilience as a system able to identify and target the system's enhancement for the inherent capacity to respond throughout the inevitable change process for both short and long duration. The resilience infrastructure can adapt, anticipate, and absorb a potentially disruptive event via rapidly recovering, whether human caused or naturally occurring.

A few studies in the broader literature have determined cyber resilience at organisational and system levels. Cyber resilience is defined in some works [22, 84, 85, 108] as the ability to anticipate, withstand, recover from cyber-attack, and adapt to adverse attacks, stresses, conditions and compromises on cyber resources. Cyber resilience can be a capability of an organisation, a business function, a mission, a system, a system-of-systems, or a cross-organisational mission; the term can also be applied to a nation, region, group, household, or an individual.

Hausken [64] described cyber resilience as the ability of an actor to resist, respond, and recover from cyber-attacks to ensure the actor's operational continuity. Moreover, the author reviewed and assessed the emerging cyber resilience role. Cyber resilience can include various actors classified into three: non-threat actors, threat actors, and hybrid actors. Threat actors can be hackers and criminals–non-threat actors such as governments, regulators, incident responders, insurers, organisations, and individuals. Mixed actors can be companies that may sometimes, inadvertently or deliberately, compromise the cyber resilience of other actors. Actors operate at various levels, from organisation, group, individual, and regional to global. Each actor chooses strategies based on beliefs and preferences that impact cyber resilience.

Smith [128] defined cyber resilience as the ability of an organisation or system to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources. It encompasses the capacity to provide and maintain an acceptable level of service in the face of faults and challenges to normal operations.

We consider cyber resilience as the ability of systems or services to roll back and continue operations in a normal situation after an attack happens with fast automation. The concept of cyber resilience involves three steps. First, it starts after a cyber attack has caused network, system, or service failure. Second, cyber resilience comes into action to address the affected networks, systems, or services. Finally, it initiates a rollback process to restore the networks, systems, or services to their normal state as quickly as possible with the help of automation. The main popular areas and sectors that implemented cyber resilience are transportation, finance, power systems, supply chain, Supervisory Control And Data Acquisition (SCADA) system, smart grid, wireless communication networks, health care, and Industrial Control System (ICS), as shown in Figure 2.

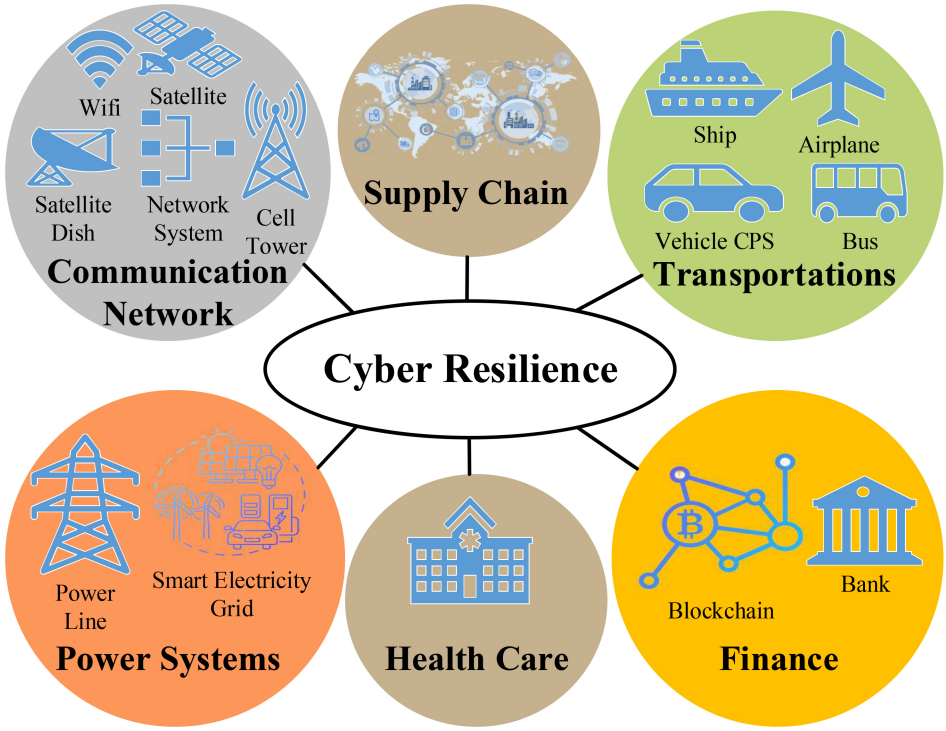

Fig. 2. The main popular areas wherein cyber resilience has been successfully implemented are transportation, finance, supply chain, health care, power systems, and communication networks.

3 CYBER RESILIENCE FRAMEWORKS

The Cambridge Dictionary defines *framework* as "the principles, ideas, and information that form a plan or the organisation structure." CRFs provide organisations with a security approach that is cost-effective, flexible, and performance based [122]. Many CRFs are proposed, and around 200 are assessment frameworks, highlighting the need for a simple approach for **Small and Medium-sized Enterprises (SMEs)** to operate cyber resilience effectively [31]. Various standards and frameworks have been developed for implementing and evaluating cyber resilience, including **International Organisation for Standardisation/International Electrotechnical Commission 27001 (ISO/IEC 27001)**, **National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST-CSF)**, **Cybersecurity Capability Maturity Model (C2M2)**, **Computer Emergency Readiness Team-Resilience Management Model (CERT-RMM)**, **Control Objectives for Information and Related Technologies (COBIT)**, and **OpenWeb Application Security Project (OWASP)**.

These frameworks help organisations understand their capabilities and guide them in implementing or refining resilience plans. Additionally, frameworks help to address the assessment of cyber resilience, taking into account factors such as the cost of implementation and the development needs of different types of organisations [110]. Organisations must apply or develop these frameworks and standards to identify areas in their system that need improvements. Several CRFs are available, but the most popular is the CREF. The main reason for comparing these frameworks is to identify their strengths and weaknesses.

CRFs provide a structured approach to identifying and addressing potential cyber threats and vulnerabilities. They help organisations develop a comprehensive understanding of their cyber risk profile and prioritise their cyber resilience efforts. Frameworks also provide a common language and set of standards for cyber resilience, which can help improve collaboration and information sharing between organisations. There are some criteria utilised to demonstrate the contrast within frameworks as follows: if it pertains to applications domain, similar to the Cyber Resilience Engineering Framework (CREF), supports multi-data sources, open source, uses metrics, and the cost of development, deployment, and maintenance, as can be seen in Table 3.

Some researchers [19, 20, 24, 48, 77, 81, 89] proposed their framework to be similar to CREF. Most previous and current frameworks do not support multi-data sources, but a few do support them (e.g., [35, 45, 57, 121]). Bodeau and Graubart [20] provided a framework that analyses cyber resilience goals, objectives, costs, structure discussions, and practices. It also serves to characterise cyber resilience metrics and motivation. The framework can evolve as the discipline of cyber resilience engineering matures. Cyber resilience engineering is a part of mission assurance engineering. Various subjects inform it, such as resilience engineering, information systems, security engineering, fault tolerance, dependability, survivability, business continuity, and contingency planning. The framework requires three components to enable cyber resilience engineering and related disciplines: cybersecurity, resilience engineering, and mission assurance.

Linkov et al. [89] used the matrix framework that was proposed by Linkov et al. [88] to implement cyber systems. They focused on developing a new framework that can inform the extent of the resiliency of cyber systems within the scope of **Executive Order 13636 (EO 13636)** and **Presidential Policy Directive 21 (PPD 21)**. The resiliency matrix must be generalised and applicable across many approaches to perform a comparative evaluation of systems' resiliency. Moreover, the metrics must be easily monitored and reported to the management changes made by system operations and decision makers. The importance of this resilience metrics framework can be realised by its ability to allocate resources to enhance resiliency at an organisation.

The frameworks presented in some works [20, 21, 24] provided and discussed a background on the CREF, which can help structure the analysis through an assessment. The CREF is illustrated in Figure 3 and described in more detail in the work of Bodeau and Graubart [20]. The CREF can organise the cyber resilience domain into goals, objectives, and techniques. Goals are the high-level intended statement outputs. Objectives are more specific information about intended outcomes to enable assessment; an objective can be determined with a single goal but may sometimes support achieving multiple goals. Techniques are approaches to achieve one or more cyber resilience purposes applied to the design or architecture of a business/mission function based on the cyber resources that support them.

Bodeau et al. [19] described how resilience techniques apply to an acknowledged system. They extended the definitions of goals, objectives, and methods presented in another work [20] on the CREF. The extended definitions are (1) extend the set of potential threat sources to include common errors, events, and adversarial actions, (2) extend the collection of adversarial actions to include vectors of non-cyber-attacks, and (3) cyber-physical consideration on pure cyber systems.

Choudhury et al. [35] focused on the problem of determining dynamic actions to achieve resilience concerning the failure of hardware, compromised systems, or services. They took the first steps towards developing a formal methodology to make a complex enterprise web resilient. Additionally, they presented a unifying graph-based model for representing the behaviour, infrastructure, and missions of the enterprise web and the dependencies among them. This approach's benefit is that it consolidates multiple data sources, such as Net-Flow, events, and logs, into one model, providing insight into the reasons for actions in the model space. They then transformed actions determined in the model space, such as deleting an edge in a graph,

Table 3. Comparisons of CRFs

Framework	Year	Application Domains	Similar to CREF	Development Cost	Deployment Cost	Maintenance Cost	Support Multi-Data Sources	Open Source	Uses Metrics	Strengths	Weaknesses
Bodeau and Graubart [20]	2011	Security systems	👍	●	◐	◐	👎	👎	👍	First CRF	Complex to implement
Linkov et al. [89]	2013	Military systems	👍	◐	◐	○	👎	👍	👍	Generalisable for many systems	Not focused on defining cyber resilience as the network property of the system
Bodeau et al. [19]	2014	System of systems	👍	●	●	◐	👎	👎	👎	Includes methods, goals, and objectives	Only applicable to general systems
Bodeau et al. [24]	2015	Security systems	👍	●	◐	○	👍	👎	👎	Helpful for structure analysis	Complex to implement
Choudhury et al. [35]	2015	Security systems	👎	●	○	○	👍	👎	👎	Can deal with multi-data sources	Complex to implement
Aoyama et al. [6]	2015	Cyber-attacks	👎	●	◐	○	👎	👎	👎	Includes different categories	Only useful when an incident or attack happens
Khan and Al-shaer [77]	2015	Network systems	👍	●	○	◐	👎	👎	👍	Allows users who used it to measure the resilience for different properties and attacks	Only supports network systems
Yano et al. [48]	2015	Network systems	👍	●	●	●	👎	👎	👎	Easy implementation with different network segments	The framework is still in the evaluation stage
Friedberg et al. [52]	2016	Cyber-Physical Systems (CPS)	👎	◐	○	◐	👎	👎	👍	It has a flexible way and a scalable system model to measure system resilience numerically	Implementation of the framework and its evaluation is challenging
Ayoub et al. [115]	2017	Cyber ecosystem	👎	●	◐	●	👎	👎	👎	It offers a range of tools that will hopefully be a strong framework	Managing and controlling the framework is very costly, as it uses various types of tools
Rose et al. [121]	2017	Cyber equipment	👎	○	○	○	👍	👎	👎	It is practical and usable	It is directly applicable only to cyber equipment
Gisladottir et al. [57]	2017	Network systems	👎	●	◐	◐	👍	👎	👎	A thorough analysis of complex networks using multi-sources	Complex to implement
Maziku and Shetty [96]	2017	Smart grid networks	👎	●	●	○	👎	👎	👎	Ability to work in real time	Only supports smart grid networks
Kott et al. [81]	2018	Supply chain networks	👍	○	◐	○	👎	👎	👎	It can structure cyber resilience efficiently by addressing the practices, objectives, and goals	It requires many steps for preparation before beginning the implementation
Haque et al. [62]	2018	Industrial Control Systems (ICS)	👎	●	●	●	👎	👎	👍	Helpful for technical experts to identify gaps in the study of ICS resilience easily	Only compatible with ICS
Dickson and Goodwin [45]	2019	Internet of Things (IoT)	👎	●	◐	○	👍	👎	👎	Applying key technologies to enable their CRF	Complex configurations
Carías et al. [33]	2020	Small and Medium-sized Enterprises (SMEs)	👎	●	●	○	👎	👎	👎	Offering a comprehensive framework with 10 domains and 32 policies, covering various dimensions of cyber resilience	The framework does not address specific technical details, such as multiple data sources
Bejarano et al. [13]	2021	Organisation management	👎	○	○	○	👎	👍	👎	The study focuses into the NIST framework that is a widely used tool for managing cybersecurity risks	The framework's complexity may pose challenges for organisations to implement
Hammad et al. [61]	2021	CPS	👎	○	○	○	👍	👎	👎	The framework uses AI technology	Any mistake into the data source will affect the final results
Al Maruf et al. [3]	2023	CPS	👎	○	○	◐	👎	👎	👎	This framework includes redundancy and restarting mechanisms	The implementation process is complex

👍=Yes, 👎=No, ○=Low, ◐=Medium, and ●=High

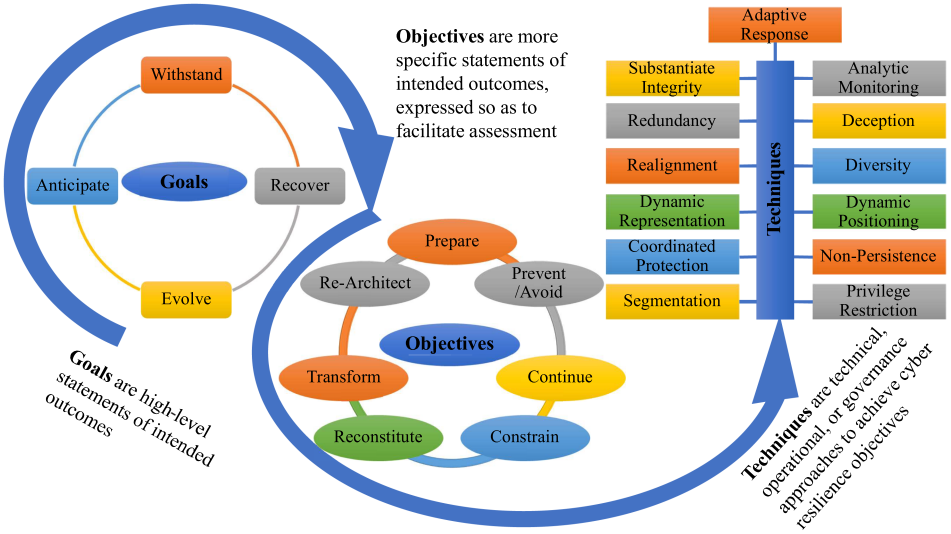

Fig. 3. Cyber resilience engineering framework.

into real-world activities, such as blocking communication between a client and a server. The recommended algorithms are implemented, and they seek to release the same as an open source software framework for simulating resilient cyber systems.

Aoyama et al. [6] presented a framework that includes four categories: (1) effective control, (2) decision and implementation, (3) communication and coordination, and (4) information and management. However, the framework was developed in safety engineering and applies to cyber incident handling. In fact, by considering each incident response task procedure to be one project, with similar projects to be managed, in this case, the situation under cyber-attack can be regarded as a dynamic resource allocation problem.

Khan and Al-shaer [77] proposed an initial version of a formal framework called *CREF*. Their proposed framework provides a comprehensive view of resilience to measure network resilience from various aspects. It covers all metrics from different levels, such as proactive, resistive, and reactive. The CREF is derived from the DREF (Dependability and Resilience Engineering Framework). It is a framework that explains the resilience quantification of communication and IT systems. The CREF is highly generic and can be used at various levels to measure the resilience of network systems. They applied their framework to firewall devices, part of cybersecurity devices, to show their approach's usefulness and practicality.

The framework proposed by Yano et al. [48] for cyber resilience is based on two elements: partitioning the system into different segments and using the kill-chain attack model to structure the defence and adoption of a lifecycle based on the goals that were described in the MITRE framework presented by Bodeau and Graubart [20]. The assets are allocated and prioritised for different segments according to the assimilation strategy that increases situational awareness and emphasises the implementation of situational awareness elements. With these elements, defenders may have a ready view of events and logs in progress and the necessary actions to contain the attacks forcing the least possible damage to the tasks in progress.

Friedberg et al. [52] presented metrics and results for the CRF. The key contributions of their framework are threefold. First, it allows the evaluation of cyber resilience concerning different performance indicators of interest. Second, simplifying the complexities related to performance indicators of importance can be done intentionally. Finally, it supports identifying

reasons for good or poor resilience to improve system design. The presented metric framework provides a scalable system model and a flexible way to measure system resilience numerically.

Nevertheless, it does not come without limitations and challenges. First, the approach aims to describe a single system, which is difficult to define in Cyber-Physical Systems (CPS). Another challenge is framework implementation and evaluation. The information required to build the interdependencies between different features and their respective performance is often unavailable for current CPS installations. The multi-dimensional performance concept makes the framework more generally applicable than the work by Rieger [119], which focuses on control response as a performance measure.

Ayoub et al. [115] outlined some recommendations and pointed out issues that governments might face in building a resilient cybernation. The reason is to devise a range of tools and materials that can adapt to the rapid changes in the digital world. Most governments will probably arm IT with a robust framework to deal with various unforeseen challenges in the future. A structure must be a platform for organisations to share information about actions quickly and collaborate over threat intelligence. This framework will raise awareness of the need to enact any resilience plan and a more proactive response mechanism than cyber-monitoring.

Rose et al. [121] presented a framework for estimating and analysing various types of resilience related to cyber itself and cyber-related sectors. They provided ranges of cost estimates and broad effectiveness of stability set through different syntheses from the academic literature, including industry-specific information. Their analysis indicates that the location of cyber resilience tactics is relatively low in cost, potentially handy, diverse, and quite extensive.

