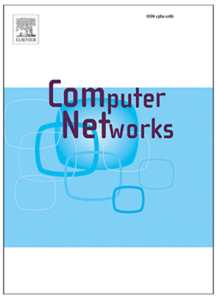
Journal Pre-proof



Towards a cyber resilience quantification framework (CRQF) for IT infrastructure

Saleh Mohamed AlHidaifi, Muhammad Rizwan Asghar, Imran Shafique Ansari

PII: S1389-1286(24)00278-0
DOI: https://doi.org/10.1016/j.comnet.2024.110446
Reference: COMPNW 110446

To appear in: *Computer Networks*

Received date : 23 October 2023
Revised date : 11 March 2024
Accepted date : 18 April 2024

Please cite this article as: S.M. AlHidaifi, M.R. Asghar and I.S. Ansari, Towards a cyber resilience quantification framework (CRQF) for IT infrastructure, *Computer Networks* (2024), doi: https://doi.org/10.1016/j.comnet.2024.110446.

Towards a Cyber Resilience Quantification Framework (CRQF) for IT Infrastructure

Saleh Mohamed AlHidaifi[a,*], Muhammad Rizwan Asghar[b,c], Imran Shafique Ansari[a]

[a] James Watt School of Engineering, University of Glasgow, G12 8LT, Glasgow, The United Kingdom.
[b] School of Computer Science and Electronic Engineering, University of Surrey, GU2 7XH, Guildford, United Kingdom.
[c] School of Computer Science, The University of Auckland, Auckland 1142, Auckland, New Zealand.

Abstract

Cyber resilience quantification is the process of evaluating and measuring an organisation's ability to withstand, adapt to, and recover from cyber-attacks. It involves estimating IT systems, networks, and response strategies to ensure robust defence and effective recovery mechanisms in the event of a cyber-attack. Quantifying cyber resilience can be difficult due to the constantly changing components of IT infrastructure. Traditional methods like vulnerability assessments and penetration testing may not be effective. Measuring cyber resilience is essential to evaluate and strengthen an organisation's preparedness against evolving cyber-attacks. It helps identify weaknesses, allocate resources, and ensure the uninterrupted operation of critical systems and information. There are various methods for measuring cyber resilience, such as evaluating, teaming and testing, and creating simulated models. This article proposes a cyber resilience quantification framework for IT infrastructure that utilises a simulation approach. This approach enables organisations to simulate different attack scenarios, identify vulnerabilities, and improve their cyber resilience. The comparative analysis of cyber resilience factors highlights pre-configuration's robust planning and adaptation (61.44%), buffering supported's initial readiness (44.53%), and network topologies' robust planning but weak recovery and adaptation (60.04% to 77.86%), underscoring the need for comprehensive enhancements across all phases. The utilisation of the proposed factors is crucial in conducting a comprehensive evaluation of IT infrastructure in the event of a cyber-attack.

Keywords:
Cyber Resilience, Cybersecurity, Cyber-attacks, Framework, Quantification, and OMNeT++ Simulator.

1. Introduction

According to the report by IBM in 2023, [1] reveals that 51% of organisations plan to increase their security investments due to a breach. Despite the rising costs of data breaches, the report found that respondents were almost equally divided on whether to increase security investments after experiencing a data breach. The top areas for additional investments include incident response planning and testing, employee training, and threat detection and response technologies. According to the report, attack surface management can quickly improve an organisation's cyber resilience by managing the expansion of the digital footprint. Additionally, organisations should consider implementing specific network topologies and network segmentation practices to limit the spread of attacks and reduce the extent of damage they can cause, thereby improving overall resiliency and minimising recovery efforts.

Cyber resilience involves a system's ability to prepare, absorb, recover, and adapt its performance to pre-cyber-attack levels. In comparison, cyber security focuses on preparing for, protecting against, and detecting cyber-attacks. Cyber resilience is all about responding and quickly recovering from them. In designing a resilient system, it is essential to acknowledge that attackers may succeed in breaching the system and plan for how to get it back up and running. Cyber resilience aims to maintain the system's ability to achieve its intended outcomes [2].

*Corresponding author.
Email addresses: s.al-hidaifi.1@research.gla.ac.uk (Saleh Mohamed AlHidaifi), r.asghar@surrey.ac.uk, r.asghar@auckland.ac.nz (Muhammad Rizwan Asghar), imran.ansari@glasgow.ac.uk (Imran Shafique Ansari)

Existing methods for quantifying cyber resilience often focus on specific components or aspects of IT infrastructure, such as vulnerability assessment or incident response planning. Traditional risk assessment and management processes focus on measuring the probability of system failure in response to well-defined threats, but this does not capture the full concept of cyber resilience [3]. These methods can help to provide valuable insights; they need to account for the broader context of cyber resilience. Most assessment and quantification approaches techniques have limitations concerning measuring cyber-resilience and may not be suitable for measuring the overall effectiveness of cyber resilience in IT infrastructure [4].

To address this gap, this paper proposes a Cyber Resilience Quantification Framework (CRQF) for IT infrastructure that combines the phases of cyber resilience and the factors that affect cyber resilience. The phases of cyber resilience include planning/preparing, absorbing, recovering, and adapting. In contrast, the factors that affect cyber resilience include managing complexity, network topology, adding resources, IT infrastructure pre-configuration, and buffering support.

This study includes main contributions as follows: 1) we provide a comparative analysis of previous research frameworks for quantifying resilience while highlighting limitations therein; 2) define and explain the phases of cyber resilience; 3) propose and describe the main five factors of cyber resilience that affect cyber resilience quantification; 4) explain the capacities of cyber resilience; 5) design the initial framework called CRQF; and 6) simulate and evaluate the factors of cyber resilience proposed with the initial framework proposed.

The proposed framework addresses the need for a broad, standardised approach to quantifying cyber resilience in IT infrastructure networks or systems. The framework is based on a simulation approach, enhancing cyber resilience by testing the environment rather than formal assessment or testing methods. This work defines and measures cyber resilience's phases, factors, and capacities. This enhances the understanding of cyber resilience and provides a standardised approach to its quantification. Additionally, the proposed factors enable organisations to prioritise cyber resilience factors based on their relative importance.

The simulation-based testing of the framework provides an accurate and effective method for evaluating the effectiveness of cyber resilience measures. This can help organisations identify areas of weakness and make informed decisions about investing in cyber resilience strategies. Overall, this work contributes to cyber resilience by providing a comprehensive and standardised approach to quantifying cyber resilience in IT infrastructure. Organisations can use the proposed framework to improve their cyber resilience and protect against cyber-attacks.

In Section 1.2, we discuss some previous resilience frameworks. The cyber resilience phases are presented in Section 2.1. In Section 2.2, we address the main three capacities of cyber resilience. In Section 2.3, we propose and explain five factors that affect cyber resilience. In Section 3, we present the novel framework for quantifying cyber resilience. In Section 4, we simulate the proposed framework and generate the results to discuss the significance of the proposed factors. In Section 5, we conclude and discuss future directions.

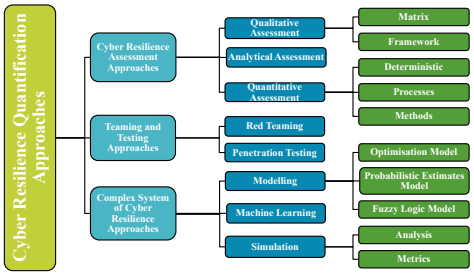


Figure 1: Approaches of cyber resilience quantification.

1.1. Definitions of Cyber Resilience

Cyber resilience refers to resisting and recovering from cyber-attacks. Measuring and evaluating a system or organisation's ability to withstand and recover from cyber-attacks can be quantified, as defined in [5] and [6]. Other definitions of cyber resilience focus on the organisational or system levels. However, these definitions have some fundamental differences. Several studies have been conducted on cyber resilience at the organisational level, such as those in [7]–[10] defined cyber resilience as an organisation's ability to defend against cyber-attacks based on three factors: prevention, detection, and response. Each of these factors has a specific resilience factor: prevention for anticipating, detection for monitoring and learning, and incident reporting response. However, this definition is limited to more than just describing cyber resilience based on cyber-attacks without considering what happens after a successful attack.

Table 1: **Comparison of various frameworks for quantifying resilience.**

Solution / Approach	Year	Objectives	Methodology	Key Features	Advantages Over Existing Research	Evaluation Techniques	Similarities	Differences
Cassottana *et al.* [11]	2023	Quantify CPS resilience before and after disruptions	Modeling	Three-step framework: CPS description, disruption scenario identification, resilience strategy selection	Offers a standardised workflow and comprehensive set of metrics for resilience assessment in CPS environments	Metrics	-	Focuses on CPS, emphasises systematic modelling and strategy selection
Jiang *et al.* [12]	2021	Evaluate network resilience during cyber-attacks and recoveries	Modeling	Dynamic Bayesian Network (DBN) approach	Provides accurate and comprehensive resilience assessment during cyber-attacks and recoveries	DBN	Similar evaluation techniques	Focuses on network resilience, employs DBN for modeling
Marino and Zio [13]	2021	Quantify resilience in gas pipeline transmission networks	Systematic	Highest flow algorithm for gas network supply capacity computation	Quantifies resilience in gas pipeline transmission networks, facilitating system robustness and recovery anticipation	Metrics	-	Addresses resilience in gas pipeline networks, utilises sensitivity analysis
Das *et al.* [14]	2020	Address multi-modal cyber-physical attacks and critical infrastructure interdependencies	Holistic	Analysis of smart grid elements, configurations, and environmental factors	Addresses multi-modal cyber-physical attacks and critical infrastructure interdependencies, offering insights into resilience decision-making	Metrics	Similar holistic approach	Focuses on smart grids and critical infrastructure
Hossain *et al.* [15]	2019	Conceptualise resilience in interdependent electrical infrastructure systems	Conceptual	Case study approach with Bayesian Network (BN) analysis	Provides a conceptual framework for quantifying resilience in interdependent electrical infrastructure systems, enhancing system reliability and resource restoration	BN	Similar conceptual framework	Focuses on interdependent electrical infrastructure systems, utilises BN
Yodo and Wang [16]	2016	Assess resilience in engineered systems	Conceptual	Bayesian Network (BN) used for resilience quantification	Empowers system designers to better grasp system weaknesses and strengths against disruptive events, improving engineering resilience	BN	Similar use of BN	Focuses on engineered systems, emphasises engineering resilience

Continued from previous page

Solution / Approach	Year	Objectives	Methodology	Key Features	Contributions	Evaluation Techniques	Similarities	Differences
Hosseini *et al.* [17]	2016	Quantify resilience drivers in supply chains	Conceptual	Case study analysis with Bayesian Network (BN)	Quantifies system resilience drivers and enhances qualitative measurement, aiding in resilience capacity design and cost evaluation	BN	Similar use of BN	Focuses on supply chains, emphasises resilience drivers
Yodo and Wang [18]	2016	Analyse resilience in engineered systems	Conceptual	Resilience analysis using engineering metrics	Offers a comprehensive resilience analysis approach using engineering metrics, aiding in system reliability and recovery assessment	Metrics	-	Focuses on engineered systems, emphasises engineering metrics
Francis and Bekera [19]	2014	Assess resilience in critical infrastructures	Conceptual	Structured framework for resilience assessment	Provides a structured framework for resilience assessment in critical infrastructures, facilitating system identification and vulnerability analysis	Metrics	Similar structured framework	Focuses on critical infrastructures, emphasises resilience assessment

While cyber resilience has been defined as a system-level concept by researchers, its application at the organisational level has yet to be fully considered. According to Vugrin and Turgeon [20], resilience refers to a system's ability to efficiently recover from a disruptive event or set of circumstances that affect its performance. However, this definition solely focuses on technical issues and excludes human errors. In contrast, Todorovic *et al.* [21] address this gap by defining cyber resilience as a system's inherent capacity to respond to short-term and long-term changes. This includes identifying areas for improvement, adapting to potential disruptions, anticipating and absorbing them, and quickly recovering from them, whether caused by humans or nature.

Several studies in the literature have explored the concept of cyber resilience at organisational and system levels. Cyber resilience refers to an organisation's ability to anticipate, withstand, recover from, and adapt to cyberspace attacks, stresses, conditions, and compromises. This term can denote the capability of an organisation, a business function, a mission, a system, a system-of-systems, or a cross-organisational mission. This versatile concept can be applied to various entities, including nations, regions, groups, households, or individuals. The definition of cyber resilience is discussed in multiple studies such as [22]–[25].

1.2. Comparative Analysis of Resilience Frameworks

There are various methods to measure cyber resilience, broadly classified into three main categories as illustrated in Figure 1. These approaches provide a valuable framework to quantify and understand the concept of cyber resilience. It may be summarised as: 1) cyber resilience assessment approaches such as analytical assessment, qualitative assessment, and quantitative assessment; 2) teaming and testing approaches; 3) complex cyber resilience approaches such as simulation, machine learning, and modelling, including probabilistic estimates model, optimisation model, and fuzzy logic model. This research will combine a complex cyber resilience approach and a cyber resilience assessment approach for accurate cyber resilience simulation quantification by proposing a framework.