Gisladottir et al. [57] called for a framework or systematic evaluation of risk, rules, and resilience of cyber systems incorporating behavioural sciences. It is partly due to the problem's complexity and the underlying system, including data vulnerabilities, event tracking, software patching, and the interdependence of stakeholders. The need to collect and systematically utilise data from existing systems and establish best practices based on the goals and performance of the optimisation also contributes to the framework's necessity. Selected numbers of well-framed rules are the key to maximising cyber systems' resilience and minimising human factor risks. Also mentioned are two main steps to evaluate the effect of a new rule inside a particular order's security. The first step to the practical application of any development involves the estimation of minimum decision latitude. The second step is to research the methodology to quantify the level of independence employees experience.

Maziku and Shetty [96] discussed achieving cyber resilience in an intelligent grid network with a security score model using a framework of a **Software-Defined Networking (SDN)** for IEC 61850-based substation communication network. The Software-Defined Networking (SDN) framework incorporates SDN principles and the security risk score model leveraged to achieve cyber resilience. They demonstrated how the SDN relieves their intelligent grid network of improvement and excessive timing performance of IEC 61850 type messages, making them time compliant. The security score model will also incorporate the device critically in the IEC 61850 network. They provided the ability to reconfigure the IEC 61850 network in real time by implementing the security score model in SDN. They approve their approach with the estimated model in an experiential **Global Energy Network Institute (GENI)** test outlined by wide-area networks with realistic and dynamic traffic scenarios to address IEC 61850 network attacks.

Kott et al. [81] introduced a CREF that was developed and offered by Bodeau and Graubart [20], which provides an overview of how to structure cyber resilience capabilities by addressing the goals, objectives, and practices in alignment with the "adversary activities" that occur within each ability to reflect the intent and potential actions that the capabilities are intended

Fig. 4. The CRF includes five components: identity, detect, protect, respond, and recover. There are some suitable and popular open source tools for each of these components.

to protect. They discussed the cyber resilience goals and associated objects from the framework [20], which aligns closely with **North Atlantic Treaty Organization (NATO)** cyber resilience goals.

Haque et al. [62] proposed a CRF for the ICS by crumbling the resilience metric into several hierarchy sub-metrics. These metrics were presented as a tree structure that can capture information of a qualitative nature on the system's security posture concerning resilience that a high-level framework to identify where analysis and modelling are needed. Additionally, they show the formalisation of cyber resilience metrics by illustrating resilience metrics calculation using the **Analytical Hierarchy Process (AHP)**. This framework serves as a versatile platform for different criteria-based decision aids, which can help the technical experts identify gaps in the study of ICS resilience.

Dickson and Goodwin [45] emphasised that organisations must build a cyber resilience capability by shortening the lifecycle stages: defence, detection, response, and recovery. They said cyber resilience is a framework designed to help organisations withstand attacks. It is not a single product or layer of protection but a way for organisations to structure their defences so that no one event is destructive. They presented the CRF with five components: identify, protect, detect, respond, and recover, as demonstrated in Figure 4. Similarly, these five components of cyber resilience are discussed by Blum [18].

Intending to aid Small and Medium-sized Enterprises (SMEs) in operationalising cyber resilience, Carías et al. [33] present a framework that SMEs could use to understand what domains and policies are implied in the cyber resilience building process. In addition, the framework has also been presented in the form of an implementation order that SMEs can follow to operationalise cyber resilience based on experts' experience. The main idea of the framework is not to be as specific and exhaustive as possible but to be synthesised and generalist for SMEs to understand what cyber resilience indicates and start implementing it without being crushed. Using the framework and implementation of the order could help SME managers in the process of cyber resilience building by giving them a synthetic tool with the essential actions and an order in which to implement them.

Bejarano et al. [13] review frameworks and standards to achieve cyber resilience in organisations, such as the NIST framework, ENISA (European Union Agency for Cybersecurity), and ISO/IEC 27032. The authors envision a new CRF that leverges **Machine Learning (ML)** techniques to improve business continuity. The National Institute of Standards and Technology (NIST) framework supports five risk management functions: identify, protect, detect, respond, and recover. Machine Learning (ML) algorithms are increasingly used in cybersecurity to detect subtle patterns and handle large volumes of data. Organisations like **ENISA!** (**ENISA!**) help countries better prepare, detect, and respond to information security problems.

These standards raise quality, safety, reliability, efficiency, and interchangeability levels. Resilience is critical for preserving system functionalities and mitigating the consequences of cyber-attacks. Cybersecurity frameworks, standards, and good practices contribute to understanding different types of attacks and managing cyber-attacks. The NIST framework provides a simple, practical framework aligned with guidelines and recommended good practices. Advances in communication technologies and hyper-connectivity drive the need for cyber resilience [13]. The NIST framework is practical and applicable to organisations but requires significant implementation effort. Companies' existing cyber resilience mechanisms require adopting relevant standards, processes, and resources. The work proposes using ML models and techniques to predict and recover from attacks and protect systems promptly.

Hammad et al. [61] propose a framework using **Artificial Intelligence (AI)** based on a hierarchy for cyber resilience in interdependent critical infrastructure systems. The framework identifies, detects, and mitigates cyber and physical attacks through enhanced situational awareness. It focuses on developing an integrated cyber-defence solution to detect and respond to attacks targeting interdependent critical infrastructures. The proposed framework, called *deep defence*, aims to improve system situational awareness through telemetry and events from different domains and layers of the systems. It utilises deep and adversarial ML elements to enhance attack anticipation and response. The framework also emphasises the need for coordinated adaptive-capacity resources on individual and interdependent systems' cyber and physical layers to strengthen resilience. The authors aim to develop a comprehensive approach that can be applied to different interconnected critical infrastructure systems and adapt to the evolving threat landscape.

In today's digital age, cyber threats are becoming more and more prevalent. That is why organisations must have a comprehensive cyber resilience program in place. The Australian Signals Directorate recognised this need and implemented a program that includes vulnerability scanning, patch management, and incident response planning [130]. However, more than these measures are required—they must also be aligned with the organisation's business objectives and priorities. This can often be challenging, but the Australian Signals Directorate has overcome it by creating a risk management framework. This framework helps prioritise resilience against cyber threats, ensuring the organisation is prepared to handle any potential attacks. Organisations can protect themselves against cyber threats and ensure business continuity by following these steps.

Al Maruf et al. [3] proposed a framework that is a timing-based approach for designing cyber resilience in CPS under safety constraints. It aims to ensure the safety of CPS in the face of faults and cyber-attacks. The framework develops a common methodology for safety analysis and computation of control policies and design parameters in CPS employing various resilient architectures. It allows for the comparison of different resilient architectures and enables the extension of analysis and design from one architecture to another. The framework utilises a hybrid system model that captures CPS adopting any of the resilient architectures.

The framework in the work of Al Maruf et al. [3] models the cyber subsystem as operating in a finite number of statuses. It formulates a problem of computing control policies and timing parameters jointly to satisfy a given safety constraint. The derived conditions from the hybrid

system model are used to compute control policies and timing parameters relevant to the employed architecture. The solution provided by the framework can be applied to a wide class of CPS with polynomial dynamics and allows for the incorporation of new architectures. The proposed framework is verified through a case study on adaptive cruise control of vehicles, demonstrating its effectiveness in ensuring cyber resilience in CPS.

PHOENI2X [53] is a project funded by the European Union, which aims to create a CRF for **Operators of Essential Services (OES)** and EU Member State authorities. The framework will be designed to provide AI-assisted orchestration, automation, and response capabilities for business continuity and recovery, incident response, and information exchange. The main objective of the project is to enhance cyber crisis management and resilience by focusing on preparedness, shared situational awareness, and coordinated incident response. PHOENI2X aims to use serious games to raise awareness of social engineering and to improve the ability to detect attacks. The project will integrate different cognitive aspects to provide an effective learning experience. The framework will be tested through use cases in the energy, transport, and health care sectors, highlighting the importance of supply chain aspects and addressing specific threats identified in each domain.

The state level should prioritise developing a shared understanding and terminology of cyber resilience in cyberspace. This lack of clarity is hindering research and policy-making efforts [67]. The concept of cyber resilience gained attention in 2012, focusing on the ability of systems, actors, and functions to prepare for, absorb, recover from, and adapt to adverse effects, including cyber-attacks. However, state-level cyber resilience is still an emerging concept that requires further research and theoretical advancements to avoid vagueness and misuse.

Hubbard [67] proposes a comprehensive conceptual framework for state-level cyber resilience that highlights the dynamic nature of resilience, the presence of resilience capacities at various levels and across actors within the state, and the need to confront and recover from specific types of cyber damage. The framework aims to establish a common terminology and promote a systematic, multi-dimensional approach to assessing and improving states' capacity for resilience in cyberspace.

The identity stage recommends using security scanner tools. N-Stalker [101] is one of the popular security scanner tools; it is a web security assessment tool. It allows scanning web applications against buffer overflow, SQL XSS injection, and SQL infusion blemishes. N-Stalker is a helpful security tool for IT auditors, developers, system/security administrators, and IT experts. The detection stage involves security monitoring, and a powerful tool for this stage is OSSEC [109]. OSSEC is open source, free, and multi-platform. OSSEC is a security tool that, through its comprehensive course of action, decides, including custom alert principles, while creating resources to make a move when alerts occur.

The protection stage that defines access control, data security, and information protection needs a specific tool to complete. The most popular tool for this stage is GnuPG [131]. GnuPG is a comprehensive and free tool that executes the OpenPGP standard characterised by RFC4880 (otherwise called *PGP*). GnuPG encodes information and correspondences; it consists of a flexible fundamental administration framework alongside modules for a wide range of vital open indexes. GnuPG, or GPG, is an order line device with highlights for a simple combination of different applications. An abundance of front-end applications and libraries are accessible. GnuPG likewise offers help for **Secure/Multipurpose Internet Mail Extensions (S/MIME)** and **Secure Shell (SSH)**.

The response stage responds to planning and analysis of the events and logs, with the famous and suitable tool for this stage being the Apache Metron tool [7]. Apache Metron gives an adaptable, propelled security investigation system developed with the Hadoop Community from the Cisco OpenSOC Project. A digital security application structure allows associations to distinguish digital irregularities and empowers associations to react to recognised inconsistencies quickly.

Table 4. Cyber Resilience Strategies That Are Implemented in Some Application Domains Such as Supply Chain, Cyber Defence, SCADA System, Cyber Warfare, and Industrial IoT

Authors	Year	Application Domains	Effectiveness	Strategic Acceptability	Cost	Quality	Flexibility	Advantages	Disadvantages
Urciuoli [139]	2015	Supply chain	👍	👎	◐	◐	◐	Easy online control and management	It is not fully integrated and accepted into all supply chain companies
Efthymiopoulos [49]	2016	Cyber defence	👍	👍	●	●	●	Incorporates strategic and operational perspectives	Requires many infrastructure configurations
Conklin [39]	2017	SCADA system	👍	👎	○	◐	○	An H-level approach in the form of principles	Only applicable to SCADA systems
Tehrani [132]	2019	Cyberwarfare	👍	👍	◐	◐	●	The strategy is powerful for highly developed and connected countries, such as the United States and the UK	Only considers protecting critical infrastructure
Carías et al. [34]	2019	Industrial IoT	👍	👍	○	●	●	Quite a feasible approach	Considers only professional security and training/awareness
Rahman et al. [116]	2021	Supply chain	👍	👍	●	●	●	It utilises a data fusion technique and the Dempster-Shafer theory	The proposed methodology of the strategy requires expert judgments
Yao et al. [146]	2023	Microgrid (MG)	👍	👍	●	●	○	It enhances the system's ability to withstand such attacks	It is appropriate for MG systems only

👍=Yes, 👎=No, ○=Low, ◐=Medium, and ●=High

The recovery stage will return to ordinary tasks and many tools available for backup and recovery, but the popularity lies with the Bacula tool [120]. It has had many open source tools for recovery and personal computer programs that grant the framework director to oversee reinforcement, recuperation, and check for personal computer information through various types along with the system. Bacula's free information reinforcement programming is generally simple to utilise and exceptionally useful while offering many propelled stockpiling executives that make it simple to discover and recoup lost or harmed records.

Limited research has addressed the existing challenges faced by CRFs will help the cybersecurity community collaborate on improving current Cyber Resilience Framework (CRF)s. Furthermore, they will assist the cybersecurity community in identifying organisations, universities, and people working on designing and developing CRFs [125].

4 CYBER RESILIENCE STRATEGIES

In this section, we compare and discuss different cyber resilience strategies. Cyber resilience strategies refer to the actions and measures taken by organisations to prepare for, respond to, and recover from cyber-attacks. Strategies can include technical measures, such as implementing firewalls and encryption, as well as non-technical measures, such as employee training and awareness programs. Effective cyber resilience strategies are critical in mitigating the impact of cyber-attacks and ensuring that organisations can continue to operate in the face of cyber threats. We present comparisons within these strategies, as seen in Table 4. Cyber resilience can be achieved by applying strategies based on principles [39, 132] and investment [34].

A great deal of previous research into cyber resilience strategy with the supply chain has focused on management strategies to improve cyber resilience, thereby pointing out how the strategy can be automated using innovative **Information and Communications Technology (ICT)** systems [139]. The Information and Communications Technologies (ICT) has already indicated playing a significant role in managing and controlling the value of a complex network. However, additional ICT capabilities, mainly aiming for improving cyber resilience, may be exploited in supply chains to ensure quick response to disruptions and risks within a short time.

These capabilities support joint development, repository IT ecosystems where B2B (Business 2 Business) or B2G (Business 2 Government) both push and pull the different web services of contemporary to be created by an actor of the supply chain and governmental agencies. Enabling **B2B!** (**B2B!**) and **B2G!** (**B2G!**) data sharing will allow companies to access an unimaginable amount of data and services that can enhance and improve the whole supply chain's cyber resilience. For example, organisations will be able to control and manage suppliers and portfolios online quickly, making more accurate **Estimated Time of Arrival (ETA)** estimations to monitor the transport infrastructure capacity in real time. Likewise, it would be easier for organisations to rapidly learn and apply any sudden changes in trading regulations while complying with regulatory frameworks.

One study by Efthymiopoulos [49] examined the trend of cyber resilience strategy in cyber defence. It included the importance of cyber resilience during the North Atlantic Treaty Organisation (NATO) strategic evaluation. This aims to approach and integrate the NATO collective defence methodologically. Additionally, it discusses the technological assessment of NATO, implying strategic and operational changes for all alliances. It will be operating strategically and operationally while considering different challenges and threats. NATO reviews cyber resilience as a tendency for building capabilities wherein fields include, but are not limited to, training/awareness/education, network protection infrastructure, systems configuration, and infrastructure protection, among others.

The first systematic study of cyber resilience strategy as principles was reported by Conklin [39] in 2017 for a cost-efficient approach and sufficient to protect the critical systems that power the way of our life. They offer pedagogy for disseminating and a staged approach to implementing cyber resilience policies and a general curriculum. A cyber resilience strategy is maintaining functionality at all costs without considering defending outside elements or lesser critical ones. They explained the cyber resilience strategy into seven principles: classify, risk, rank, deploy, test, recover, and evolve. The organisation implementing a cyber resilience strategy will give them more ability to withstand and recover rapidly from disruptive events.

In 2019, Tehrani [132] presented another cyber resilience strategy as principles that discussed and illuminated the underlying national critical infrastructure defence principles integrated with cyber warfare. The discussion showed how to establish cyber resilience policies to face growing and new threats. Likewise, they demonstrated how states might use the attribution concept and its applicability to deal with actors behind malicious cyber activities. In other words, it examined the issue of the applicability of international rules and attribution regulations to state and non-state actors for malicious cyber activities in the attribution context.

A detailed examination of cyber resilience strategy by Carías et al. [34] showed a road map for building cyber resilience using an efficient investment strategy. To achieve this, the system dynamics methodology will be followed to get experts' opinions on the best approach to supporting cyber resilience. Cyber resilience experts must use technology and personal training, and neither should be overlooked as an investment strategy. This strategy will be helpful to factories in minimising the probability of any cyber-attack efficiently. Factory managers can use their model as a decision-making tool because it shows the behaviour of main variables that are

not easily quantifiable in simple graphs. Therefore, this model could be a helpful tool in a factory manager's decision-making process to develop strategies for enhancing cyber resilience.

An excellent strategy is to enable cyber resilience in SMEs based on a few simple steps as part of the new digital world. Those few steps can be summarised into seven steps [91] that can pave the way for SMEs to cyber resilience. These seven steps are (1) invest in effective antivirus, anti-malware, and firewall solutions; (2) ensure the critical data of the business is protected; (3) have clear and simple policies in place; (4) have awareness training regularly; (5) review policies and contracts with suppliers; (6) have an up-to-date plan for incident response; and (7) consider investing in cyber insurance for covering the disclosure of security and data privacy incidents.

One of the strategic decision-making frameworks for assessing the cyber resilience of additive manufacturing supply chains was proposed by Rahman et al. [116]. The strategy framework utilises a data fusion technique called the *hierarchical evidential reasoning based approach*, which handles the data's incomplete, uncertain, and subjective nature. The strategy is based on the Dempster Shafer theory and incorporates Yager's recursive rule of combination for validation.

The assessment process essential criteria (factors) are aggregated by Rahman et al. [116] to obtain a Cyber Resilience Index using the Dempster Shafer combination rule. Based on their experience, knowledge, and education, the subjective data experts used to evaluate the cyber resilience attributes. The strategy allows for a holistic assessment of the cyber resilience of additive manufacturing supply chains, considering both cyber structures and organisation-wide operations. Practitioners can adopt the proposed methodology to assess the condition state of cyber resilience and compare multiple organisations' cyber resilience.

One of the cyber-resilient control strategies proposed is to enhance the cyber resilience of **Microgrid (MG)** systems and restore cyber connectivity after **Denial of Service (DoS)** and latency attacks presented by Yao et al. [146]. The strategy consists of two control modes. The adaptive-gain resilient controller's first model is designed to sustain the fast stabilisation of Microgrid (MG) systems under non-uniform time-varying latency attacks. It is proved by the stochastic stability analysis using the Lyapunov-Krasovskii functional method.