In this section, we will focus on the framework approach and compare various quantification resilience frameworks to help us propose our framework. We describe and analyse each individually and showcase their comparison, as demonstrated in Table 1. The Dynamic Bayesian Network (DBN) is used for designing a novel quantification framework for quantifying network resilience [12]. The framework can measure a network's resilience during multiple-stage cyber-attacks and recoveries. It can evaluate various performances of processes like processing preparation, resistance, adaptation, recovery, and evolution. Additionally, the framework can work with resilience network capacities to describe the resilient networking processes.

This section undertakes a comparative analysis of various resilience frameworks, including our proposed approach, aiming to identify key features and elucidate both similarities and differences to underscore the advantages of our methodology over existing research.

Application domain: Our proposed framework is tailored to quantifying cyber resilience in IT infrastructure, explicitly focusing on assessing resilience levels before and after disruptions, as articulated by Cassottana *et al.* [11]. Conversely, Jiang *et al.* [12] evaluate network resilience amidst cyber-attacks and recoveries, whereas Marino and Zio [13] direct their efforts toward enhancing resilience within gas pipeline transmission networks. Moreover, existing frameworks discussed within our work target a diverse array of domains, including smart grids, power systems, and engineered systems, as evidenced by the works in [14], [15], and [16].

Type of framework: Our framework adopts a modelling-centric approach akin to that in [12] and [13], integrating systematic analysis and metric-based evaluations for resilience assessment in alignment with the work by Cassottana *et al.* [11]. Concurrently, conceptual frameworks, exemplified by those proposed in [15] and [19], aim to conceptualise resilience capacities and metrics.

Methods and evaluation techniques: Our framework incorporates methodologies encompassing IT infrastructure description, attack scenario identification, and resilience factor selection bolstered by a comprehensive set of evaluation metrics, as advocated by Cassottana *et al.* [11]. Analogously, comparable evaluation techniques are leveraged by other frameworks, including DBN in the work of Jiang *et al.* [12], sensitivity analysis as demonstrated by Marino and Zio [13], and Bayesian Network (BN) in studies conducted in [15] and [16].

Advantages over existing research: Our framework offers a holistic approach to quantifying IT infrastructure resilience, encompassing before and after attack scenarios through a systematic modelling and evaluation process outlined by Cassottana *et al.* [11]. In contrast to existing frameworks, our approach provides a standardised workflow and comprehensive metrics for resilience assessment, thereby streamlining decision-making processes and strategy selection within Cyber-

Physical Systems (CPS) environments.

Evidence and examples: Empirical evidence from case studies and simulation experiments underscores the effectiveness and universality of our proposed framework, validating its accuracy and comprehensiveness in quantifying resilience within CPS, as illustrated by Cassottana *et al.* [11].

Jiang *et al.* [12] present a framework for evaluating the resilience of temporal networks. The authors identified five key network performance indicators and quantified them using a DBN approach. Through simulation experiments, they demonstrated the effectiveness and universality of their proposed evaluation framework. Their study showed that the proposed method is more accurate and comprehensive than previous approaches when applied to network scenarios under various attack and recovery intensities. The authors provide valuable insights into network resilience and can help develop more effective network management and security strategies.

An original resilience analysis framework is provided for a complex gas pipeline transmission network, viewing the interdependence cybernetic of the physical gas pipeline network with the Supervisory Control And Data Acquisition (SCADA) system in [13]. The highest flow algorithm computes the gas network supply capacity. When a failure occurs, such as cyber-attacks, the pressure of the network nodes and the gas supply capacity change, leading to discontentment with customer demands.

The framework allowed quantifying the resilience value through characteristic performance metrics [13]. The SCADA communication network implemented in Network Simulator provides the necessary information regarding the data delay packets arriving from the sensors along the pipelines. The packet delay value evaluates the time the SCADA system blocks the remote control valves to keep the pipelines under pressure when a failure occurs. Essential insights into the resilience model are obtained through a systematic sensitivity analysis (SA) framework customised for gas pipeline transmission networks. Specifically, they investigated the model's influence on network robustness and recovery anticipation.

The individual parameters and group effects formed by inputs with similar functionalities provide helpful information, such as how the supervisory SCADA system interconnection affects the degradation and recovery process of the physical gas pipeline network. The case study results confirm that gas transmission networks are vulnerable to cyber and physical disappointments, pointing to the need for systemic analysis methods to manage the system's resilience.

One of the reviewed and comparatively in-detailed quantification resilience frameworks and quantitative metrics for studying resilience is presented by Das *et al.* [14]. They highlighted the desirable properties of a resilience metric and the challenges associated with discussing, formulating, developing, and calculating such a metric in practical scenarios. The authors summarised future research routes in developing a holistic framework for quantifying resilience and focusing on challenges related to multi-modal cyber-physical attacks, significant data-related issues, and interdependence of critical infrastructures.

One of the quantification resilience frameworks that systematise existing knowledge on CPSs analysis was proposed by Cassottana *et al.* [11]. Specifically, they focus on measuring and quantifying CPSs before and after the cyber-attack or occurrence of a disruption. Through the systematic analysis of the models and methods adapted in their literature, they developed a CPS resilience estimation framework consisting of three steps, namely, (1) CPS description, (2) disruption scenario identification, and (3) resilience strategy selection. For each step of the framework, they suggest established methods for CPS analysis and four criteria for method selection. The framework proposes a standardised workflow to evaluate the resilience of CPSs before and after the cyber-attack. The proposed framework application is exemplified regarding a power substation and associated communication network. The proposed framework case study supports resilience decision-making by quantifying the effects of implementing resilience strategies.

The authors in [15] presented utilisation using a BN to address possible risks to the power system and its interdependent electrical networks. It offers possible options to mitigate the consequences of a disruption. The interdependent electrical infrastructure system in Washington, DC, is used as a case study to quantify the BN's resilience. Quantification of resilience is further analysed based on different types of analysis such as forward propagation, backward propagation, sensitivity analysis, and information theory. The general insight drawn from these analyses indicates that reliability, backup power source, and resource restoration are the prime factors that enhance the resilience of an interdependent electrical infrastructure system.

The first conceptual framework proposed for modelling engineering resilience is presented by Yodo and Wang [16]. It aims to bridge the gap between quantitative and qualitative resilience measures in designing industrial systems. Then, BN is employed as a quanti-

tative tool for assessing and analysing the resilience of engineered systems. Two industrial-based case studies, supply chain and production process, demonstrate the proposed approach. The proposed resilience quantification and analysis approach using BNs would empower system designers to better grasp their systems' weaknesses and strengths against system disruptions induced by adverse failure events.

Hosseini *et al.* [17] explored the key drivers contributing to designing resilient supply chains based on the three capacities: absorptive, adaptive and restorative. Many phases will help design a conceptual framework, such as threat analysis, cyber resilience capacity design, cost evaluation, quantification, and improvement. The main challenge to the current literature on system resilience is qualitative measurement. The current literature indicates that many of the drivers of system resilience are qualitative, such as staff cooperation and collaboration during disruptive events and the level of preparation against natural disasters.

The authors in [17] employed a BN to quantify the system's resilience to fill the quantitative and qualitative gaps. The BN is a rigorous tool for measuring risks under uncertainty, representing dependency between causes and effects, and making particular types of reasoning. Additionally, it can handle both qualitative and quantitative variables regarding probability. They have been defined and implemented in different scenarios to identify critical variables susceptible to sulfuric acid manufacturers' system resilience.

A framework for analysing resilience includes a metric for measuring it, as demonstrated by Francis and Bekera [19]. The framework reviewed various approaches to defining and quantifying resilience. Also, it has been seen that while resilience is a valuable concept, its diversity in usage complicates its interpretation and measurement. The framework includes system identification, resilience objective setting, vulnerability analysis, and stakeholder engagement. The implementation of the framework is focused on achieving three resilience capacities: adaptive capacity, absorptive capacity, and recoverability capacity.

Furthermore, the three capacities proposed in [19] have formed the basis of their proposed resilience factor and uncertainty-weighted resilience metric. Likewise, they have identified two critical unresolved discussions for emerging the resilience idea as an epistemological versus inherent property both of the system and the design for ecological versus engineered resilience in socio-technical systems. While they have not resolved their tension, they have shown that their framework and metric promote the methodologies for investigating "deep" uncertainties in resilience quantification. At the same time, they retain the probability of expressing uncertainties about highly uncertain, unforeseeable, or unknown hazards in design and management activities.

A comprehensive understanding of the historical development of cyber resilience is necessary due to the increasing frequency and complexity of cyber threats, as proposed by Tzavara and Vassiliadis [26]. It explores the definition of cyber resilience and its critical components and traces its origin to the early 2000s. The study analyses the significant events and milestones that have influenced the evolution of cyber resilience, taking into account technological advancements and societal factors up to the outbreak of the COVID-19 pandemic. The authors also highlight the recognition of cyber resilience as a critical component of cyber security strategy across diverse public and private sectors. By analysing the historical and contextual factors that influenced the concept, this report provides insights into future challenges for ensuring the resilience of digital infrastructure.

A resilience glossary containing 93 definitions of terms related to critical infrastructures is presented by Mentges *et al.* [27]. The definitions and use of these terms, including resilience, show significant variability in the literature. The authors use multiple published definitions, integrate contrasting views, compare terms, and provide precise terminology references to improve resilience. The understanding of resilience outlined in the glossary supports the practical assessment and management of the resilience of critical infrastructures. Resilience refers to the ability of a system to handle unexpected disruptions and their impacts. This ability comprises three pillar capacities, and their quality can be extracted from performance curves. Learning capacity plays a role in increasing the performance of a system after a disruptive event.

Christine and Thinyane [28] explore the socio-technical shortcomings in cyber resilience management frameworks proposed in academic literature. Cyber resilience management frameworks serve as the standard for organisations to build or improve their cyber resilience posture. However, most frameworks have primarily employed a techno-centric approach. The authors conceptualise organisational cyber resilience from the perspectives of the socio-technical system. The systematic analysis aims to identify the extent of inclusion of socio-technical systems thinking in cyber resilience management frameworks and proposes potential future research directions.

The authors in [28] discuss the Socio-technical Systems (STS) theory, the framing of organisations and cy-

Table 2: **A description of the Cyber Resilience phases: plan / prepare, absorb, recover, and adapt.**

Phase	Description	Objectives	Key Activities	Key Outcomes	Main Stakeholders	Key Tools / Technologies
Plan	Proactive preparation for cyber-attacks	Identify risks, develop response plans, and establish controls	Risk assessment and incident response planning	Enhanced preparedness and defined response plans	IT/security teams and risk management	Risk assessment tools and incident response plan templates
Absorb	Detect and contain the impact of cyber-attacks	Real-time cyber-attack detection to minimise the effect	Implement security controls and continuous monitoring	Timely detection and containment of cyber-attacks	Security Operations Centre (SOC) and IT infrastructure teams	Intrusion detection systems and threat intelligence feeds
Recover	Respond to and recover from cyber-attacks	Reduce downtime and restore operations	Activate incident response, restore systems, and analyse	Low downtime and restore operations	Incident response teams and IT security operations	Backup systems, incident response management platforms, and forensic analysis tools
Adapt	Learn and improve from past cyber-attack incidents	Enhance practices and improve cyber resilience	Post-incident analysis, updated controls, and training	Increased knowledge and improved cyber resilience	Management, IT leadership, and compliance	Incident management systems, lessons learned repository, and training resources

ber resilience as socio-technical, and related works in cyber resilience management. A comprehensive search of published literature examined a specific data set. The review centred around various aspects of cyber resilience frameworks, such as their objectives, gaps in the existing literature, target users, development processes, and cyber threats. The authors summarise the summarising and provide recommendations for future improvements to enhance cyber resilience.

2. The Concept of Cyber Resilience

This section offers a comprehensive discussion of the various cyber resilience concepts. It presents a well-organised framework that helps understand and improve cyber resilience in IT infrastructure. The section is structured in detail, covering different aspects of cyber resilience, such as phases, capacities, and factors. We describe and analyse each individually and showcase their comparison, as demonstrated in Table 3.

2.1. Phases of Cyber Resilience

This section will present the phases of cyber resilience, which assesses how to achieve cyber resilience. Thus, phases are called a functionality-based approach in [29], which is mainly related to National Academy of Sciences (NAS) that defines four phases of cyber resilience as an event management cycle that will help to maintain and achieve cyber resilience [30]. The four cyber resilience phases are plan / prepare, absorb, recover, and adapt. We can compare and represent the difference between those cyber resilience phases as shown in Table 2.

Plan / prepare: During the preparation phase, individuals' cyber functioning, supported by cyber resources, is at the average baseline level. This is the phase before the onset of adverse cyber incidents [31]. The prepare phase represents the baseline level of individuals' system functioning, during which preparations for responses in the subsequent steps are made. It is essential to have comprehensive security policies that provide cyber resilience training and on-the-job support to ensure everyone knows their role [32].

Making the foundation of services and assets ready and available during any disruptive event, such as failures or attacks, is the first stage of cyber resilience. Generally, cyber-attack prevention is better than badly affecting the networks and systems. Preventing cyber-attacks and data breaches requires a multi-layered approach to cyber resilience that includes technologies, people, and processes [33].