The ETTR (Event-Trigger Topology Reconfiguration) controller [146] is a model designed to mitigate excessive latency and connectivity issues resulting from Denial of Service (DoS) attacks. The **ETTR!** (**ETTR!**) controller optimally reestablishes the damaged cyber topology and restores the destroyed control objective under DoS attacks, such as accurate power sharing. A switching mechanism is also designed to coordinate the preceding control modes to guarantee the secondary control functions of MG systems. The proposed control strategy provides a systematic control framework for the complicated MG scenario under both attacks with sufficient stability and optimal cyber performance.

The U.S. **Department of Defense (DoD)** has been taking proactive measures to ensure its cyber resilience systems are robust against potential cyber-attacks [40]. One of the main aspects of this effort involves implementing a cyber resilience strategy program that includes network segmentation, multi-factor authentication, and continuous monitoring. However, integrating these measures with the existing systems and processes has proven challenging.

A step-by-step implementation strategy was developed by De Cristofaro et al. [44] to address this issue, which involves rigorous testing and validation before full deployment. This approach is crucial to ensuring that the cyber resilience measures effectively protect against potential threats. The Department of Defense (DoD)'s commitment to cybersecurity is commendable, and its efforts serve as a model for other organisations looking to strengthen their cybersecurity systems. By prioritising cyber resilience, the DoD is taking a proactive stance against threats that could compromise national security and the safety of its personnel.

5 RECENT ADVANCEMENTS IN CYBER RESILIENCE

In this section, we introduce techniques to improve and increase cyber resilience. Additionally, we compare different cyber resilience improvements, as seen in Table 5. Recent advancements in cyber resilience have come in multiple forms, such as based on recommendations [58], based on best practices and standards [129], and based on using technologies [111] to improve cyber resilience or based on multiple factors [90].

Several examined the advancements in cyber resilience, but the first one by Partridge and Young [76] presented the CERT-RMM applicable in organisations. The model allows its adopter's continuity in using preferred codes and standards of practice at a tactical level that improves the management of operational cyber resilience at the process level. This technique shows the areas of overlap and redundancy between Computer Emergency Response Team (CERT)-Resilience Management Model (RMM) process areas and the guidance in the NIST discussed in the work of Mylrea et al. [100], and it also identifies the gaps that may affect the maturity of practice. It aligns the tactical practices suggested in the NIST publications to the process areas that represent operational resilience management at a process level.

One of the cyber resilience improvement studies to the supply chain was established by Goldman et al. [58], which presented several approaches to improve cyber resilience and described an application scenario. They mentioned techniques that did not apply to all systems. However, to begin building cyber resilience into existing or appearing systems, the designers must analyse which strategies are most suitable for the environments and missions. Furthermore, they focused on actionable operation and architectural recommendations to enable mission assurance and address advanced critical services threats. These recommendations can create improvements leading to a transformation with minimal impact on essential functions, acting as a deterrent, reversing adversary advantage, and increasing adversary cost and uncertainty.

Bodeau and Graubart [21] discussed a general assessment approach to cyber resilience and improved the recommendations with architectural evolution and process improvement to make more productive use of cyber resilience practices. They focused on resilience assessment for family systems, system-of-systems, mission/business segments, or common infrastructures. The advantage of their approach is that it can also be applied to components, services, and individual systems. Moreover, the method can be applied as a built-in architecture or an operational where the emphasis may be on either "low-hanging fruit" or opportunities for high-leverage improvements while using a few numbers of cyber resilience techniques.

The organisation has many steps to improve cyber resilience, but we will demonstrate the five main phases. At first, while initiating a discussion about cyber resilience, it is critical to be aware of its executive management. Second, finding the right balance between corrective controls, detective, and prevention is vital. Third, making the right balance between technical rules, processes, and people is required. Fourth, implementing best practices and standards in the organisation, such as **ISO/IEC 27001!** (**ISO/IEC 27001!**) and AXELOS cyber resilience best practice guide, must be carried out. Finally, testing and keeping the organisation up to date with new cyber-attacks will ensure cyber resilience is under control and working properly [129].

One of the manageability implementations for improving the cyber resilience and risk management processes of SMEs is proposed by Nykänen and Kärkkäinen [106]. They presented the semantic wiki as a platform for information security knowledge. They introduced traditional information security based on **Confidentiality, Integrity, and Availability (CIA)** properties to control the catalogue to select appropriate controls from availability viewpoints. Suppose we wish to focus on the authorities and resilience. Then, in this case, they must be using the NIST SP 800-53 control catalogue, including 115 low controls, with only 87 of these on level one as expected

Table 5. Most Recent Advancements in Cyber Resilience Either at the Organisation Level or Specific to Applications Such as Supply Chain, Cyber Systems, Cyber-Attack Mitigation, Cyber Defence, and ICS

Approach	Year	Makes Improvements in	Organisational Management	Operational Management	Provides Recommendations	Based on Standards	Uses Technologies	Improvement Cost	Performance after Improvement	Advantages	Disadvantages
Partridge and Young [76]	2011	Organisation	👎	👍	👎	👍	👎	○	○	It shows the gaps that may affect the maturity of practices to improvements	It is very complicated, as it has several vital components
Goldman et al. [58]	2011	Supply chain	👍	👍	👍	👎	👎	○	◐	It is low cost, as it builds resilience into existing infrastructure; the approach does not require a new one	Built-in existing infrastructure will make attacks more likely to succeed, and will increase the consequences
Bodeau and Graubart [21]	2013	Cyber systems	👎	👍	👍	👎	👎	○	●	It can be applied to various categories, such as components, services, and individual systems	It is very hard and costly because it should be applied to various levels of the infrastructure
Rance [129]	2014	Organisation	👍	👎	👍	👍	👎	●	●	More than one standard	Scope of implementation is complex
Nykänen and Kärkkäinen [106]	2016	Organisation	👍	👎	👎	👍	👎	◐	○	Easy implementation	Not useful for big organisations
Aguilera [145]	2017	Cyber-attack mitigation	👎	👍	👍	👎	👍	●	●	By using technology, it can perform stateful recovery fast with minimal overheads	Requires multiple configuration steps to implement
Galinec and Steingartner [54]	2017	Cyber defence	👎	👍	👎	👎	👍	●	◐	Powerful for all levels of hierarchy in military systems	It is not useful to implement inside a small organisation
Li et al. [86]	2018	Industrial Control Systems (ICS)	👎	👍	👎	👎	👍	●	●	It can be reduced if assigning various products to a pair of connected hosts	Not useful for large organisations
Bissel et al. [75]	2018	Organisation	👍	👍	👍	👎	👍	●	●	Compatible with organisational and operational parts	Requires a long time for implementation
Linkov and Kott [90]	2019	Organisation	👍	👎	👎	👎	👎	◐	◐	Can deal with complex situations	Only beneficial for small organisations
Ponemon Institute [69]	2019	Organisation	👍	👍	👍	👎	👍	●	●	Compatible with different industries and sectors	Costly because it involves multiple technologies
Ahmed et al. [2]	2020	Mobile Field Hospitals (MFHs)	👍	👍	👎	👍	👍	●	●	Provides a standardised framework for assessing and managing cyber resilience in MFHs	Implementation may involve costs for developing the assessment framework
Qu et al. [114]	2020	Software-Defined Networking (SDN)	👎	👍	👎	👎	👍	●	◐	The use of SDN allows for efficient network control	It is costly to implement
Dacorogna et al. [41]	2023	Risk management	👍	👍	👎	👍	👍	●	●	Classification attack can help in identifying different types of cyber-attacks and developing targeted strategies to mitigate them	The configuration is very complex and challenging for non-experts
Kim and Kim [78]	2023	Blockchain	👎	👍	👎	👍	👍	◐	●	The blockchain-based NSCC system is found to be time- and cost-efficient compared to the current customs clearance system	The blockchain-based NSCC system is still vulnerable to APT and network attacks aimed at legacy systems

👍=Yes, 👎=No, ○=Low, ◐=Medium, and ●=High

to implement it in all information systems in the first phase. The number of authorities can also reduce this first power phase in their classifications to 50 only.

A recent study by Aguilera [145] has shown improved cyber resilience to overcome cyber-attacks using the Flooid resilience platform. Their resilience platform is designed to manage and orchestrate the container lifecycle while applying cyber resilience techniques and enforcing security. Flooid allows for deploying an application, executing its security, and returning the system to a specific state in case of a cyber-attack. They presented Flooid's strategy to decrease the number of threats through the most common vulnerabilities, such as new code, inner-container attacks, cross-container attacks, container escaping, and resource consumption. They proved that Flooid could perform stateful recovery with minimal overhead. The recovery strategy includes container rollback, cloning, or live migration. They found that the performance of their approach is up to four times faster due to less information transmitted relative to the traditional procedure to reinstate the steady state.

Galinec and Steingartner [54] undertook the preliminary work on advancing cyber resilience in cyber defence. The study investigated how cyber defence and cybersecurity can be combined to increase cyber resilience while describing cybersecurity relations, IT security, operational technology security, information security, and other related disciplines and practices within cyber defence. Exploring new techniques and standards for achieving cyber resilience is necessary, particularly in light of emerging cyber-attacks.

Li et al. [86] introduced the metric of similarity to capture how similar vulnerabilities between two different products are by applying it in a statistical study on databases of **Common Vulnerabilities and Exposure (CVE)/National Vulnerability Database (NVD)**. They showed that multiple products could result from most vulnerabilities, even from other vendors. The similarity metric can estimate the probability of a zero-day to exploit successful self-propagation between two different products. Such propagation can be effectively reduced by assigning various effects to a pair of connected hosts.

A high-performance post-implementation of cyber resilience in any organisation requires five steps to attain augmented performance. The first step builds on a solid foundation of protecting and hardening core assets. The second step performs a pressure test to identify the resistance via coached incident simulation. The third step applies automated defence technologies such as automated orchestration capabilities and advanced identity access management. The fourth step uses data and intelligence for proactive threat hunting, such as implementing strategy and providing tactical knowledge of the threat. Last but not least, evolving chief information security officer roles in business leadership means that the next generation such officers should be business adept and tech-savvy [75].

Linkov and Kott [90] discussed the resilience of a system, an organisation, and a network, considering several factors in an often complex and contradictory manner, enhancing the stability and improving cyber resilience. These factors are managed based on complexity, chosen topology, added resources, design for reversibility, control propagation, provided buffering, prepared active agents, built agents capabilities, considered adversary, and the conducted analysis.

The Ponemon Institute [69] presented the importance of improving cyber resilience to ensure a strong security position. They highlighted the importance of automation for cyber resilience. Automation allows security technologies that replace or increase intervention to contain and identify breaches or cyber exploits. Such technologies depend on Artificial Intelligence (AI), orchestration, analytics, and ML. They have shown improvements with some recommendations for achieving a more substantial cyber resilience level, such as investing in automation, hiring a skilled workforce, participating in threat intelligence, considering a valuable and integral, aligning privacy and cybersecurity, and using key metrics for measuring cyber resilience.

Baykara and Das [12] propose a honeypot-based approach for **Intrusion Detection and Prevention Systems (ID/PS)** that can detect zero-day attacks and reduce false positives in Intrusion Detection Systems (IDS). This system can help improve organisations' cyber resilience by providing an additional security layer to their information systems. Using virtualisation technologies can also reduce the cost of configuration, maintenance, and management. Therefore, the study's proposed system is a potential solution for enhancing organisations' cyber resilience.

In the study conducted by Ahmed et al. [2], a notable advancement in cyber resilience pertains to evaluating cyber resilience within field hospitals, aligning with the burgeoning trends in the field hospital domain and the broader health sector. This evolving landscape introduces potential vulnerabilities that malicious actors could exploit, underscoring the need to enhance response strategies to achieve robust cyber resilience. The assessments conducted in this context serve a dual purpose: they inform users and stakeholders about the extent of risks surrounding the hospital's cyber assets and shed light on the avenues through which threat vectors could manifest. This approach starkly contrasts prevailing practices that assess the cyber assets of mobile field hospitals, illustrating a shift towards recognising and mitigating potential vulnerabilities.

To bolster the cyber resilience of Phasor Measurement Unit networks against malicious assaults and system anomalies, Qu et al. [114] devised an optimisation-centered approach for network management. This approach capitalises on the SDN communication framework to facilitate the reinstatement of the Phasor Measurement Unit connectivity and reestablish observability within power systems. Their scheme facilitates swift network recovery by optimising the path generation and installation procedure while streamlining the SDN rule implementation on switches. This effort has culminated in creating a functional prototype system through which the authors gauged power system observability, recovery speed, and the efficiency of rule compression. Their evaluation hinged on the IEEE 30-bus system and the IEEE 118-bus system.

A new algorithm for modelling heavy-tailed data to understand cyber risks better and improve cyber resilience was proposed by Dacorogna et al. [41]. Using this algorithm, the authors analyse a database of cyber complaints filed at the Gendarmerie Nationale, which reasonably estimates the whole distribution, including the tail. The study confirms the finiteness of the loss expectation, a necessary condition for insurability. The authors draw the consequences of this model for risk management, then compare its results to other standard EVT models, and lay the ground for the classification of attacks based on the fatness of the tail. The study aims to contribute to understanding cyber risks and improving cyber resilience in modern economies.

Kim and Kim [78] propose a blockchain-based **Non-Stop Customs Clearance (NSCC)** system for cross-border trains. The proposed system addresses delays and resource consumption issues caused by customs clearance processes. The purpose of the proposed system is to create an NSCC process for cross-border trains, reducing delays and resource consumption associated with traditional customs clearance systems. The proposed system uses a blockchain network to connect various trade and customs clearance agreements. This integration ensures the integrity and minimal resource consumption of the system.

The system proposed in the work of Kim and Kim [78] includes various participants, such as railroads, freight vehicles, transit stations, and the existing customs clearance system. The proposed system utilises sequence diagrams and blockchain technology to protect customs clearance data's confidentiality and integrity. The article demonstrates the structural attack resilience of the proposed system using a blockchain, a consensus algorithm, and an attack sequence diagram created with MITRE ATT&CK. This approach strengthens the system's ability to withstand attacks. The results show that the blockchain-based Non-Stop Customs Clearance (NSCC) system is time- and cost-efficient compared to the current customs clearance system. The proposed system offers improved cyber resilience attacks, making it more secure and reliable.

Table 6. Popular Tools and Technologies Used to Improve or Evaluate Cyber Resilience from 2011 to 2020

Tool	Year	Brief Description	Organisational Management	Operational Management	Ease-of-Use	Web Based	Efficient	Software Based	Open Source	Cost	Performance	Uses Database	Paths to Improvements	Strengths	Weaknesses
Cyber Resilience Review (CRR) [107]	2011	CRR tool helps evaluate operational resilience within critical resources and critical infrastructures at the organisation	👍	👎	👍	👎	👎	👍	👎	○	○	👎	👎	The final report comprehensively maps the organisational resilience to different domains	The tool is not useful for a technical assessment of cyber resilience
C-suite Checklist Tool [144]	2012	Simple checklist tool for helping internal review of the organisation for analysing capabilities of cyber resilience	👍	👎	👍	👎	👎	👍	👎	○	○	👎	👍	The tool helps identify specific strengths and weaknesses	The result of the tool does not reflect an accurate situation of the organisation
CyGraph [103]	2017	It provides reactive and proactive cyber resilience	👎	👍	👍	👎	👍	👍	👎	◐	●	👍	👍	Uses a database while making the technology readily accessible to analyse in the future	CyGraph only supports NoSQL database technology, to store and process resilience knowledge
Joint User cyber Mission Planning (JUMP) application for cyber resilience [46]	2017	It has the ability to show the concept demonstration environment to check activities in cyberspace, for analysing cyber resilience	👎	👍	👎	👍	👍	👍	👎	●	◐	👍	👍	It shows interactive exploration of a network that will help analysts with cyber resilience simulations	The JUMP cyber analyst screen provides graph-based analysis that is not easy to understand
Byzantine Fault Tolerant++ Technology (BFT++) [97]	2019	BFT++ is the first known approach in CPS to improve cyber resilience	👎	👍	👍	👎	👍	👍	👎	●	●	👎	👎	It uses triple redundancy and artificial software diversity that will improve cyber resilience and is more powerful	The redundancy aspect in the BFT++ architecture makes it more challenging to implement
Cyber Resilience Assessment Tool (CRAT) [63]	2019	The CRAT tool is useful to guide ICS operators in improving cyber resilience of the ICS network	👎	👎	👍	👎	👍	👍	👎	◐	●	👍	👍	CRAT can generate cyber resilience metrics based on the ICS CRF	It is only useful for ICS networks
Cyber Resilience Progression Model [32]	2020	The model is a tool that helps companies prioritise and strategise the implementation of cyber resilience policies over time	👍	👍	👍	👎	👍	👍	👎	◐	●	👍	👍	Its based on semi-structured interviews and data analysis, ensuring that it is grounded in reality and aligned with current research in the field	Its effectiveness may vary depending on the specific needs and characteristics of each company

👍=Yes, 👎=No, ○=Low, ◐=Medium, and ●=High

6 CYBER RESILIENCE TOOLS AND TECHNOLOGIES

This section reviews additional tools and technologies developed to evaluate and improve cyber resilience. This section first compares and discusses various tools and technologies used for cyber resilience, including **Cyber Resilience Review (CRR)**, C-suite Checklist, CyGraph, **Joint User cyber Mission Planning (JUMP)**, **Byzantine Fault Tolerant++ (BFT++)**, and **Cyber Resilience Assessment Tool (CRAT)**. We describe them individually and showcase their comparison under a few criteria, as demonstrated in Table 6.