Cyber resilience begins with the planning phase, where organisations proactively prepare for potential cyber threats and incidents. This involves conducting risk assessments, developing incident response plans

Table 3: **Comparison between phases, capacities, and factors of cyber resilience.**

Aspect	Phases of Cyber Resilience	Capacities of Cyber Resilience	Factors of Cyber Resilience
Definition	Chronological progression of activities in response to cyber-attacks or incidents.	Foundational attributes enabling organisations to navigate through resilience phases.	Specific elements or resources contributing to resilience enhancement.
Focus	Structured approach guiding organisations through preparation, response, and recovery phases.	Essential pillars supporting cyber resilience strategies and organisational capabilities.	Contributing mechanisms bolstering overall cyber resilience.
Purpose	Guide organisations in anticipating, withstanding, recovering from, and adapting to cyber-attacks.	Recognise essential attributes organisations must possess to enhance cyber resilience.	Pinpoint actionable strategies and resources for improving resilience posture.
Examples	Plan/prepare, absorb, recover, and adapt.	Absorptive, pre-recovery, and restorative capacities.	Managing complexity, network topology, resource allocation, pre-configuration, buffering support, and human factors .
Objective	Ensure organisations are equipped to respond effectively to cyber-attacks in a structured manner.	Strengthen organisations' overall cyber resilience by providing necessary capabilities.	Provide actionable strategies to mitigate the impact of cyber-attacks effectively.
Temporal Relationship	Sequential and occur in a specific order, reflecting progression of activities.	Ongoing attributes continuously developed and reinforced by organisations.	Ongoing considerations addressed continuously to adapt to evolving cyber-attacks.

and policies, and establishing security controls and procedures. The objective is to enhance preparedness and define clear response plans. Key activities include risk assessment, incident response planning, and allocating necessary resources [34]. Risk assessment tools, incident response plan templates, and vulnerability management tools are utilised during this phase to improve cyber resilience.

Absorb: The authors in [31] define the absorb phase as triggered by an adverse cyber event, which diminishes and degrades individuals' overall core cyber resilience functioning. The absorption phase ensures uninterrupted functionality and availability of critical assets by isolating or repelling disruptions. Layered security approaches should be used when designing network systems, which incorporate technical, procedural, and human elements to absorb attacks [33].

The impact of an adverse incident depends on the effectiveness of the measures taken to absorb it. The absorb phase includes actions taken when an adverse cyber event eventuates to isolate the disruptions caused by the event and ensure that pressure is kept at the correct level to minimise initial negative impacts while maintaining the stability of most critical individuals' cyber functioning [31].

In the absorbing phase, the focus is on detecting and containing cyber-attacks in real-time. Organisations implement security controls and monitoring systems, perform continuous monitoring and analysis of network traffic, and leverage threat intelligence. The objective is to achieve timely detection and containment of cyber-attacks. The primary stakeholders are the Security Operations Centre (SOC) and IT infrastructure teams [35]. Essential tools and technologies include Intrusion Detection Systems (IDS) to combine monitoring and analysis across subsystems [36], Security Information and Event Management (SIEM) systems [37], and threat intelligence feeds.

The absorb phase aligns closely with the concept of survivability. El Korchi [38] defined survivability as the ability of systems to stay alive in a temporary, non-viable equilibrium during a significant disruption. The core of survivability is the ability to remain alive and continue to exist during disruptions. During this phase, the system absorbs the initial impact of a disruptive event and focuses on maintaining core functionalities. This corresponds to the phase of resilience where the system strives to continue essential operations despite the immediate shock. It involves implementing measures to absorb the initial impact and prevent total failure, similar to survivability.

Recover: The recovery process involves restoring all services and assets to their normal functioning state. In other words, the foremost important goal of the cyber resilience strategy is to recover and roll back to a normal situation after an attack [32]. For instance, if a successful ransomware attack encrypts or locks down all the organisation's data, this will ultimately stop the business from operating [33]. Therefore, adequate data backup and recovery is necessary to avoid similar situations and a phase of cyber resilience to prevent similar problems [39].

In [31], the recovery phase starts when the adverse incident stops or is halted, and restoration of lost cy-

ber functioning begins. Timely and effective recovery actions are necessary to reduce the compounded negative impacts of disrupted cyber functioning. On the other hand, the recovery phase can measure performing account recovery, data recovery, system recovery, fact-checking, and accessing external support to assess adverse cyber events and their impacts to make informed decisions about recovery actions and to restore the original state as quickly as possible.

During the recovery phase, organisations respond to and recover from cyber incidents. Incident response teams are activated and communication channels are established. The primary goal is minimising downtime, containing and eradicating the cyber-attack incident, and restoring affected systems and data. Essential tools and technologies include incident response management platforms and forensic analysis tools [34]. The outcomes of this phase include lower downtime and restore operations. Stakeholders such as incident response teams and IT operations are involved in executing activities [35].

Adapt: The adapt phase starts once the system returns to normal functioning after the cyber-attack. The adapt phase can use the learnings and experience from the adverse event to inform the evolution and increase in cyber resilience functioning and to bounce forward better positive adaptation [31]. In the adapt phase, individuals learn about their resilience opportunities and limits from previous experience dealing with adverse cyber events.

Enhance cyber resilience using knowledge from abnormal events, system configuration, altered protocol, and personnel training. Adaptability is a crucial phase of cyber resilience that makes networks and systems automatically adapt to any cyber-attacks [32]. Accordingly, it will be necessary to consider the systems and networks used, the security postures assumed, and the trial and adaption of new types of cybersecurity technology, such as artificial intelligence in cybersecurity [33].

The adapt phase focuses on learning from past incidents and continuously improving cyber resilience capabilities. Organisations conduct post-incident analysis and lessons known sessions, update security controls and procedures, and implement improvements [40]. The objective is to enhance cyber resilience capabilities and increase knowledge and understanding of cyber-attacks. Stakeholders such as management, IT leadership, and compliance teams play a vital role in this phase. Essential resources needed include incident management systems [34], security awareness and training programs, and a repository for lessons learned.

The adapt phase can be seen as encompassing elements of both sustainability and adaptation. After the immediate recovery efforts, the focus shifts to adapting and strengthening the system to improve resilience over the long term. This involves learning from the event, integrating lessons learned, and implementing changes to enhance resilience. It aligns with the sustainability phase of the resilience curve, where the system stabilizes and implements longer-term strategies to sustain functionality and adaptability.

2.2. Capacities of Cyber Resilience

In this section, we introduce the capacities of cyber resilience, which evaluates the achievement of cyber resilience. Cyber resilience capacities are enhancement features that could increase the ability of network systems to absorb, adapt, and recover from cyber-attacks. Capacity is the property of the IT infrastructure network and system to achieve its goals. Cyber resilience improves a network system's capability to absorb, adapt, and recover from any cyber-attacks or disruption [15].

Cyber resilience capacity can take the form of resources such as the facilities of assets, including intelligence systems, activities, and actions. Many resilience capacities are presented, including rapid response, sustained resistance, continuous running, rapid convergence, and dynamic evolution. Jiang *et al.* [12] used a two-time slice approach with DBN to measure network resilience based on core capacities.