The comparison criteria refer to the capability of tools or technologies, such as easy to use, web-based, efficient, software based, open source, cost, performance, uses a database, and supports the organisation's management operational perspective. Cyber resilience tools and technologies

are the software components organisations use to implement their cyber resilience strategies. These can include firewalls, encryption technologies, and backup and recovery systems. Practical cyber resilience tools and technologies are critical in protecting organisations from cyber threats and ensuring they can recover quickly during attacks.

6.1 Cyber Resilience Review Tool

Cyber Resilience Review (CRR) is a tool for reviewing the cyber resilience organisations offered by the **Department of Homeland Security (DHS)** on a voluntary, without any cost, basis to critical infrastructure organisations and state, tribal, local, and territorial governments. The CRR is granted by cybersecurity advisors who are regionally located. Additionally, the CRR offers insights into the resilience of an organisation's operational and cybersecurity capabilities. The CRR approach is derived from the CERT-RMM by Carnegie Mellon University's Software Engineering Institute and developed by a process improvement model for managing operational cyber resilience. The CRR is based on deploying organisational assets (information, people, facilities, and technology) for critical services and products. The CRR evaluates the capacities and capabilities in defining, planning, managing, measuring, and performing cybersecurity capabilities across 10 domains [107].

6.2 C-suite Checklist Tool

The C-suite checklist tool is a simple tool presented by **World Economic Forum (WEF)** for chief executives and other C-suite executives to help the internal reviewer of the organisations for analysing cyber resilience. The device can provide intended executives with specific and generic information to inform organisations of their actions. After answering all questions, it also provides a rough composite score to locate the organisation with a hyperconnection readiness curve. The questions asked in the tool can help executives identify specific weaknesses and strengths and show paths for improving cyber resilience within their respective organisations [144].

6.3 CyGraph Tool

The CyGraph tool is used for system improvements for network security posture while maintaining situational awareness in the face of cyber-attacks and protecting mission-critical assets and services. CyGraph raises a unified graph-based cybersecurity model relevant to actual and potential cyber-attacks, mission impacts, and defences. It can capture incremental attack vulnerability, events, security, and mission dependencies within a network environment, creating an imminent model of possible attacks and critical vulnerabilities while correlating events to a known exposure. Additionally, it includes dependencies among network assets and mission requirements for analysis in the mission context assurance [104].

Noel et al. [103] described the application of MITRE's CyGraph as a tool for reactive and proactive cyber resilience. Using a multi-relational graph formalism, CyGraph can combine data from numerous sources to build a unified graphical representation of network infrastructure, cyber-attacks/threats, security posture, and mission dependencies, as illustrated in Figure 5 and explained in the work of Noel et al. [103]. The CyGraph tool of resilience knowledge base associates risky network traffic paths, including traffic filtering rules and devices that allow reactive mitigation and proactive remediation. CyGraph uses **Not Only SQL (NoSQL)** database technology to store and process the resilience knowledge base at scale, including domain-specific language query that exposes the reachability by multi-steps from threats to vulnerable hosts and critical cyber assets.

6.4 Cyber Mission Planning Application for Cyber Resilience

Dudman et al. [46] presented this tool to show the concept demonstration environment of cyberspace activities for analysing cyber resilience. Additionally, it provided cyber resilience

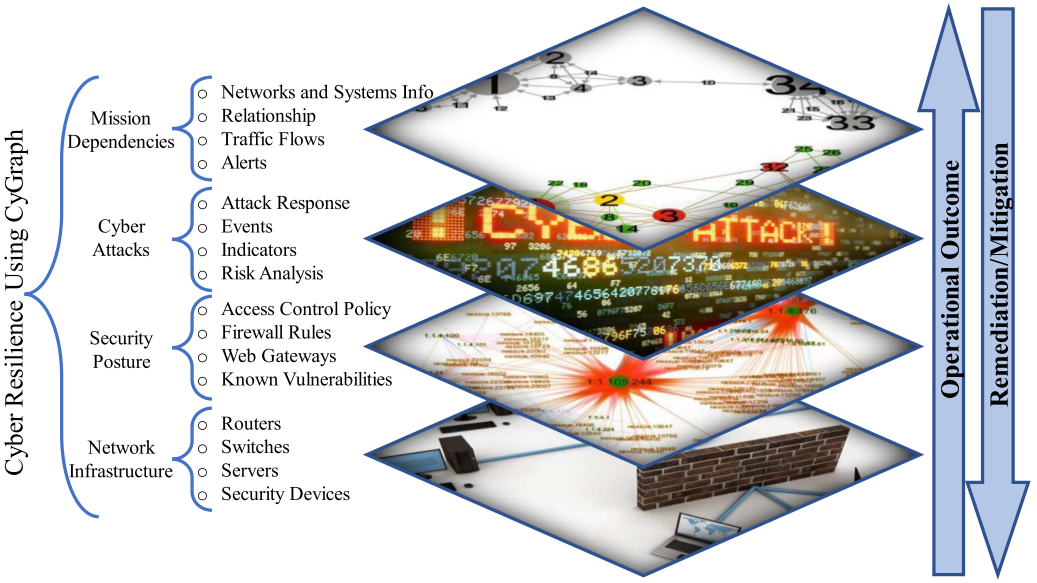

Fig. 5. CyGraph enhances cyber resilience, which has knowledge layers, including network infrastructure, security posture, cyber-attacks/cyber threats, and mission dependencies.

information using a separate Joint User Cyber Mission Planning (JUMP) application screen for cyber analysts. It allows cyber analysts to understand the impact of air, land, and sea activities on cyberspace for various offensive and defensive joint force missions using interactive visualisations and state-of-the-art analysis algorithms. The highly interactive visual analysis is powered by leading industry on open source technologies, including Facebook's React Framework [51], Bootstrap [15], and Data-Driven Documents [25]. The cyber analyst's **Graphical User Interface (GUI)** supports topological editing of the mission vignette to allow viewing of interactive exploration of cyber resilience simulation, assignment of network threats, data analytics, and network vulnerabilities. It also enables cyber-attack mitigation by hardening the network or patching critical vulnerabilities to be assessed and staged.

6.5 Byzantine Fault Tolerant++ Technology

Mertoguno et al. [97] presented Byzantine Fault Tolerant++ (BFT++), which is the first known developmental approach for cyber resilience, particularly for attack resilience in CPS. BFT++ accomplishes the recovery of automated controllers from an attack state to a known-good state, a real achievement in a system with a known vulnerability. The approach supports a full legacy of CPS implementations. Generally, it works for any system that establishes a connection with a periodic set of tasks and can tolerate some inactive epochs in the end loop.

6.6 Cyber Resilience Assessment Tool

CRAT is a new simulation tool for evaluating cyber resilience in ICS. They provide several simulation outputs that can allow an understanding of the rationale and extent to which the CRAT can give a realistic assessment of the ICS cyber resilience. Further, they offer a simulation of the system architecture engine and tool validation that provides valuable insights into the cyber resilience assessment [63].

There are some new technologies beyond what we discussed in this section. For example, Dickson and Goodwin [45] presented and described five key technologies an organisation can

implement to address the potential business disruption from a cyber-attack. Those five technologies are instrumental in allowing organisations to create the best environment for resilience. We summarise them as follows: (1) orchestration for recovery of both platforms and application data, (2) air-gapped protection, (3) read many and write once by utilising immutable storage technology to prevent deletion or corruption, (4) data verification and efficient point in time for copying the data to be able to identify the recoverable data quickly, and (5) regulatory assurances and reporting.

6.7 Cyber Resilience Progression Model

Cyber resilience is crucial in the current hazardous cyber environment, as companies risk cyber incidents. However, the existing literature on cyber resilience needs more guidance on prioritising and strategising the implementation of policies. Carías et al. [32] propose a progression model to help companies prioritise and strategise cyber resilience policies based on their natural evolution over time. The model was developed through semi-structured interviews and data analysis.

The progression model for asset management policies includes stages such as listing company assets, performing corrective and preventive maintenance, and enhancing asset information in the inventory. The evolution of policies in the model allows for a realistic view of their progression, considering the company's capacities at different maturity levels. Information security policies in the model have a technological progression, as agreed upon by experts. Risk management policies in the model should be started from level 2, based on consensus among experts.

The proposed progression model can serve as a tool for companies to implement cyber resilience policies effectively. The model gives companies a roadmap to prioritise and strategies for implementing these policies over time. It helps companies understand the natural evolution of each approach and provides insights on how to progress from one maturity level to another. The model complements the existing literature on cyber resilience operationalisation by offering concrete descriptions and guidelines for companies to follow.

It can be particularly beneficial for SMEs or companies with low experience levels in cyber resilience, as it reduces the need for extensive knowledge and experience to implement these policies. However, it is essential to note that the model should be followed promptly, as circumstances and context must be considered in decision-making processes. The progression model presented in the study is grounded in reality and based on expert insights, making it a valuable starting point for companies to improve their cyber resilience capabilities.

7 THREAT MODELLING FOR CYBER RESILIENCE

Threat modelling is one of the approaches for identifying security requirements to design the systems correctly and securely [117]. Threat modelling makes it possible to identify all potential threats to the systems and therefore assists system designers in considering the mitigation and making their design more secure and reliable. A threat model covers policies against various security threats and possible mitigation strategies [60]. The primary purpose of a threat model is to facilitate awareness and identification of all possible threat scenarios that may be applicable in a specific context. Threat modelling can help identify, classify, and describe threats [98].

Threat modelling finds application in two main ways: first, as an assessment tool to evaluate the existing state of a system, and second, as a security-by-design instrument during the development of novel approaches [141]. These models can be employed as inputs for running attack simulations, a technique that delves into the actions of potential attackers within the system. By leveraging the outcomes of these simulations, stakeholders can delve into security scenarios, enabling them to identify and implement measures more efficiently to fortify the security of their systems.

Several popular threat modelling methodologies summarised in Table 7 are classified based on the volume of data. Some of these methodologies are suitable for cyber resilience, such

Table 7. Threat Modelling Methodologies and Suitability for Cyber Resilience

Threat Modelling Methodology	Year	Description	Suitable for Cyber Resilience	Reason
OCTAVE [4]	2003	It is the first threat modelling methodology created specifically for cybersecurity	👎	It is primarily for risk management in the organisation
Trike [124]	2005	It is an open source tool focused on security auditing	👎	Trike modelling is especially for cybersecurity but not cyber resilience
STRIDE [133]	2014	STRIDE is designed by Microsoft to be helpful for Windows software developers	👍	It is robust for planning and adapting cyber resilience
PASTA [137]	2015	The output of PASTA includes scoring, enumeration, and threat management	👍	PASTA modelling increases the adaptation phase of cyber resilience
DREAD [105]	2020	This modelling is powerful for quantifying and prioritising the amount of risk	👍	It may be useful for quantifying cyber resilience
VAST [1]	2020	VAST generates useful outputs for security teams, senior executives, and developers	👎	VAST modelling works as dataflow information only
👍=Suitable and 👎=Not Suitable				

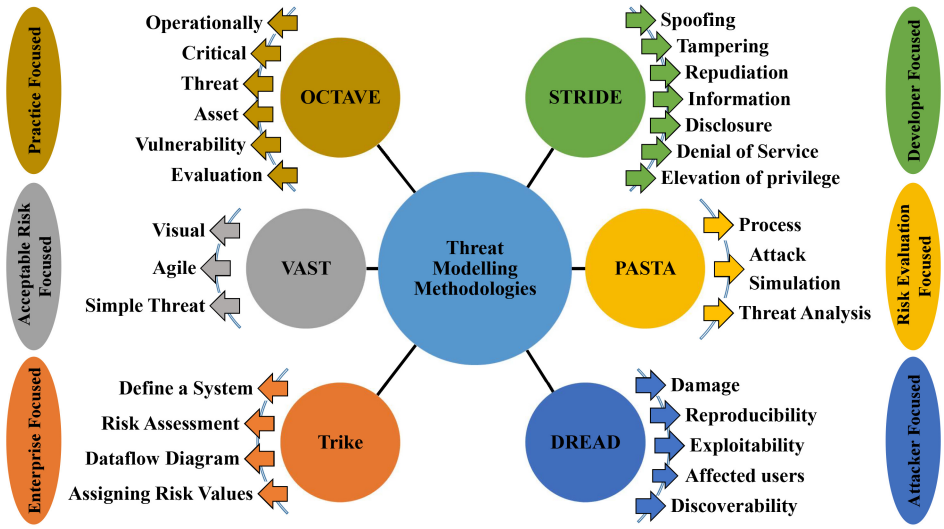

Fig. 6. Threat modelling methodologies with their stages and focus point.

as **Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of privilege (STRIDE)** modelling [133]; **Process for Simulation and Threat Analysis (PASTA)** modelling [137]; and **Damage, Reproducibility, Exploitability, Affected, and Discoverability (DREAD)** modelling [105]. However, some of them are not suitable for cyber resilience, such as **Visual, Agile, and Simple Threat (VAST)** modelling [1]; **Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)** modelling [4]; and Trike modelling [124]. These threat modelling methodologies are illustrated in Figure 6.

Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege (STRIDE) defines both a threat model and a stepwise threat modelling process. STRIDE is widely applied to analyse the security of systems since it provides a precise classification of threats [140]. The STRIDE primary helps the software developers consider security during the

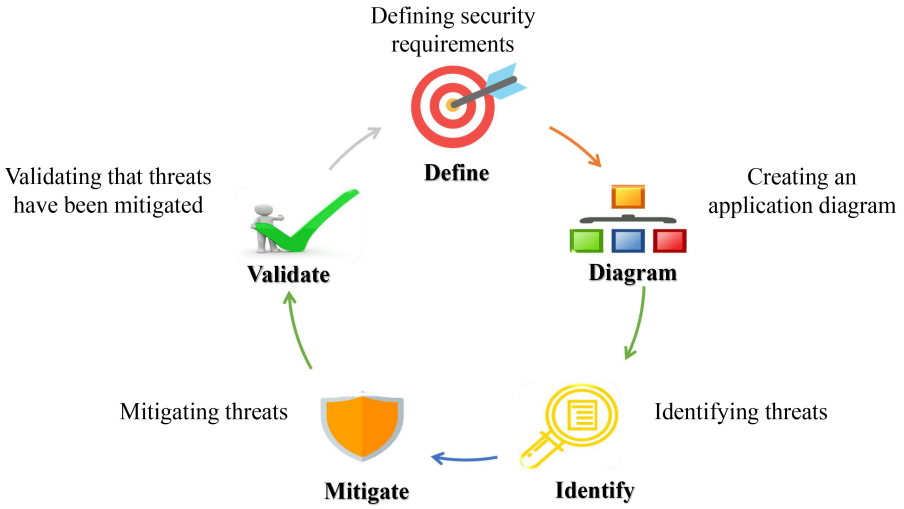

Fig. 7. Threat modelling phases.

design phase [79]. The implementation of PASTA begins at the system level, using a high-level architecture. This initial round enables threat modellers to define all inputs and outputs for each system component [82]. Damage, Reproducibility, Exploitability, Affected, and Discoverability (DREAD) is an asset-centric threat modelling approach developed by Microsoft in 2018. DREAD considers the traditional qualitative risk rating (low, medium, and high). In general, the DREAD threat modelling approach utilises a scoring system to calculate the probability of occurrence for each identified area of the asset being threat modelled [105]. DREAD acts as a classification scheme for comparing, quantifying, and prioritising the amount of risk presented by each threat [73].

The Visual, Agile, and Simple Threat (VAST) methodology is designed for performing an in-depth analysis of the process and application-level threats that focus on enterprise business [1]. It incorporates three necessary posts for supporting a scalable solution: automation, integration, and collaboration [1]. The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology is a risk-based strategic assessment and planning method for cybersecurity. OCTAVE focuses on assessing organisational risks and does not address technological risks. Its main aspects are operational risk, technology, and security practices [126]. Trike methodology is an open source security audit framework that uses threat modelling. Trike was introduced in 2006 as a stand-alone desktop application and evolved into a spreadsheet [117]. Trike modelling focused on satisfying security auditing processes for cyber risk management.

Microsoft presents five significant threat modelling phases [94] that are illustrated in Figure 7. These five phases are (1) defining security requirements, (2) creating an application diagram, (3) identifying threats, (4) mitigating threats, and (5) validating the threats that have been mitigated. The popular tool for threat modelling developed by Microsoft called the **Threat Modelling Tool (TMT)** helps software developers identify and mitigate security issues early in the **Software Development Life Cycle (SDLC)**. The tool was first released in 2008 under the name of Microsoft **Security Development Lifecycle (SDL)** and later replaced with Microsoft Threat Modelling Tool (TMT) in 2011, with the latest version released in 2018 [99]. Microsoft TMT is designed for all developers, including those who are not experts in software security.

The threat model of cyber resilience is a model of malware rebirthing botnet. It can be used in different ways to modify and collect existing malware systems, including inserting known malware signatures into the code of non-malicious and processing systems to achieve confidence in denial

and network traffic to overload sensors. It can use program signatures of known malware to trigger malware detection systems that the system was taken offline for further analysis [29].

8 DISCUSSION

This section summarises findings, limitations, open problems, and future directions related to cyber resilience. Several works have shown that cyber resilience is necessary for academic and industrial environments. As mentioned in the previous sections, most cyber resilience areas discussed by the researchers address frameworks, strategies, improvements, applications, and tools for cyber resilience. Some areas, such as principles, metrics, life-cycle management, assessment methods, and organisational cyber resilience, were lacking during the discussion on cyber resilience. Current studies on cyber resilience have highlighted the importance of these areas and how they will improve cyber resilience at different organisational levels.

8.1 Research Challenges

In our survey on cyber resilience, we discovered various research challenges in the field. These include the need for standardisation and consistency in CRFs, strategies, recent advancements, and tools. The existing frameworks for cyber resilience have implementation complexity and cannot properly measure and quantify cyber resilience. The strategies and approaches discussed in the literature need to be more compatible with specific applications. Recent advancements in cyber resilience studies require multiple and complicated configurations for implementation.

While there are many cyber resilience tools available, they can often be limited in terms of performance, features, and accessibility. Furthermore, these tools can be quite costly. Measuring and evaluating cyber resilience can also be a complex task, and it is important to understand further how human factors impact it. This is especially challenging in systems and networks with autonomous agents. Many assessment approaches and tools need to be more effective in measuring cyber resilience during cyber-attacks.

To address these challenges, more comprehensive and integrated approaches to cyber resilience are needed. This highlights the importance of developing better frameworks, strategies, tools, and techniques to measure, enhance, and quantify cyber resilience in various domains. It is recommended that investigation and development efforts be directed towards various areas to enhance cyber resilience capabilities. There is a need to establish standardised and consistent CRFs and strategies that can be implemented in different fields and industries.

Furthermore, it is important to develop metrics and tools that can measure and quantify cyber resilience, conduct research on the influence of human factors such as employee behaviour and decision making on cyber resilience, and create comprehensive and integrated approaches to cyber resilience that incorporate both technical and non-technical strategies. Addressing these research challenges and developing new approaches and techniques is critical to enhancing cyber resilience capabilities and mitigating the impact of cyber-attacks.

8.2 Findings

Many existing works and surveys focused on the fundamental frameworks for attaining cyber resilience. Most CRFs involve very high developmental but low maintenance costs. Between developmental costs and complexity, the implementation of most frameworks reported in this survey has a healthy proceeding. There are limited studies on CRFs that support a multi-data source to analyse complex infrastructure efficiently.

Very few frameworks are open source. The current study's most important clinically relevant finding was that few previous frameworks used metrics for quantifying cyber resilience. Most of the findings in this survey demonstrate that the current cyber resilience strategies are technical.

The existing strategies and approaches are of high quality and will enhance cyber resilience. In general, most current studies on cyber resilience strategies involve high flexibility.

The recent studies on cyber resilience advancements found that most of them apply to developing cyber resilience at an organisational level instead of the system level. However, few studies enhance cyber resilience in supply chain systems, cyber systems, cyber-attacks, and ICS. Most of these enhancement works are discussed at the organisational level. The recent advancements studies found and discussed in this survey use international standards such as **ISO/IEC 27001!** to improve cyber resilience.

Many applications and areas implemented cyber resilience, such as the transportation sector, financial sector, power systems, supply chain, SCADA systems, smart grid, wireless communication networks, healthcare, and ICS. For example, communication networks favour applications executing cyber resilience, particularly in the intelligent grid network. There are few tools and technologies available for cyber resilience with some limitations.

One unanticipated finding is that no cyber resilience tools could simultaneously work with organisational and operational management. However, when comparing these tools, we found most of them have helpful features such as being easy to use, efficient, and software based—besides, most of the cyber resilience tools generate detailed reports. In general, the performance of current cyber resilience tools is quite reasonable, given that most are efficient.

8.3 Limitations

The major limitation of the existing frameworks is their implementation complexity. The frameworks discussed in this survey cannot properly measure and quantify cyber resilience. The principal limit of the existing strategies and approaches in the literature is their low compatibility with specific applications. Recent advancements in cyber resilience studies require multiple and complicated configurations for implementation. The limitations of the existing cyber resilience tools naturally include features and performance. The fundamental issue with these tools and technologies is that they are not open source. Moreover, the cost of most cyber resilience tools is extremely high.

Systems and networks enabled with autonomous agents can respond to cyber-attacks with speed and scale that are unachievable with purely human defenders. Still, the mere presence of autonomous agents in the system adds vulnerabilities and can reduce cyber resilience. Most assessment approaches presented in this survey on frameworks, strategies, improvements, and tools have limitations for quantifying cyber resilience, especially in systems and networks with autonomous agents that can enable cyber resilience with new technologies such as the **Internet of Things (IoT)** and AI.

The main limitation of most of these studies is that they do not thoroughly discuss cyber resilience. Understanding the cyber resilience concept is critical before implementation. A well-established systematic literature review can provide an in-depth understanding of the cyber resilience concept, strategies, applications, tools, and limitations. It is necessary to have a systematic literature review that provides a systematic approach to the domains discussed in this survey.

8.4 Open Problems

There are still many unanswered questions about cyber resilience at the organisational or operational levels. The organisation's strategy for cyber resilience overlooks the individuals in charge of its implementation and management, and additionally who will be responsible technically for measuring cyber resilience at the operational level. One open problem is achieving consensus control of complex networks and systems with cyber resilience for resisting distributed DoS attacks on the communication infrastructure.

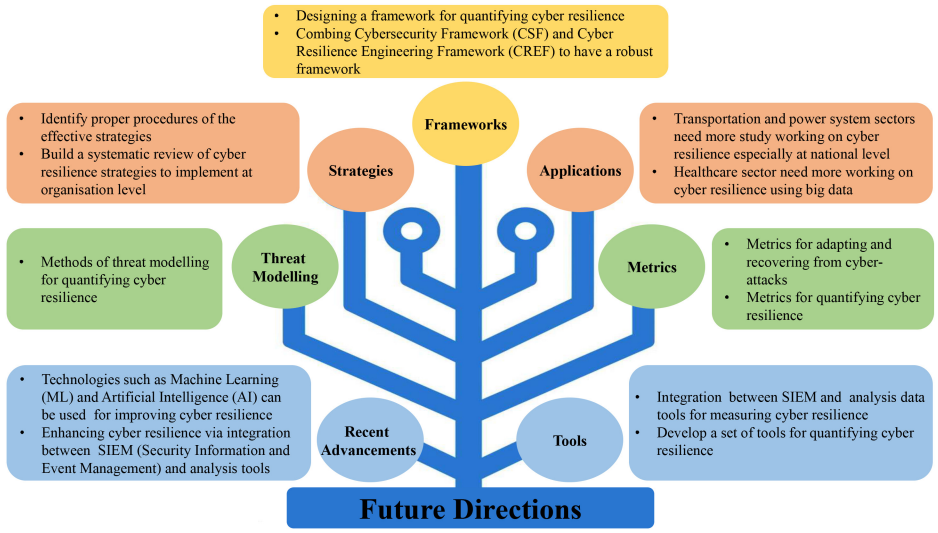

Fig. 8. Future research directions for cyber resilience that recommends frameworks, strategies, recent advancements, applications, tools, metrics, and threat modelling.

The main reason is that complex systems and networks may create additional difficulties in analysing and quantifying cyber resilience. We discuss and analyse cyber resilience assessment studies in this survey in different domains, such as frameworks and recent advancements. However, most assessment studies and tools cannot measure cyber resilience under cyber-attacks. The measurements and benchmarking using assessment tools in cyber resilience are one of the current leading open problems.

Most existing research trust and importance systems utilise various defence mechanisms against specific cyber-attacks. Although researchers have proposed and implemented several such defence techniques, current systems typically address only minimal cyber-attacks and hardly provide a comprehensive solution. We believe the ability to design a comprehensive stable system with cyber resilience to an entire collection of cyber-attacks is an open problem and a big challenge.

Many types of cyber-attacks affect the systems and networks, but most current works on cyber resilience considered only the distributed DoS attacks. Different types of cyber-attacks need to be considered when implementing cyber resilience. Unfortunately, the literature reviewed in this survey only concerns a specific type of cyber-attack. Cyber resilience needs more investigation and consideration with multiple cyber-attack types, which can be mounted simultaneously.

9 FUTURE RESEARCH DIRECTIONS

This section focuses on future research directions for cyber resilience. Many superior works have emerged recently, and many challenges still lead to future research directions. In this section, we summarise some potential future research directions, as illustrated in Figure 8.

9.1 Frameworks

There is little work related to a systematic literature review of the CRFs for many reasons. One is a systematic literature review by authors Sepúlveda-Estay et al. [125]. Many CRFs are discussed in their survey, but most are designed for a specific field. The future direction is to build a framework like the CSF that can be used in different fields.

Most of these frameworks need to evaluate and validate instruments within other current categories, such as the economy or large businesses in the industrial, financial, or other sectors. Engineering-driven actions must develop more resilient systems by integrating cybersecurity frameworks such as the NIST framework [11] and CRFs such as the CREF [20]. The CREF was developed by MITRE [20] that provides an overview of cyber resilience, including how to structure cyber resilience capabilities. These capabilities address the goals, objectives, and practices aligned with malicious activities to reflect the plan and possible actions to protect [81].

On combining the CREF and Cyber Security Framework (CSF) presented by NIST, the combination will present a new framework that will be robust for further developing cyber resilience. We discuss some frameworks based on the metrics in other works [20, 52, 62, 89] for improving only the system and network functionality. However, we need a metrics-based framework for quantifying cyber resilience to enhance cyber resilience.

Furthermore, seeking metrics that will tell us what kind of cyber resilience is essential in a policy or algorithm for a particular use. It is exciting but insufficient to differentiate algorithms quantitatively. The systematic review of cyber resilience assessment frameworks [125] demonstrates the work has not been concerned with defining what a CRF must contain, but instead with content and description analysis of CRFs that have been proposed. Future work involves analysing requirements that a CRF must fulfil and thoroughly evaluating existing CRFs.

9.2 Strategies

As few cyber resilience strategies are present in this survey, future researchers must conduct a more detailed investigation to identify more procedures to develop them. This investigation aims to help the organisation develop the right goals and targets of cyber resilience to help everyone focus their efforts on completing them. Additionally, it is necessary to have a systematic review of cyber resilience strategies, including the management and operational comparison in detail. Further work requires organisational cyber resilience to have a strategic approach and dynamic capabilities for becoming a cyber resilience organisation. Despite this clear definition and the number of works recognising the strategic need for systematic cyber resilience planning, there is still a lack of research on dealing with cyber resilience strategies that require further investigations.

Some cyber resilience strategies are discussed in this survey, and most are considered at the organisation level rather than the national level. However, national cyber resilience strategies are equally required to support private sectors and the general public. These national strategies will evaluate cyber resilience as more manageable and efficient. One future direction is implementing and evaluating cyber resilience strategies at the national level. One of the future directions is that organisations must have a strategy to invest more in technology and training to help factories mitigate cyber-attacks. Carías et al. [34] defined and modelled an effective cyber resilience strategy, then concluded that technology and personnel training are essential in cyber resilience, and neither must be overlooked in an investment strategy. However, to efficiently invest in cyber resilience, the first step must be to invest more in tools and technical solutions, and when these are in place, the next one will be an investment in cyber resilience training.

9.3 Recent Advancements

Few studies on enhancing cyber resilience are mostly based on the assessment. Future research needs to investigate more thorough simulations to make better estimates. Integrating SIEM with data analysis software such as Infoxdb, Kdb+, Prometheus, Graphite, or any other software that has the time series databases feature can help organisations respond faster to attacks and increase cyber resilience. Therefore, a further study on enhancing cyber resilience using ML and AI is

suggested, especially in communication networks. Such networks can be part of the critical infrastructure and are much affected by cyber-attacks.

AI and ML are recent approaches considered to make intelligent and data-driven device and system-level control decisions based on the data generated by their models [147]. AI and ML disrupt cyber resilience and cybersecurity, enhancing cyber resilience by detecting malicious activities. Additional autonomous monitoring and more intelligent network data analytics include different types of cyber-attacks using AI to enhance cyber resilience in systems and networks [26]. Future research should focus on measuring the impact of cyber-attacks using AI to enhance cyber resilience.

9.4 Applications

Further research must investigate cyber resilience in critical infrastructure areas such as health care, power systems, and transportation. A further study could assess the long-term reliance of health care on cyber resilience. Big data is being utilised extensively by academia and industry, but its role in health care may have the most significant impact on our lives. Big data technologies can improve cyber resilience in health care sectors, such as the automation of hospital administrative processes and the availability of patient health care information under cyber-attacks. The power systems sector needs more future research work for robust cyber resilience strategies. Technological innovations can benefit society by securely optimising our infrastructure networks at the organisational and national levels.

9.5 Tools

It is necessary to develop tools and technologies for cyber resilience, including simulating the cyber resilience of systems and networks. Distributed autonomous agents may specialise in measuring the degradation of individual components' functionality and performance rather than measuring overall impact. Moreover, those distributed agents would respond to cyber-attacks and recover only the features they are responsible for paying the cyber "antibodies" role, similar to that presented by Ligo et al. [87]. Additionally, the agents might send measurements to a central "genius" to estimate the overall change in performance, functionality, and mission impact. As well, integration between SIEM solutions and analysis tools will build a new tool for quantifying cyber resilience.

The current cyber resilience tools are only for assessment (e.g., [63, 107, 127, 144]). We cannot reliably improve what we cannot quantify and measure. Moreover, no technical discipline has achieved maturity without proper measurement and quantification tools. For this reason, the need for measurement tools in cyber resilience is significant in quantifying and improving our systems and networks. Researchers should also investigate the value and potential of the model as a measurement tool, with supporting metrics, to evaluate and quantify the level of organisational cyber resilience.

The simulations and tools assessing cyber resilience involve problem identification, system description, digital model design, metrics definition, modelling failure scenarios, and cyber resilience assessment [127]. Simulation is used to compare the performance of a system under cyber-attacks with its nominal performance, and cyber resilience is calculated based on the comparison. It is necessary to have more research using tools and simulations for quantifying cyber resilience.

9.6 Metrics

Several metrics are presented for cyber resilience, and most of them are related to recovery. Few cyber resilience metrics calculate the adaptation capability of the systems and networks against cyber-attacks. Considerably, more work will be needed to determine cyber resilience using

metrics. Cyber resilience metrics are necessary for evaluating and measuring cyber resilience, including the adaptation and recovery indicators to develop a toolkit. The toolkit provides a rationale for monitoring, evaluating, and guidance for envisioning adaptation success and then identifying, prioritising, and tracking appropriate indicators and metrics.

Lee et al. [83] review various resilience quantification techniques and metrics to provide a systematic understanding of the field. They also discuss the challenges faced in current quantification methods and propose ideas for future research to improve cyber resilience measurements. Challenges in quantifying cyber resilience include selecting appropriate metrics, adapting metrics to different systems, and addressing uncertainties in cyber-enabled systems. Efforts are being made to build testbeds and perform simulations to improve confidence in cyber resilience metrics. Cyber resilience metrics provide an effective instrument for identifying optimal resilience parameters [5]. Nevertheless, cyber resilience is rare, and many aspects, primarily related to complex multi-level resilience stills, require further research.

9.7 Threat Modelling

There is little research into threat modelling for enhancing cyber resilience. Threat modelling will enable organisations to identify and mitigate the attacks that they work with cyber resilience. Such threat modelling includes some methods for quantifying cyber resilience using detailed simulations. The works of the threat modelling of cyber resilience are limited and need more future research in this direction. The threat modelling will assist the evolution of cyber resilience by anticipating, withstanding, and recovering from cyber-attacks. One of the future directions that will help quantify and evaluate cyber resilience is using threat modelling methodologies for cyber resilience.

10 CONCLUSION

This survey has provided a comprehensive review of different domains of cyber resilience. Complex system operations are thoroughly discussed, emphasising the applied technologies to improve cyber resilience in terms of quick recovery achievable after cyber-attacks. Besides, vital insights and promising solutions for improving and implementing cyber resilience were presented for different applications. The main goal of this survey is to understand cyber resilience and related critical issues. We have provided a comparative analysis of existing studies in this survey. Furthermore, we have concisely reviewed the existing research that involves frameworks, strategies, recent advancements, applications, and tools. There are many frameworks of cyber resilience exhibited in this survey, and most of them are similar or extend from the CREF. Most recent advancements in cyber resilience are based on recommendations, practices, standards, and technologies. During our discussion, we covered a range of tools and technologies for enhancing cyber resilience. However, it is worth noting that the majority of these solutions are not available as open source alternatives. Additionally, we discussed in depth the main findings, limitations, and open problems related to cyber resilience. Finally, we have provided several insights and findings concerning cyber resilience. Last but not least, we have shed light on many future research directions and open research problems to make a call for action for improving cyber resilience.

APPENDICES

In this section, we have included supplementary information for our survey. Firstly, we present a list of applications related to cyber resilience. We compare and evaluate recent literature on cyber resilience applications, highlighting strengths and weaknesses. Lastly, we provide a list of all the acronyms used in this survey.

A APPLICATIONS OF CYBER RESILIENCE

This section presents the applications within the areas discussed under cyber resilience. Additionally, we introduce comparisons between them and demonstrate the strengths and weaknesses of the recent literature on cyber resilience. Cyber resilience applications are sectors that use software tools and platforms that can help organisations monitor, detect, and respond to cyber threats. Applications can include SIEM systems, IDS, and vulnerability scanners. These tools can help organisations identify potential threats and vulnerabilities and respond quickly and effectively to cyber-attacks.

A.1 Cyber Resilience in Transportation Sector

Kiesling and Kreuzer [135] discussed the ARIEL project's holistic approach and presented eight key recommendations, which they believe are vital in increasing cyber resilience in air traffic systems. Implementing these recommendations requires continuous adaptation and keeping cyber resilience at a high level. The architectures of technical and operational procedures must be restricted based on persistently completing risk analysis results. From this point of view, they strongly recommend balancing the performance and the cost of development and focusing on comprehensive, sustainable, and continuous improvement with general cyber resilience systems.

Bouk et al. [27] investigated security challenges and the cyber-attacks in **Vehicular Cyber-Physical Systems (VCPS)** and associated them with the working principle of **Named Data Network (NDN)**. They explicitly proposed a solution based on the Named Data Network (NDN) architecture for the cyber resilience Vehicular Cyber-Physical Systems (VCPS). The proposed layered architecture includes several function components ranging from the NDN daemon, resilience provision, detection, and threat aversion. They identified the challenges of security encountered by a scenario termed as *Named Data Vehicular Cyber-Physical Systems* that must be addressed in the future by the research community to ensure proper cyber resilience in the transportation network.