Absorptive capacity: It is defined as how a system can withstand and absorb attacks from cyber-attacks and minimise attacks' corresponding impacts. It must be established before a cyber-attack event happens and can usually be thought of as the first course of defence [41].

Absorptive capacity is the capability of the network system to absorb or withstand the impact of disruptive events and minimise the consequences, thereby approaching the robustness of the network system's cyber resilience. Absorptive capacity refers to all activities that must be taken to absorb from cyber-attacks in advance [42].

This capacity is defined by Vugrin *et al.* [43] as the "degree to which a system can automatically absorb the impacts of system perturbations and minimise consequences with little effort" and discussed in [44]. Absorptive capacity can be considered as the first line of defence or the primary as it highlights the ability of a network system to absorb cyber-attacks.

Pre-recovery capacity: The second capacity of cyber resilience is pre-recovery capacity, which indicates a network system's capability to adjust to disruption using non-standard operating practices to avoid any dis-

Table 4: **Explanation of cyber resilience factors.**

	Cyber Resilience Factors				
	Manage Complexity	**Network Topology**	**Add Resources**	**Pre-configuration**	**Buffering Supported**
Description	Complexity of links between systems' elements	Choice of appropriate network topology	Addition of redundant resources	Designing reversible and adaptable infrastructure	Provision of buffering and caching functions
Effect on Cyber Resilience	Improves or reduces cyber resilience	Enhances cyber resilience	Enhances cyber resilience	Enhances cyber resilience	Enhances cyber resilience
Impact	Can make cyber-attack control difficult	Influences network and system resilience	Enables system absorption and fast recovery	Enables faster restoration after an attack	Enhances data availability and access
Connection to Phases	Plan / prepare, absorb, recover, and adapt	Plan / prepare	Plan / prepare	Plan / prepare	Recover
Examples	Increase in interconnected systems	Selection of star or mesh topology	Duplication of servers or data storage	Configuration management systems	Caching mechanisms and data backups
Benefits	Increased system robustness	Resistance against certain attacks	Improved system availability	Faster recovery and adaptation	Improved data access and availability

continuity in the network system's performance. Pre-recovery capacities are usually temporary non-standard solutions that impose high costs [41].

Pre-recovery capacity is the capability of an IT infrastructure network and system to adjust itself and attempt to overcome a disruption without any recovery activity. It refers to a system's ability to be reorganised and perform efficiently with some extra effort and cost in response to a disruption. Design for pre-recovery capacity can enhance the cyber resilience of infrastructure network systems [42].

Vugrin *et al.* [43] defined pre-recovery capacity as "the degree to which the system is capable of self-organisation for recovery of system performance levels". It is a set of properties that reflects actions that result from ingenuity or extra effort over time in response to a crisis. In contrast to pre-recovery capacity, pre-recovery capacity refers to the capability of a network system to adjust internally during the recovery period after a cyber-attack or a post-disaster network system capacity [44].

Restorative capacity: The last course of defence is restorative capacity, which implies the capability of a system to repair or restore the disrupted component of the system. In contrast to adaptive capacity, restorative capacity is a permanent solution that returns the system to a steady state. For example, restorative capacity can include the manufacturer's capacity to fix or return network system links affected by cyber-attacks like Distributed Denial of Service (DDoS) attacks, malicious attacks, etc. Restorative capacity is highly dependent on the restoration and availability of technical resources [41].

Restorative capacity refers to the ability of a network system to repair or restore damages from a cyber-attack or disruption. Restorative capacity is different from pre-recovery capacity in the reason that it is considered to be an enduring feature of network system resilience. In contrast, pre-recovery capacity is a temporary feature (i.e., repairing links and nodes constantly in place versus ensuring continuity through a non-standard manner that increases service cost or time). Restoring network system facilities during the recovery period may not necessarily restore performance to its pre-damaged state and may exceed prior performance capabilities [41].

2.3. Factors of Cyber Resilience

In this section, we propose and discuss the main factors of cyber resilience. Several factors affect an organisation's IT infrastructure to be resilient and improve cyber resilience. However, this work presents the five factors of cyber resilience. The factors include managing complexity, network topologies, adding resources, pre-configuration IT infrastructure, and buffering supported factors.

Managing complexity involves understanding the intricate links between systems' elements and balancing between making cyber-attacks challenging to control and improving cyber resilience. The network topology factor ensures that the proper selection network and framework is in place to enhance cyber resilience.

Table 5: **Summary of the relationship between phases and factors of cyber resilience in IT infrastructure.**

Plan/Prepare	Absorb	Recover	Adapt
● The greater complexity of connections between system elements will increase the function of redundancy. ◆ Provide buffering will increase the system's resilience using caching. ■ Choose the correct topology that will increase the strength of systems and be more available.	⬢ Adding resources to systems will provide redundancy, and the performance will improve.	★ Design reversibility of the system will be easy to reverse in the process of recovering the system. ⬢ Adding resources will make recovery resources after the attack faster. ◆ Enable buffering of the system will increase the cyber resilience to recover the system after an attack.	● The managing complexity will increase cyber resilience, especially with the adapt phase.
● Complex within the network will increase the network's performance. ◆ Provide buffering that will increase the cyber resilience of data access in resource availability. ■ Choose the correct topology to increase cyber resilience and reduce failures.	⬢ Adding network resources will reduce the likelihood of causing losses.	● A web complex of links will reconnect to restore functions after an attack. ⬢ Adding resources to the network will speed up the service restoration. ◆ Provide buffering will increase resilience to restore performance and connectivity after an attack.	■ Choosing a proper network topology, such as mesh topology, will positively affect the cyber resilience to cyber-attacks.

Proposed Factors: ● =Manage Complexity, ■ =Network Topology, ⬢ =Add Resources, ★ =Pre-configuration, and ◆ =Buffering Supported

Adding redundant resources strengthens the system's capacity to absorb and recover from attacks.

Pre-configuration infrastructure allows for swift restoration and adaptation while buffering supported factors ensures data availability and access during attacks. We compare and describe differences between those factors as illustrated in Table 4. Likewise, we can provide a detailed summary of the processes that are needed between phases and factors of cyber resilience as presented in Table 5. By incorporating these factors, organisations can enhance their overall cyber resilience and mitigate the impact of cyber threats.

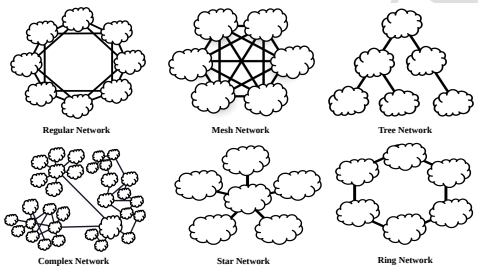


Figure 2: Types of network topology and connectivity between their sites.