The cyber resilience of autonomous mobility systems has been investigated quite comprehensively in the literature. The literature also covers cyber components, plausible autonomous mobility systems, and operational scenarios before identifying possible cyber-attacks applicable to autonomous mobility systems at the design and vehicle levels. Then, they examined the existing practices to enhance cybersecurity and several strategies for improving the cyber resilience of autonomous mobility systems. At the vehicular level, creating separate layers to reduce cyber component connectivity and deploying an independent processing and data collection procedure are essential in vehicle design and manufacturing. At the system level, recommended strategies include establishing redundancy in transportation, maintaining a separate road network, and capacity, and deploying different sub-autonomous mobility systems [148].

Lykou et al. [92] discussed implementing cybersecurity measures and best practices for improving cyber resilience at airports, developing a robust cybersecurity government, and enhancing operational practices at intelligent airports. Additionally, they analysed security gaps in different areas, including policies, organisational procedures, and technical proceedings. Securing smart airports and continually evolving cyber threats are shared responsibilities of airports, airlines, regulatory authorities, and vendors working with the airports.

Mathew [95] presented airport cybersecurity and cyber resilience controls. They discussed airport intelligence classifications and cybersecurity malicious threats analysis. The Internet of Things (IoT) is a necessary technology used in airports to facilitate communications among various intelligent systems and devices. IoT has helped improve cyber resilience and operational efficiencies. The increase in integrating airport services and facilities with IoT will increase the vulnerabilities to network attacks, which is the importance of cyber resilience at airports.

Lykou et al. [93] discussed advanced services in surveillance systems of air traffic control to address existing territories and vulnerabilities to improve cyber resilience in airports. Moreover, it is very important to introduce and analyse resilience aspects in the aviation sector and then classify resilience recommendations based on their economic dimensions across social, organisational, and technical aspects. Additionally, they concluded with resilience analysis and the benefits of cyber resilience in the aviation sector.

A.2 Cyber Resilience in Financial Sector

Putranti [113] focused on designing cyber resilience using the legal instruments and technological policies from international trade facilitation in Indonesia. Furthermore, he discussed the implementation factors in Indonesia's cyber resilience development system within trade facilitation. Cyber resilience is a critical need in trade facilitation due to the high standards for automation and digitisation. Therefore, improving human resources with sound knowledge regarding the individual (public), public sector, private sector, and cyber-attacks, and alleviating cyber resilience is essential.

Pinckard et al. [70] described the methodology used and the observations they made while mapping the declarative statements in the Federal Financial Institutions Examination Council and Cybersecurity Assessment Tool as the best practice questions in the CRR. This mapping will enable financial organisations to use the results of CRR to measure their cyber resilience level and examine their current baseline considering the NIST Cybersecurity Framework.

Dupont [47] considered the need for cyber resilience in the financial sector, highlighting several threat types that target economic systems and different outcomes due to adverse consequences. Besides, the presenting "protect and prevent" paradigm that has prevailed so far as inadequate must be included within the cyber resilience orientation as part of the risk managers' toolbox. He briefly traced the scientific history of cyber resilience and outlined the central five dimensions of organisational resilience, which are networked, adaptive, dynamic, practised, and contested. Moreover, he analysed three main institutional approaches that foresee using cyber resilience in the financial sector. The first uses standards bodies to embed cyber resilience into their cybersecurity standards. The second is improving regulatory agencies with various complying tools to enhance cyber resilience. The third is to expand cybersecurity as a growing industry towards the future of cyber resilience.

A.3 Cyber Resilience in Power System

Arghandeh et al. [118] defined resilience for power systems and discussed system resilience concepts. A system's resilience is defined as reducing disruption duration and magnitude. The authors advanced the field by adding cyber-physical resilience concepts to power systems vocabulary. They offered a new thinking way about grid operation with unexpected extreme disturbances and threats for enhancing system resilience.

Babu [10] presented best practices of cyber resilience for electricity infrastructure and shared lessons they learned to enhance the electricity supply industry's cyber resilience and reduce cyber-attacks on the interconnected power systems. They addressed certain issues, such as changes required for reorganising the industry to prepare for cyber-attacks in the corresponding system given the critical interconnectivity of the Internet and communication technologies.

Pöyhönen et al. [72] discussed applying CRR to a single electricity company in the power system. They considered a SWOT analysis used to analyse and improve an organisation's cybersecurity level. Reviewing cyber resilience can help in contingency planning. The authors applied and reviewed the resilience metrics framework presented by Linkov et al. [89] for measuring resilience to utilise the organisation's operational preparedness planning.

Sahu et al. [123] propose a mixed-domain **Reinforcement Learning (RL)** environment for enhancing power distribution systems' cyber and physical resilience. The proposed environment uses OpenDSS for the power system and SimPy for the cyber system, which is operating system agnostic. The work presents the results of co-simulation and training Reinforcement Learning (RL) agents for a cyber-physical network reconfiguration and Volt-Var control problem in a power distribution feeder.

Additionally, Sahu [123] demonstrate that RL-based techniques offer a credible alternative to conventional optimisation-based solvers, particularly when there is environmental uncertainty, such as renewable generation or cyber system performance. However, efficiently training an agent requires numerous interactions, including an environment to learn the best policies. Existing co-simulation methods are efficient but are both resource and time intensive to generate large-scale datasets for training RL agents. The proposed mixed-domain RL environment can help overcome these challenges and improve the resilience of power distribution systems.

A.4 Cyber Resilience in the Supply Chain

McPhee and Khan [28] conferred cyber resilience in the supply chain that has received less attention than security, cyber risk, and resilience. That may be because, naturally, most experts view IT security as mainly responsible for cyber-related issues. This compartmentalisation of disciplines is the main problem and must be resolved to achieve cyber resilience in the supply chain. They highlighted the significance of cyber resilience in the supply chain. They developed a shared understanding of the theory, definition, and managerial implications of cyber resilience and risk in the supply chain.

Davis [43] convened the concept of cyber resilience in the supply chain and how an information-centric approach can help create more cyber resilience in the supply chain. Additionally, Davis presented five steps for organisations that can be used to improve their information and cyber resilience. The five measures can be summarised as follows: (1) build capability in the organisation; (2) share knowledge and expertise; (3) create a clear map of the supply chain; (4) state requirements across the supply chain using different languages, common frameworks, and standards; and (5) measure, audit, and assess cyber resilience in the supply chain.

Boyes [28] considered cyber resilience in a supply chain that delivers services and products. In both cases, critical cybersecurity issues require attention at a satisfactory level to achieve cyber resilience. Cyber resilience and cybersecurity must not be considered purely technical issues, as it is also affected by personnel, process, and physical aspects. When designing or modifying a supply chain, the organisations involved must consider the cyber resilience implications of the global technology components they plan to use. Supply chain managers should review the technical vulnerabilities in achieving cyber resilience while developing a holistic approach to ensure higher security. However, genuine technical solutions are not the same to address the breadth of potential weaknesses and threats.

A.5 Cyber Resilience in SCADA Systems

Kolosok and Korkina [80] examined the cyber resilience in SCADA systems for increasing the capability to deter cyber threats. SCADA systems are famous relative to other systems in the energy industry: SCADA supports the automated dispatch of electric power systems control along with the automatic control. Today, the consequences of cyber-attacks are hazardous to the information subsystem of the control system. The SCADA forms the information system's technical backbone, which is most crucial in controlling the power system facility. These measures will increase the cyber resilience of the SCADA system.

SCADA systems are critical infrastructures vulnerable to cyber-attacks due to their interconnectedness and internet accessibility. Birnbaum et al. [16] presented programmable logic controllers used in SCADA systems, which are persistent, making them ill suited for virtual and dynamic environments. Applying conventional cyber defence techniques to SCADA systems is challenging due to limited resources and high availability demands. Cyber resilience is crucial for SCADA systems to recover functionality after being degraded or disrupted rapidly. It ensures continuity of operations and goes beyond attack prevention. Virtualisation is a promising technology for implementing defensive and cyber resilience techniques in SCADA environments. It enables security techniques to be applied and systems to be rebooted on demand. A resilient SCADA architecture with non-persistence, redundancy, state restoration, and blockchain technology can mitigate the harmful effects of cyber-attacks.

A.6 Cyber Resilience in a Smart Grid

Nazir et al. [102] reviewed the strategies of cyber resilience and vulnerabilities in a smart grid, and they proposed the combined use of micro and macro management techniques as an evolutionary process to enhance the system's availability. A holistic approach to tackling resilience at the micro and the macro levels was proposed to contain, isolate, identify, and overcome cybersecurity challenges. It is an ongoing process rather than one small operation and must continually evolve to reduce further new problems.

Maziku and Shetty [96] advised the need for cyber resilience in a smart grid network on its ability to deliver service in a reliable and timely manner, even in the persistent presence of attacks. At the same time, the smart grid of digital communications provides instant benefits such as higher data transfer rates. It increases the surface of attacks while permitting IP based on network attacks, such as DoS attacks. Incorporating cyber resilience capability in intelligent grid networks will mitigate emerging attacks and meet power system requirements. Security risk assessment is critical in providing cyber resilience in intelligent grids.

One of the studies that discussed cybersecurity and directories related to cyber resilience is presented by Gunduz and Das [59]. It concerns the potential cyber threats and countermeasures for IoT-based intelligent grid systems. The authors highlight the importance of resilient ICT for reliable operation in smart grid applications and emphasise the need to prevent malfunctions and intrusion by malicious agents. The authors also examine the efforts to create new standards for augmenting old systems and protocols to improve security against malicious attacks. Therefore, this study provides valuable insights into enhancing cyber resilience in smart grid systems.

Hossain et al. [66] focus on modelling and assessing the cyber resilience of smart grid systems using a Bayesian network approach. The study identifies potential causes and mitigation techniques for the smart grid and analyses the overall cyber resilience of the system. The Bayesian network is an analytical tool for risk, reliability, and resilience assessment under uncertainty. Different scenarios were developed and analysed to identify critical variables that affect the cyber resilience of the smart grid system. The authors highlight the importance of developing countermeasures against access domain vulnerability to enhance the overall cyber resilience of the smart grid. Furthermore, the authors emphasise the efficacy of the Bayesian network in assessing and strengthening the cyber resilience of the smart grid system.

To address the consensus problem in networked intelligent grids, especially in MGs subject to multi-layer DoS attacks, Ge et al. [55] proposed a unified notion of persistency of dataflow to characterise the data unavailability in different information network links and quantify the multi-layer DoS effects on the hierarchical system. The authors provide a sufficient condition for preserving consensus under DoS attacks with the proposed edge-based self-triggered distributed control framework. An online self-adaptive scheme of control parameters is developed to mitigate the

conservativeness of offline design against the worst-case attack. The effectiveness of the proposed cyber resilience self-triggered distributed control is verified through representative case studies.

A.7 Cyber Resilience in Communication Networks

Buinevich and Vladyko [30] proposed cyber resilience in wireless communication network technologies for **Intelligent Transportation System (ITS)** applications. They applied cyber resilience to motor transport such as the **Vehicular Adhoc Network (VANET)**. The authors provided an analytical overview of cyber-attacks on Vehicular Adhoc Network (VANET)/Intelligent Transportation System (ITS). They analysed the top 10 cyber threats, considering threat models such as an object of attack, damage, a countermeasure, vulnerability, and attack mechanism. Subsequently, they identified open-ended issues and research opportunities: the threats formalisation, vulnerability lamination, the level crossing of network management consolidation, and the prediction and modelling of VANET/ITS cyber resilience.

One study evaluates nodes' cyber resilience in hybrid network operations using a framework presented by Ur-Rehman et al. [138]. The proposed framework integrates cyber resilience with the **Common Vulnerability Scoring System (CVSS)** to standardise node resilience capabilities in the cyber industry. Integrating cyber resilience with the Common Vulnerability Scoring System (CVSS) framework helps standardise operational resilience across the cyber industry when evaluating vulnerabilities. The proposed model better evaluates node vulnerabilities by incorporating the resilience capability of the nodes compared to the CVSSIoT-ICS model. Assessing vulnerabilities under the proposed framework prioritises nodes based on their resilience index, helping system admins allocate resources effectively. Cyber resilience evaluation includes measuring system capabilities to detect cyber security incidents promptly, manage and recover from those incidents, and assess system resistance to attacks. Integrating cyber resilience with the CVSS framework helps standardise node resilience capabilities for continuous business operations.

A.8 Cyber Resilience in Healthcare

Williams [142] proposed cyber resilience in Australia's health care system to consider how malleable is a medical information security and its necessity to return to a normal situation or functioning state. The cyber resilience of medical practice to cope with a cybersecurity incident is extremely necessary. Resuming regular activity within an acceptable time frame must be essential after a major attack on Australia's infrastructure. The author looked at the issues from the end user perspective, including government security, medical software vulnerability, and security capability within general practices.

Boddy et al. [8] presented how to increase cyber resilience in healthcare infrastructure by analysing a system that can find unusual data behaviour through advanced visualisation techniques and data analytics. A sophisticated set of ML algorithms can understand the patterns of data and functioning of the user's profile, presenting three datasets related to three primary services: (1)the Active Directory Server allows access to the organisational infrastructure, including security group user accounts and passwords; (2) the Electronic Prescribing Server enables an attacker to monitor doses and prescriptions administrated to a user; and (3) the Patient Administration System allows an attacker access to patient data with viewing or modifying rights.

Port mapping servers are crucial for any organisation, particularly in hospital networks. Monitoring ports can be a challenging task that requires more resources [8]. Cleansing and preparing the data will highlight anomalous data activity to cybersecurity analysts to mitigate the threat that will increase cyber resilience. Utilising ML algorithms as assistance will leverage the expertise and the in-house knowledge to assist the IT department of hospitals or any organisation in finding potential cyber-attacks based on their vast data infrastructure.

Porter et al. [112] presented the description of the methodology that is used in observations performed while mapping the requirements for the **Health Insurance Portability and Accountability Act (HIPAA)** combined with a set of security rules found under CERT CRR. The emerging mapping allows health care providers to use CRR results to calculate their cyber resilience capability and examine their current baseline concerning the Health Insurance Portability and Accountability (HIPAA) security rules and the NIST. Both HIPAA and CRR security rules were mapped to the NIST CSF. The mappings between the HIPAA security rules and the CRR practices will comply with any health care regulations. The proposed mapping shows that the CRR provides complete coverage of the HIPAA security rule. As a result, organisations involved in the HIPAA security rule can use the CRR to indicate their compliance with the security rule.

Ahmed et al. [2] assess cyber resilience in **Mobile Field Hospitals (MFHs)** during emergencies. The healthcare sector, including Mobile Field Hospital (MFH)s, is a prime target for cybercriminals and cyber-attacks. It is crucial to assess the cyber assets and identify possible threat vectors. Healthcare organisations are recommended to adopt frameworks for cyber resilience assessment. Customised adoption of security frameworks is necessary for MFHs due to its unique organisational setup and ad-hoc security infrastructure. The study emphasises the importance of research in finding suitable security frameworks for different healthcare industry sub-sectors. The cyber resilience assessment in MFHs helps users and stakeholders understand the risks associated with its cyber assets.

The UK National Health Service created a program to enhance cyber resilience after the 2017 WannaCry ransomware attack on 200,000 computers across 150 countries [56]. The program involved conducting regular vulnerability scans, managing patches, and providing employee training and awareness programs. However, the implementation of the program was smooth. The primary challenge was maintaining a balance between security and timely access to patient data. A risk-based approach was developed for cyber resilience, prioritising protecting critical systems and data to overcome this challenge. The program aimed to enhance National Health Service's ability to withstand cyber threats and maintain patient data confidentiality, integrity, and availability.

A.9 Cyber Resilience in ICS

Bissell et al. [75] discussed some technologies that will increase cyber resilience in an organisation and enable fast provisioning and de-provisioning of networks. With security in mind, they leverage this capability to failover, cloak, protect, segment, or retract any resources or devices on the system. Micro-segmentation and dynamic segmentation enable security organisations to respond to threats and present adaptable protection to adversaries in real time.

The second technology is advanced identity access, a critical element of minimally slowing or stopping a cyber adversary. Using multi-factor authentication will require additional information and context before enabling access to essential applications or transactions to make authentication safer. AI and robotics provide an automated, reliable, and consistent way to give only the right person access to critical data. Haque et al. [62] analysed cyber resilience of ICS in the presence of cyber-attacks using a subjective approach. They briefly described cyber resilience characteristics, complying with a cyber resilience assessment model for ICS.

B LIST OF ACRONYMS

AI	Artificial Intelligence	**CPS**	Cyber-Physical Systems
BFT++	Byzantine Fault Tolerant++	**CRAT**	Cyber Resilience Assessment Tool
CERT	Computer Emergency Response Team		

DREAD	Damage, Reproducibility, Exploitability, Affected, and Discoverability	**ML**	Machine Learning
		NATO	North Atlantic Treaty Organisation
CREF	Cyber Resilience Engineering Framework	**NDN**	Named Data Network
		NIST	National Institute of Standards and Technology
CRF	Cyber Resilience Framework		
CRR	Cyber Resilience Review	**NSCC**	Non-Stop Customs Clearance
CSF	Cyber Security Framework	**OCTAVE**	Operationally Critical Threat, Asset, and Vulnerability Evaluation
CVSS	Common Vulnerability Scoring System		
DoD	Department of Defense	**PASTA**	Process for Attack Simulation and Threat Analysis
DoS	Denial of Service		
HIPAA	Health Insurance Portability and Accountability	**RL**	Reinforcement Learning
		RMM	Resilience Management Model
ICS	Industrial Control System	**SCADA**	Supervisory Control And Data Acquisition
ICT	Information and Communications Technologies s	**SDN**	Software-Defined Networking
		SIEM	Security Information and Event Management
IDS	Intrusion Detection Systems		
IoT	Internet of Things	**SMEs**	Small and Medium-sized Enterprises
ISO	International Organisation for Standardisation	**STRIDE**	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege
IEC	International Electrotechnical Commission		
IT	Information Technology		
ITS	Intelligent Transportation System	**TMT**	Threat Modelling Tool
		VANET	Vehicular Adhoc Network
JUMP	Joint User Cyber Mission Planning	**VAST**	Visual, Agile, and Simple Threat
MG	Microgrid	**VCPS**	Vehicular Cyber-Physical Systems
MFH	Mobile Field Hospital		

REFERENCES

[1] Ghazanfar Abbas, Syed, Shahzaib Zahid, Faisal Hussain, Ghalib A. Shah, and Muhammad Husnain. 2020. A threat modelling approach to analyze and mitigate botnet attacks in smart home use case. *Proceedings of the 2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE'20)*. 122–129. arXiv:2101.02147.

[2] Nasir Baba Ahmed, Nicolas Daclin, Marc Olivaux, and Gilles Dusserre. 2020. Improving cyber resilience in mobile field hospitals: Towards an assessment model. *International Journal of Computer and Information Engineering* 14, 12 (2020), 542–548.

[3] Abdullah Al Maruf, Luyao Niu, Andrew Clark, J. Sukarno Mertoguno, and Radha Poovendran. 2023. A timing-based framework for designing resilient cyber-physical systems under safety constraint. *ACM Transactions on Cyber-Physical Systems* 7, 3 (2023), 24. https://doi.org/10.1145/3594638 arXiv:2208.14282.

[4] Christopher Alberts, Audrey Dorofee, James Stevens, and Carol Woody. 2003. *Introduction to the OCTAVE Approach*. Carnegie Mellon University, Pittsburgh, PA.

[5] Eduardo Alvarenga, Jan R. Brands, Peter Doliwa, Jerry den Hartog, Erik Kraft, Marcel Medwed, Ventzislav Nikov, Joost Renes, Martin Rosso, Tobias Schneider, and Nikita Veshchikov. 2022. Cyber resilience for the Internet of Things: Implementations with resilience engines and attack classifications. *IEEE Transactions on Emerging Topics in Computing*. December 29, 2022. https://doi.org/10.1109/TETC.2022.3231692

[6] Tomomi Aoyama, Hidemasa Naruoka, Ichiro Koshijima, Wataru Machii, and Kohei Seki. 2015. Studying resilient cyber incident management from large-scale cyber security training. In *Proceedings of the 2015 10th Asian Control Conference: Emerging Control Techniques for a Sustainable World (ASCC'15)*. 1–4.

[7] Apache Metron. 2020. What Apache Metron Does. Retrieved September 9, 2021 from http://metron.apache.org/
[8] Aaron Boddy, William Hurst, Michael Mackay, and Abdennour El Rhalibi. 2017. A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures. *ACM International Conference Proceeding Series* 32, May (2017), 1–6. https://doi.org/10.1145/3109761.3109793
[9] Mary Asante, Gregory Epiphaniou, Carsten Maple, Haider Al-Khateeb, Mirko Bottarelli, and Kayhan Zrar Ghafoor. 2021. Distributed ledger technologies in supply chain security management: A comprehensive survey. *IEEE Transactions on Engineering Management*. Published Online, March 1, 2021.
[10] Ram Babu. 2016. *Best Practices to Increase Cyber Resilience of Smart Electricity of Grid with Focus on Advance Metering and Distribution Infrastructure*. World Energy Council.
[11] Matt Barrett. 2018. Framework for improving critical infrastructure cybersecurity. *Proceedings of the Annual ISA Analysis Division Symposium* 535 (2018), 9–25.
[12] Muhammet Baykara and Resul Das. 2018. A novel honeypot based security approach for real-time intrusion detection and prevention systems. *Journal of Information Security and Applications* 41 (2018), 103–116. https://doi.org/10.1016/j.jisa.2018.06.004
[13] Miguel Hernandez Bejarano, Ricardo J. Rodriguez, and Jose Merseguer. 2021. A vision for improving business continuity through cyber-resilience mechanisms and frameworks. In *Proceedings of the 2021 16th Iberian Conference on Information Systems and Technologies (CISTI'21)*. 1–5. https://doi.org/10.23919/CISTI52073.2021.9476324
[14] Emanuele Bellini, Stefano Marrone, and Fiammetta Marulli. 2021. Cyber resilience meta-modelling: The railway communication case study. *Electronics (Switzerland)* 10, 5 (2021), 1–26.
[15] Sufyan bin Uzayr. 2022. *Mastering Bootstrap*. Vol. 1. CRC Press. https://doi.org/10.1201/9781003310501
[16] Zachary Birnbaum, Matthew Davis, Salman Salman, James Schaffter, Lanier Watkins, Saikiran Yamajala, and Shruti Paul. 2020. Cyber-resilient SCADA systems via secure state restoration. *IFIP Advances in Information and Communication Technology* 596 (2020), 183–207. https://doi.org/10.1007/978-3-030-62840-6_9
[17] Fredrik Björck, Martin Henkel, Janis Stirna, and Jelena Zdravkovic. 2015. Cyber resilience—Fundamentals for a definition. In *New Contributions in Information Systems and Technology*. Advances in Intelligent Systems and Computing, Vol. 353. Springer, 311–316.
[18] Dan Blum. 2020. *Rational Cybersecurity for Business*. Springer.
[19] Deborah Bodeau, John Brtis, Richard Graubart, and Jonathan Salwen. 2014. Resiliency techniques for systems-of-systems extending and applying the cyber resiliency engineering framework to the space domain. In *Proceedings of the 7th International Symposium on Resilient Control Systems (ISRCS'14)*. 1–6.
[20] Deborah Bodeau and Richard Graubart. 2011. *Cyber Resiliency Engineering Framework*. MITRE.
[21] Deborah Bodeau and Richard Graubart. 2013. *Cyber Resiliency Assessment: Enabling Architectural Improvement*. MITRE.
[22] Deborah Bodeau and Richard Graubart. 2016. *Cyber Resilience Metrics: Key Observations*. MITRE.
[23] Deborah Bodeau and Richard Graubart. 2017. *Cyber Resiliency Design Principles*. MITRE.
[24] Deborah Bodeau, Richard Graubart, William Heinbockel, and Ellen Laderman. 2015. *Cyber Resiliency Engineering Aid*. MITRE.
[25] Michael Bostock, Vadim Ogievetsky, and Jeffrey Heer. 2011. D3 data-driven documents. *IEEE Transactions on Visualization and Computer Graphics* 17, 12 (2011), 2301–2309. https://doi.org/10.1109/TVCG.2011.185
[26] Ioannis Bothos, Vasileios Vlachos, Dimitris M. Kyriazanos, Ioannis Stamatiou, Konstantinos Georgios Thanos, Pantelis Tzamalis, Sotirios Nikoletseas, and Stelios C. A. Thomopoulos. 2021. Modelling cyber-risk in an economic perspective. In *Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR'21)*. 372–377.
[27] Safdar Hussain Bouk, Syed Hassan Ahmed, Rasheed Hussain, and Yongsoon Eun. 2018. Named data networking's intrinsic cyber-resilience for vehicular CPS. *IEEE Access* 6 (2018), 60570–60585.
[28] Hugh Boyes. 2015. Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review* 5, 4 (2015), 13–18.
[29] M. Brand, C. Valli, and A. Woodward. 2011. A threat to cyber resilience: A malware rebirthing botnet. In *Proceedings of the 2nd International Cyber Resilience Conference*. 7.
[30] Mikhail Buinevich and Andrei Vladyko. 2019. Forecasting issues of wireless communication networks' cyber resilience for an intelligent transportation system: An overview of cyber attacks. *Information (Switzerland)* 10, 1 (2019), 27. https://doi.org/10.3390/info10010027
[31] Eko Budi Cahyono, Suriani Binti Mohd Sam, Noor Hafizah Binti Hassan, Norliza Mohamed, Norulhusna Ahmad, and Yusnaidi Yusuf. 2022. A review on cyber resilience model in small and medium enterprises. In *Proceedings of the 4th International Conference on Smart Sensors and Application: Digitalization for Societal Well-Being (ICSSA'22)*. 114–119. https://doi.org/10.1109/ICSSA54161.2022.9870952
[32] Juan F. Carías, Saioa Arrizabalaga, Leire Labaka, and Josune Hernantes. 2020. Cyber resilience progression model. *Applied Sciences (Switzerland)* 10, 21 (2020), 1–32. https://doi.org/10.3390/app10217393

[33] Juan Francisco Carías, Marcos R. S. Borges, Leire Labaka, Saioa Arrizabalaga, and Josune Hernantes. 2020. Systematic approach to cyber resilience operationalization in SMEs. *IEEE Access* 8 (2020), 174200–174221. https://doi.org/10.1109/ACCESS.2020.3026063

[34] Juan Francisco Carías, Leire Labaka, José María Sarriegi, and Josune Hernantes. 2019. Defining a cyber resilience investment strategy in an Industrial Internet of Things context. *Sensors (Switzerland)* 19, 1 (2019), 138.

[35] Sutanay Choudhury, Luke Rodriguez, Darren Curtis, Kiri Oler, Peter Nordquist, Pin Yu Chen, and Indrajit Ray. 2015. Action recommendation for cyber resilience. In *Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig'15)*. 3–8.

[36] Chris McPhee and Omera Khan. 2015. Editorial: Cyber-resilience in supply chains. *Technology Innovation Management Review* 5, 4 (2015), 13–18.

[37] Debora Christine and Mamello Thinyane. 2020. *Cyber Resilience in Asia-Pacific—A Review of National Cybersecurity Strategies*. United Nations University.

[38] Zachary A. Collier, Daniel Dimase, Steve Walters, Mohammad Tehranipoor, Mark, James H. Lambert, and Igor Linkov. 2014. Cybersecurity standards: Managing risk and creating resilience. *Computer* 47, 9 (2014), 70–76. https://doi.org/10.1109/MC.2013.448

[39] William Arthur Conklin. 2017. Teaching cyber resilience for critical infrastructure systems. *Journal of the Colloquium for Information System Security Education* 1 (2017), 1–15.

[40] Megan J. Culler, Justin J. Welch, Jakob P. Meng, Dylan W. Reen, and Kurt S. Myers. 2022. *Cyber-Risk Management Feasibility Study Technologies (RESET)*. Idaho National Laboratory.

[41] Michel Dacorogna, Nehla Debbabi, and Marie Kratz. 2023. Building up cyber resilience by better grasping cyber risk via a new algorithm for modelling heavy-tailed data. *European Journal of Operational Research* 311, 2 (2023), 708–729. https://doi.org/10.1016/j.ejor.2023.05.003

[42] Michal Danilak. 2016. What's the difference between cyber security and cyber resilience? https://ascentor.co.uk/cyber-security-resources/the-difference-between-cyber-security-and-cyber-resilience/

[43] Adrian Davis. 2015. Building cyber-resilience into supply chains. *Technology Innovation Management Review* 5, 4 (2015), 13–18.

[44] Emiliano De Cristofaro, Honglu Du, Julien Freudiger, and Greg Norcie. 2014. A comparative usability study of two-factor authentication. *arXiv:2014.02325* (2014). https://doi.org/10.14722/usec.2014.23025

[45] Frank Dickson and Phil Goodwin. 2019. *Five Key Technologies for Enabling a Cyber-Resilience Framework*. IBM.

[46] Tim Dudman, Antony Waldock, and Steve Barrington. 2017. JUMP: Modelling and simulation of cyber resilience for mission impact assessment. *CEUR Workshop Proceedings* 2040 (March 2017), 22–29.

[47] Benoit Dupont. 2019. The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity* 5, 1 (2019), 1–17.

[48] Edgar Tashiro Yano, Welton De Abreu, Per M. Gustavsson, and Rose-Mharie Åhlfeldt. 2015. A framework to support the development of cyber resiliency with situational awareness capability. In *Proceedings of the 20th International Command and Control Research and Technology Symposium*. 1–11.

[49] Marios P. Efthymiopoulos. 2016. *NATO Smart Defense and Cyber Resilience*. Tufts University.

[50] Eric D. Vugrin and Jennifer Turgeon. 2014. Advancing cyber resilience analysis with performance-based metrics from infrastructure assessments. In *Cyber Behavior: Concepts, Methodologies, Tools, and Applications*. IGI Global, 1–23.

[51] Fabio Ferreira and Marco Tulio Valente. 2023. Detecting code smells in react-based web apps. *Information and Software Technology* 155 (April 2023), 107111. https://doi.org/10.1016/j.infsof.2022.107111

[52] Ivo Friedberg, Kieran McLaughlin, Paul Smith, and Markus Wurzenberger. 2016. Towards a resilience metric framework for cyber-physical systems. In *Proceedings of the 2016 4th International Symposium for ICS and SCADA Cyber Security Research*. 19–22.

[53] Konstantinos Fysarakis, Alexios Lekidis, Vasileios Mavroeidis, Konstantinos Lampropoulos, George Lyberopoulos, Ignasi Garcia Milà Vidal, José Carles Téres I. Casals, Eva Rodriguez Luna, Alejandro Antonio Moreno Sancho, Antonios Mavrelos, Marinos Tsantekidis, Sebastian Pape, Argyro Chatzopoulou, Christina Nanou, George Drivas, Vangelis Photiou, George Spanoudakis, and Odysseas Koufopavlou. 2023. PHOENI2X—A European cyber resilience framework with artificial-intelligence-assisted orchestration, automation and response capabilities for business continuity and recovery, incident response, and information exchange. In *Proceedings of the 2023 IEEE International Conference on Cyber Security and Resilience (CSR'23)*. 538–545. https://doi.org/10.1109/CSR57506.2023.10224995

[54] Darko Galinec and William Steingartner. 2017. Combining cybersecurity and cyber defense to achieve cyber resilience. In *Proceedings of the 2017 IEEE 14th International Scientific Conference on Informatics (INFORMATICS'17)*. 87–93.

[55] Pudong Ge, Boli Chen, and Fei Teng. 2022. Cyber-resilient self-triggered distributed control of networked microgrids against multi-layer DoS attacks. *IEEE Transactions on Smart Grid*. Published Online, December 15, 2022. https://doi.org/10.1109/TSG.2022.3229486

[56] Saira Ghafur, Emilia Grass, Nick R. Jennings, and Ara Darzi. 2019. The challenges of cybersecurity in health care: The UK National Health Service as a case study. *Lancet Digital Health* 1 (2019), e10–e12. https://doi.org/10.1016/S2589-7500(19)30005-6
[57] Viktoria Gisladottir, Alexander A. Ganin, Jeffrey M. Keisler, Jeremy Kepner, and Igor Linkov. 2017. Resilience of cyber systems with over- and underregulation. *Risk Analysis* 37, 9 (2017), 1644–1651.
[58] Harriet Goldman, Rosalie McQuaid, and Jeffrey Picciotto. 2011. Cyber resilience for mission assurance. In *Proceedings of the 2011 IEEE International Conference on Technologies for Homeland Security (HST'11)*. 236–241.
[59] Muhammed Zekeriya Gunduz and Resul Das. 2020. Cyber-security on smart grid: Threats and potential solutions. *Computer Networks* 169 (2020), 107094. https://doi.org/10.1016/j.comnet.2019.107094
[60] Rajesh Gupta, Sudeep Tanwar, Sudhanshu Tyagi, and Neeraj Kumar. 2020. Machine learning models for secure data analytics: A taxonomy and threat model. *Computer Communications* 153 (2020), 406–440.
[61] Eman Hammad, Abhijit Kumar Nag, Anitha Chennamaneni, Mohsen Aghashahi, and Erdogan Dogdu. 2021. A Deep-defense approach for next-gen cyber-resilient inter-dependent critical infrastructure systems. In *Proceedings of Resilience Week 2021 (RWS'21)*. https://doi.org/10.1109/RWS52686.2021.9611790
[62] Md. Ariful Haque, Gael Kamdem De Teyou, Sachin Shetty, and Bheshaj Krishnappa. 2018. Cyber resilience framework for industrial control systems: Concepts, metrics, and insights. In *Proceedings of the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI'18)*. 25–30.
[63] Md. Ariful Haque, Sachin Shetty, and Bheshaj Krishnappa. 2019. ICS-CRAT: A cyber resilience assessment tool for industrial control systems. In *Proceedings of the 5th IEEE International Conference Big Data Security*. 273–281.
[64] Kjell Hausken. 2020. Cyber resilience in firms, organizations and societies. *Internet of Things* 11 (Sept. 2020), 100204.
[65] Lewis Herrington and Richard Aldrich. 2013. The future of cyber-resilience in an age of global complexity. *Politics* 33, 4 (2013), 299–310.
[66] Niamat Hossain, Ibne Ullah, Morteza Nagahi, Raed Jaradat, Chiranjibi Shah, Randy Buchanan, and Michael Hamilton. 2020. Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: A system of systems problem. *Journal of Computational Design and Engineering* 7, 3 (2020), 352–366.
[67] Geoffrey A. Hubbard. 2023. State-level cyber resilience: A conceptual framework. *NASK* 2, 1 (2023), 1–14. https://doi.org/10.5604/01.3001.0053.7401
[68] Helmar Hutschenreuter, Salva Daneshgadeh Çakmakçı, Christian Maeder, and Thomas Kemmerich. 2021. Ontology-based cybersecurity and resilience framework. In *Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP'21)*. 458–466.
[69] Ponemon Institute. 2019. *The Cyber Resilient Organization*. Technical Report. Ponemon Institute. https://www.ibm.com/downloads/cas/GAVGOVNV
[70] Jeffrey Pinckard, Michael Rattigan, and Robert Vrtis. 2016. *A Mapping of the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT) to the Cyber Resilience Review (CRR)*. Carnegie Mellon University.
[71] Joseph Steinberg. 2019. *Cyber-Resilience vs. Cyber-Security: Business Leaders Must Understand the Difference*. Ramsac.
[72] Pöyhönen Jouni, Nuojua Viivi, Lehto Martti, and Rajamäki Jyri. 2018. Application of cyber resilience review to an electricity company. *LAUREA* June (2018), 380–389.
[73] Sathya Prakash Kadhirvelan and Andrew Söderberg-Rivkin. 2014. *Threat Modelling and Risk Assessment*. Master's Thesis. Chalmers University of Technology.
[74] Habeenzu Keleba, Oteng Tabona, and Thabiso Maupong. 2022. Developing a cyber-resilience state in Botswana's energy industry. In *Proceedings of the 2022 International Conference on Smart Applications, Communications, and Networking (SmartNets'22)*. https://doi.org/10.1109/SmartNets55823.2022.9993997
[75] Bissell Kelly, LaSalle Ryan, Dool Floris, and Kennedy-White Joshua. 2018. *Gaining Ground on the Cyber Attacker 2018 State of Cyber Resilience*. Technical Report. Accenture Security. 1–28.
[76] Kevin G. Partridge and Lisa R. Young. 2011. *CERT® Resilience Management Model Publication 800-66 Crosswalk*. Carnegie Mellon University.
[77] Yasir Imtiaz Khan and Ehab Al-shaer. 2015. Cyber resilience-by-construction: Modeling, measuring & verifying. In *Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig'15)*. 9–14.
[78] Sungbeen Kim and Dohoon Kim. 2023. Securing the cyber resilience of a blockchain-based railroad non-stop customs clearance system. *Sensors* 23, 6 (2023), 2914. https://doi.org/10.3390/s23062914
[79] Alissa Knight. 2020. Threat modeling. In *Hacking Connected Cars: Tactics, Techniques, and Procedures*. Wiley, 61–85. https://doi.org/10.1002/9781119491774.ch3
[80] Irina Kolosok and Elena Korkina. 2018. *Cyber Resilience of SCADA at the Level of Energy Facilities*. Atlantis Press.
[81] Alexander Kott, Benjamin Blakely, Diane Henshel, Gregory Wehner, James Rowell, Nathaniel Evans, Luis Muñoz-González, Nandi Leslie, Donald W. French, Donald Woodard, Kerry Krutilla, Amanda Joyce, Igor Linkov, Carmen Mas-Machuca, Janos Sztipanovits, Hugh Harney, Dennis Kergl, Perri Nejib, Edward Yakabovicz, Steven Noel, Tim Dudman, Pierre Trepagnier, Sowdagar Badesha, and Alfred Møller. 2018. Approaches to enhancing cyber resilience: Report of the North Atlantic Treaty Organization (NATO) workshop IST-153. *arXiv:1804.07651* (2018).