Manage complexity factor: The complexity of links between the systems' elements will increase catastrophic failures of systems [45]. On the other hand, it will improve cyber resilience, making cyber-attack control difficult in a complex environment. The complexity of networks of paths connecting the network's elements will increase cyber resilience. However, sometimes, the complexity of the network will reduce cyber resilience.

Manage complexity factor relates to implementing strategies to mitigate the complexity of interconnected systems, which can enhance and challenge cyber resilience. Several strategies can be used to manage complexity, such as modularisation, standardisation, optimisation, and redundancy [46].

Modularisation involves breaking down complex systems into smaller, more manageable modules or components. Standardisation entails establishing standardised configurations and protocols to streamline operations and reduce variation. Optimising the connections and interdependencies of a system can minimise points of failure, resulting in improved efficiency.

Redundancy refers to introducing extra components or processes in critical systems. This improves the system's fault tolerance and resilience against potential failures. Backup measures allow the system to function even if one or more components fail.

Network topology factor: The choice of the proper topology will help the improvement of cyber resilience on the network and systems. Different research addresses the fundamental vulnerabilities in various networks as a function of their topological pro properties [47]. The plan and preparation phase of cyber resilience will be necessary, and choosing the suitable topology will increase network and system resilience. The selected network topology helps manage complexity and improves cyber resilience. Figure 2 shows the variety of network topologies and the connectivity between their sites or branches.

Network topology refers to the layout and interconnections of network components, whether physical or logical [48]. Various network topologies, such as star, mesh, tree and ring, offer varying performance levels and cyber resilience under different attacks. One must select the appropriate topology based on reliability, scalability, and fault tolerance requirements to optimise network topology [49]. Additionally, redundancy in network paths or components can improve fault tolerance and ensure continuous operation during failures. For instance, a mission-critical network may use a mesh topology to provide multiple paths for data transmission and reduce the impact of single-point failures.

Add resources factor: Different systems or network resources will improve cyber resilience and stabilise. That will reduce the number of failures in the hall systems. Also, in case of an attack or negligence of a specific resource, it will help the system absorb and recover the system fast [47]. The redundancy between the resources will increase the systems or networks for absorbing and speedy recovery under attack to move to the normal state. The added resources factor of cyber resilience configuration can be demonstrated in Figure 3.

Adding resources to enhance system capabilities and protect against cyber-attacks is essential [50]. One way to accomplish this is by adding extra resources or capacity as a backup. Several strategies for adding resources include duplicating hardware components such as servers and storage devices. This ensures continuous operation and data availability even during hardware failures. Another approach is implementing scalable infrastructure solutions, such as cloud computing or virtualisation.

This allows for dynamically allocating resources based on demand and mitigating the impact of resource constraints [47]. Load balancing is also a practical method involving distributing workloads across multiple resources to optimise performance, enhance fault tolerance, and prevent resource exhaustion. For example, implementing a redundant data storage solution with mirroring or replication can ensure data integrity and availability during disk failures or data corruption.

Pre-configuration factor: The IT infrastructure designed and capable of reversible under any attack will be more resilient than others. In other words, it will allow the systems and networks to absorb, recover, and adapt to cyber-attacks [47]. That will make the IT infrastructure recoverable, automated, and able to be restored faster than other systems. The pre-configuration factor of cyber resilience configuration can be illustrated in Figure 4.

Pre-configuration involves designing systems with

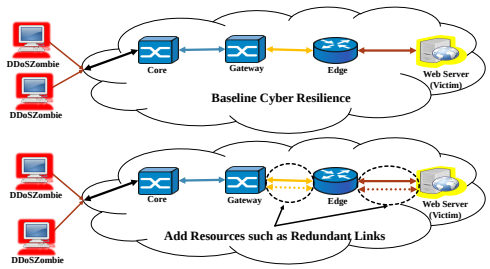


Figure 3: Add resources factor of cyber resilience quantification in IT Infrastructure.

built-in cyber resilience features and capabilities to facilitate rapid recovery and adaptation in the face of cyber-attacks or disruptions. Strategies for pre-configuration include automated failover, redundant configurations, designing systems with recovery, and establishing a cloud infrastructure. Implementing automated failover mechanisms to quickly switch to backup systems or resources in the event of failures [51].

Redundant configuring systems with redundant components or resources to ensure continuous operation and minimise downtime [52]. Designing systems with rapid recovery processes and procedures is crucial to minimise the impact of disruptions and restore normal operations promptly. Establishing a cloud infrastructure that includes automated scaling and load balancing is necessary. This ensures that resource allocation is dynamically adjusted based on demand, maintaining high performance and availability.

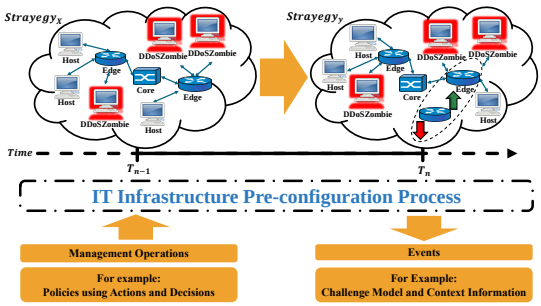


Figure 4: IT Infrastructure pre-configuration process.

Buffering supported factor: The networks or systems that provide the buffering and caching function will be more resilient, and the recovery will be easier and faster [47]. The buffering or chasing will make the data access and resources available, especially un-

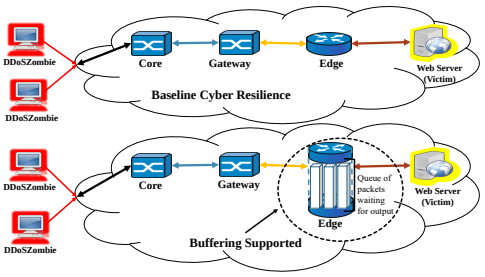


Figure 5: Buffering supported factor of cyber resilience quantification in IT Infrastructure.

der any cyber-attack situation. Much work discusses the buffering on the network to increase the cyber resilience of data availability and access when an attack happens. The buffering-supported resources factor of cyber resilience configuration can be exhibited in Figure 5.

Buffering-supported mechanisms provide buffering and caching functions, enhancing data availability and access during cyber-attacks, thus improving cyber resilience. Strategies for supporting buffering include the use of caching mechanisms. Caching mechanisms can reduce latency and improve responsiveness by storing frequently accessed data or resources closer to the end users [53].

Buffering resources also involves allocating additional buffer space or resources to temporarily store incoming data or requests, which can help smooth out workload fluctuations and prevent resource contention. Another option is to leverage Content Delivery Networks (CDNs) to cache and distribute content across geographically distributed servers, improving delivery speed and resilience to network congestion or outages [54]. For example, deploying a CDN to cache and serve static website content reduces the load on origin servers and improves website performance and availability during peak traffic or DDoS attacks.