[82] Chye Lee, Cher, Guan Tan, Teik, Vishal Sharma, and Jianying Zhou. 2021. Quantum computing threat modelling on a generic CPS setup. In *Applied Cryptography and Network Security Workshops*. Lecture Notes in Computer Science, Vol. 12809. Springer, 171–190.

[83] Hwiwon Lee, Sosun Kim, and Huy Kang Kim. 2022. SoK: Demystifying cyber resilience quantification in cyber-physical systems. In *Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience (CSR'22)*. 178–183. https://doi.org/10.1109/CSR54599.2022.9850312

[84] Oleksandr Lemeshko, Oleksandra Yeremenko, Maryna Yevdokymenko, and Dmytro Ageyev. 2021. Redundancy cyber resiliency technique based on fast rerouting under security metric. In *Proceedings of the 2020 IEEE International Conference on Problems of Infocommunications Science and Technology (PIC S&T'20)*.

[85] Oleksandr Lemeshko, Oleksandra Yeremenko, Maryna Yevdokymenko, Anastasiia Shapovalova, Ahmad M. Hailan, and Amal Mersni. 2019. Cyber resilience approach based on traffic engineering fast reroute with policing. In *Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'19)*. 117–122. https://doi.org/10.1109/IDAACS.2019.8924294

[86] Tingting Li, Cheng Feng, and Chris Hankin. 2018. Improving ICS cyber resilience through optimal diversification of network resources. *arXiv:1811.00142v2* (2018).

[87] Alexandre K. Ligo, Alexander Kott, and Igor Linkov. 2021. How to measure cyber-resilience of a system with autonomous agents: Approaches and challenges. *IEEE Engineering Management Review* 49, 2 (2021), 89–97.

[88] Igor Linkov, Daniel A. Eisenberg, Matthew E. Bates, Derek Chang, Matteo Convertino, Julia H. Allen, Stephen E. Flynn, and Thomas P. Seager. 2013. Measurable resilience for actionable policy. *Environmental Science and Technology* 47, 18 (2013), 10108–10110.

[89] Igor Linkov, Daniel A. Eisenberg, Kenton Plourde, Thomas P. Seager, Julia Allen, and Alex Kott. 2013. Resilience metrics for cyber systems. *Environment Systems and Decisions* 33, 4 (2013), 471–476.

[90] Igor Linkov and Alexander Kott. 2019. *Cyber Resilience of Systems and Networks*. Risk, Systems and Decisions Series. Springer.

[91] Guy Lloyd. 2020. The business benefits of cyber security for SMEs. *Computer Fraud and Security* 2020, 2 (Feb. 2020), 14–17.

[92] Georgia Lykou, Argiro Anagnostopoulou, and Dimitris Gritzalis. 2018. Implementing cyber-security measures in airports to improve cyber-resilience. In *Proceedings of the 2018 Global Internet of Things Summit (GIoTS'18)*. 1–6.

[93] Georgia Lykou, Argiro Anagnostopoulou, and Dimitris Gritzalis. 2019. Smart airport cybersecurity: Threat mitigation and cyber resilience controls. *Sensors (Switzerland)* 19, 1 (2019), 19.

[94] Alan Magar. 2016. *State-of-the-Art in Cyber Threat Models and Methodologies*. Sphyma Security. http://cradpdf.drdc-rddc.gc.ca/PDFS/unc225/p803699_A1b.pdf

[95] Alex Mathew. 2019. Airport cyber security and cyber resilience controls. *arXiv:1908.09894* (2019).

[96] Hellen Maziku and Sachin Shetty. 2017. Software defined networking enabled resilience for IEC 61850-based substation communication systems. In *Proceedings of the 2017 International Conference on Computing, Networking, and Communications (ICNC'17)*. 690–694.

[97] Sukarno Mertoguno, Ryan M. Craven, Matthew S. Mickelson, and David P. Koller. 2019. A physics-based strategy for cyber resilience of CPS. In *Proceedings of SPIE 11009, Autonomous Systems: Sensors, Processing, and Security for Vehicles and Infrastructure*.

[98] Jan Meszaros and Alena Buchalcevova. 2017. Introducing OSSF: A framework for online service cybersecurity risk management. *Computers and Security* 65 (2017), 300–313.

[99] Microsoft Docs. 2017. *Microsoft Threat Modeling Tool Overview—Azure*. Microsoft.

[100] Michael Mylrea, Sri Nikhil Gupta Gourisetti, and Andrew Nicholls. 2018. An introduction to buildings cybersecurity framework. In *Proceedings of the 2017 IEEE Symposium on Computational Intelligence (SCCI'17)*. 1–7. https://doi.org/10.1109/SSCI.2017.8285228

[101] N-Stalker. 2010. N-Stalker the Web Security Specialists. Retrieved July 22, 2021 from https://www.nstalker.com/

[102] Sajid Nazir, Hassan Hamdoun, and Jafar Alzubi. 2015. Cyber attack challenges and resilience for smart grids. *European Journal of Scientific Research* 134, 1 (2015), 111–120.

[103] Steven Noel, Deborah Bodeau, and Rosalie McQuaid. 2017. Big-data graph knowledge bases for cyber resilience. *CEUR Workshop Proceedings* 2040, 17 (2017), 6–21.

[104] S. Noel, E. Harley, K. H. Tam, M. Limiero, and M. Share. 2016. CyGraph: Graph-based analytics and visualization for cybersecurity. *Handbook of Statistics* 35 (2016), 117–167.

[105] Obiora Nweke, Livinus and Stephen D. Wolthusen. 2020. A review of asset-centric threat modelling approaches. *International Journal of Advanced Computer Science and Applications* 11, 2 (2020), 1–6. https://www.ijacsa.thesai.org

[106] Riku Nykänen and Tommi Kärkkäinen. 2016. Supporting cyber resilience with semantic wiki. In *Proceedings of the 12th International Symposium on Open Collaboration (OpenSym'16)*. 35.

[107] The Department of Homeland Security's (DHS) Office of Cybersecurity & Communications. 2011. *Cyber Resilience Review*. Technical Report. DHS. https://www.dhs.gov/pcii
[108] Cyril Onwubiko. 2020. Focusing on the recovery aspects of cyber resilience. In *Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics, and Assessment (CyberSA'20)*. https://doi.org/10.1109/CyberSA49311.2020.9139685
[109] OSSEC Project Team. 2019. OSSEC—World's Most Widely Used Host Intrusion Detection System—HIDS. Retrieved March 1, 2024 from https://www.ossec.net/
[110] João Pavão, Rute Bastardo, Dário Carreira, and Nelson Pacheco Rocha. 2023. Cyber resilience, a survey of case studies. *Procedia Computer Science* 2019 (2023), 312–318. https://doi.org/10.1016/j.procs.2023.01.295
[111] Ponemon Institute. 2018. *The Third Annual Study on the Cyber Resilient Organization: Asia-Pacific*. Ponemon Institute.
[112] Greg Porter, Heinz College, and Robert A. Vrtis. 2018. *A Mapping of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule to the Cyber Resilience Review (CRR)*. Carnegie Mellon University.
[113] Ika Riswanti Putranti. 2015. Developing of cyber resilience system of the international trade facilitations: Specific reference Indonesia. *Indonesia National Resilience Institute* 9, 3 (2015), 1–28.
[114] Yanfeng Qu, Gong Chen, Xin Liu, Jiaqi Yan, Bo Chen, and Dong Jin. 2020. Cyber-resilience enhancement of PMU networks using software-defined networking. In *Proceedings of the 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm'20)*. https://doi.org/10.1109/SmartGridComm47815.2020.9303004
[115] Raddad Ayoub, Clinton M. Firth, and Mohamed Nayaz. 2017. *Cyber Resilience in the Digital Age*. Technical Report. EY.
[116] Sazid Rahman, Niamat Ullah Ibne Hossain, Kannan Govindan, Farjana Nur, and Mahathir Bappy. 2021. Assessing cyber resilience of additive manufacturing supply chain leveraging data fusion technique: A model to generate cyber resilience index of a supply chain. *CIRP Journal of Manufacturing Science and Technology* 35 (2021), 911–928. https://doi.org/10.1016/j.cirpj.2021.09.008
[117] Ghulam Rasool, Sajid Iqbal, Shafiq Hussain, Asif Kamal, and Shabir Ahmad. 2014. Threat modelling methodologies: A survey. *Science International (Lahore)* 26, 4 (2014), 1607–1609.
[118] Reza Arghandeh, Alexandra Meier, Laura Mehrmanesh, and Lamine Mili. 2016. On the definition of cyber-physical resilience in power systems. *Renewable and Sustainable Energy Reviews* 58 (2016), 1060–1069.
[119] Craig G. Rieger. 2014. Resilient control systems practical metrics basis for defining mission impact. In *Proceedings of the 7th International Symposium on Resilient Control Systems (ISRCS'14)*.
[120] Álvaro Rocha, Ana Maria Correia, Sandra Costanzo, and Luís Paulo Reis. 2015. Open source backup systems for SMEs. In *New Contributions in Information Systems and Technologies*. Advances in Intelligent Systems and Computing, Vol. 353. Springer, III–IV. https://doi.org/10.1007/978-3-319-16486-1
[121] A. Rose, N. Miller, S. Chatterjee, and R. Brigantic. 2017. *Measurement of Cyber Resilience from an Economic Perspective*. University of Southern California.
[122] RSI Security. 2020. Cyber Security Resilience Framework: How to Get Started. Retrieved March 1, 2024 from https://blog.rsisecurity.com/cyber-security-resilience-framework-how-to-get-started/
[123] Abhijeet Sahu, Venkatesh Venkatraman, and Richard Macwan. 2023. Reinforcement learning environment for cyber-resilient power distribution system. *IEEE Access* 11 (2023), 127216–127228. https://doi.org/10.1109/ACCESS.2023.3282182
[124] Paul Saitta, Brenda Larcom, and Michael Eddington. 2005. Trike v.1 methodology document. Draft. OCTOTRIKE.
[125] Daniel A. Sepúlveda-Estay, Rishikesh Sahay, Michael B. Barfod, and Christian D. Jensen. 2020. A systematic review of cyber-resilience assessment frameworks. *Computers & Security* 97 (2020), 101996. https://doi.org/10.1016/j.cose.2020.101996
[126] Nataliya Shevchenko, Timothy A. Chick, Paige O. Riordan, Thomas Patrick Scanlon, and Carol Woody. 2018. *Threat Modelling: A Summary of Available Methods*. Carnegie Mellon University, Software Engineering Institute.
[127] Francesco Simone, Antonio Javier Nakhal Akel, Giulio Di Gravio, and Riccardo Patriarca. 2023. Thinking in systems, sifting through simulations: A way ahead for cyber resilience assessment. *IEEE Access* 11 (Jan. 2023), 11430–11450. https://doi.org/10.1109/ACCESS.2023.3241552
[128] Sidney Smith. 2023. Towards a scientific definition of cyber resilience. In *Proceedings of the International Conference on Cyber Warfare and Security*, Vol. 18. 379–386. https://doi.org/10.34190/iccws.18.1.960
[129] Stuart Rance. 2014. *Cyber Resilience: Bridging the Business and Technology Divide*. White Paper. AXELOS.
[130] Dan Jerker B. Svantesson. 2023. Australia's cyber security reform—An update. *International Cybersecurity Law Review* 4 (2023), 347–350. https://doi.org/10.1365/s43439-023-00087-w
[131] Dabeeruddin Syed, Abdullah Hussein Al-Ghushami, Ameema Zainab, Shafii Muhammad Abdulhamid, and Mohammed Salem Daen A. Al-Kuwari. 2023. Information security using GNU privacy guard. In *Proceedings of the 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC'23)*. 295–300. https://doi.org/10.1109/CCWC57344.2023.10099196

[132] Pardis Moslemzadeh Tehrani. 2019. Cyber resilience strategy and attribution in the context of international law. In *Proceedings of the European Conference on Information Warfare and Security (ECCWS'19)*. 501–507.
[133] Russ McRee. 2014. Toolsmith Microsoft threat modeling tool 2014: Identify & mitigate. *ISSA Journal* 2014 (May 2014), 39–42.
[134] Heli Tiirmaa-Klaar. 2016. Building national cyber resilience and protecting critical information infrastructure. *Journal of Cyber Policy* 1, 1 (2016), 94–106.
[135] Tobias Kiesling and Marcus Kreuzer. 2017. Recommendations to Strengthen the Cyber-Resilience of the Air Traffic System. Retrieved March 1, 2024 from http://lb-campus.de/images/content/ARIEL_Recommendations_v2.0.pdf
[136] Branislav Todorovic, Darko Trifunovic, Katarina Jonev, and Marina Filipovic. 2016. Resilience and evolution—Angola banking survey. *University of Belgrade* 9, 1 (2016), 41–45. https://doi.org/10.1007/978-94-024-1123-2
[137] Tony Ucedavélez and Marco M. Morana. 2015. *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. Wiley.
[138] Attiq Ur-Rehman, Joarder Kamruzzuman, Iqbal Gondal, and Alireza Jolfaei. 2022. Cyber resilience modelling for the operations of hybrid network. In *Proceedings of the 2022 IEEE International Symposium on Dependable, Autonomic, and Secure Computing (DASC'22)*. 1–7. https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9928023
[139] Luca Urciuoli. 2015. Cyber-resilience: A strategic approach for supply chain management. *Technology Innovation Management Review* 5, 4 (2015), 13–18.
[140] Alexandr Vasenev, Florian Stahl, Hayk Hamazaryan, Zhendong Ma, Lijun Shan, Joerg Kemmerich, and Claire Loiseaux. 2019. Practical security and privacy threat analysis in the automotive domain: Long term support scenario for over-the-air updates. In *Proceedings of the 5th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS'19)*. 550–555.
[141] Wenjun Xiong. 2021. *Enhancing IT Systems Cyber Resilience through Threat Modeling: Cyber Security Analysis of Enterprise Systems and Connected Vehicles*. Ph.D. Thesis. KTH Royal Institute of Technology.
[142] Patricia Williams. 2010. *Is Cyber Resilience in Medical Practice Security Achievable?* Edith Cowan University.
[143] Patricia Williams and Rachel J. Manheke. 2010. Small business—A cyber resilience vulnerability. In *Proceedings of the International Cyber Resilience Conference*.
[144] World Economic Forum. 2012. *Partnering for Cyber Resilience*. World Economic Forum.
[145] Xavier J. Merino Aguilera. 2017. *Managed Containers for Increased Cyber-Resilience*. Master's Thesis. Florida Institute of Technology.
[146] Weitao Yao, Yu Wang, Yan Xu, and Chao Deng. 2023. Cyber-resilient control of an islanded microgrid under latency attacks and random DoS attacks. *IEEE Transactions on Industrial Informatics* 19, 4 (2023), 5858–5869. https://doi.org/10.1109/TII.2022.3191315
[147] Jin Ye, Annarita Giani, Ahmed Elasser, Sudip K. Mazumder, Chris Farnell, Homer Alan Mantooth, Taesic Kim, Jianzhe Liu, Bo Chen, Gab-Su Seo, Wenzhan Song, Mateo D. Roig Greidanus, Subham Sahoo, Frede Blaabjerg, Jinan Zhang, Lulu Guo, Bohyun Ahn, Mohammad B. Shadmand, Nanditha R. Gajanur, and Mohammad A. Abbaszada. 2021. A Review of cyber-physical security for photovoltaic systems. *IEEE Journal of Emerging and Selected Topics in Power Electronics*. Published Online, September 10, 2021.
[148] Bo Zou, Pooria Choobchian, and Julie Rozenberg. 2020. *Cyber Resilience of Autonomous Mobility Systems: Cyber Attacks and Resilience-Enhancing Strategies*. Policy Research Working Papers. World Bank Group.

Received 1 September 2022; revised 29 December 2023; accepted 31 January 2024