Human factors: Previously, the emphasis was primarily on technology solutions with little focus on human factors. Now, cyber resilience improvement programmes take into account human behaviors, culture, and organisational factors [55]. In cyber resilience, acknowledging and understanding the role of human factors is paramount. Despite the advanced technological solutions available, the behaviour and intervention of humans are still crucial factors in an organisation's ability to withstand and recover from cyber threats. The human factors of cyber resilience can be summarised in Figure 6.

Giacomello and Pescaroli [56] discuss the importance of managing human factors in the context of cyber resilience. It emphasises the need to consider human behaviour, decision-making, and actions to defend computers and networks effectively. The authors highlight that organisations can adopt new strategies and technologies that align with their information and control infrastructure as research in this field progresses to defend against adversaries actively.

Employees play a vital role in helping organisations become more cyber-resilient. In theory, employees could perform monitoring, responding, anticipating, and learning functions to maintain cyber resilience capabilities [57]. Human factors include user behaviour, security awareness, training, organisational culture, and incident response protocols. These factors significantly influence an organisation's resilience to cyber threats and can either enhance or undermine the effectiveness of technical defences.

It is essential to acknowledge that cyber resilience is highly contextual and varies depending on factors such as industry sector, organisational size, budgetary constraints, regulatory requirements, and existing cybersecurity posture.

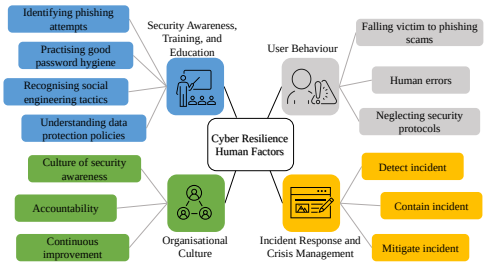


Figure 6: Human factors in cyber resilience.

3. Proposed Cyber Resilience Quantification Framework (CRQF)

In this section, we will propose a framework called CRQF, which combines the phases, factors, and capacities of cyber resilience. The phases, factors, and capacities of the framework proposed are presented and examined in Sections 2.1, 2.3, and 2.2 respectively. The framework aims to help quantify the capacity of cyber resilience for networks and systems. The overall picture of the proposed CRQF is shown in Figure 7.

The CRQF is a methodology for measuring the cyber resilience of IT infrastructure. It is based on the concept

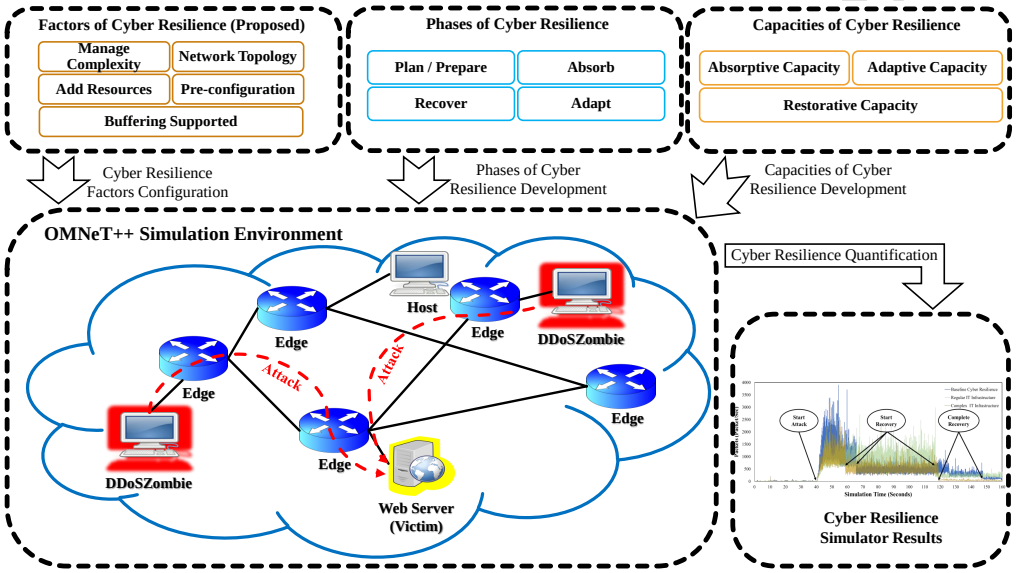


Figure 7: Overview of Cyber Resilience Quantification Framework (CRQF).

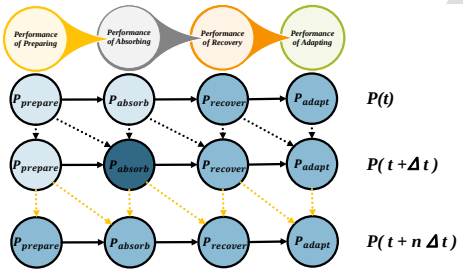


Figure 8: The DBN structure system performance of the network nodes.

of cyber resilience and the impact of cyber-attacks on a network or a system's ability to withstand and recover successfully and quickly. The framework is designed to be adaptable to various types of networks and systems, from small businesses to large corporations. The framework comprises three main elements: phases, factors, and capacities.

Phases: The framework consists of four phases: plan / prepare, absorb, recover, and adapt that discussed in Section 2.1. Each phase represents a stage in the system's response to a cyber-attack. The plan / prepare phase involves preparing for potential attacks, while the absorb phase involves mitigating the impact of an attack. The recovery phase focuses on restoring the system to its pre-attack state. The adaptation phase involves learning from the attack and improving the system's overall cyber resilience.

Factors: The framework includes five factors influencing cyber resilience: Managing complexity, network topology, adding resources, IT infrastructure pre-configuration, and buffering supported that is proposed and discussed in Section 2.3. These factors represent the key areas that needed to be addressed for cyber resilience in an IT infrastructure.

Capacities: The framework identifies three capacities of cyber resilience: absorptive capacity, adaptive capacity, and vital capacity is summarised in Section 2.2. These capacities represent the system's ability to absorb, adapt, and recover from cyber-attacks.

To quantify cyber resilience using this framework, you would first define measurable metrics for each factor and capacity. These metrics would then be mapped to the appropriate phase, factor, or capacity. Weights would also be assigned to each phase, factor, and capacity to reflect their relative importance in the overall framework.

The CRQF is a comprehensive approach in measuring cyber resilience considering modern systems' com-

plexity and diversity. By using this framework, organisations can better understand their cyber resilience and identify areas for improvement.

3.1. The BN and DBN with Cyber Resilience

The BN, called the Causal or Belief Networks, is a directed cyclic that illustrates the practice of describing the conditional probability relationship between data variables based on probabilistic inference theory [58]. The nodes represent in BN as random variables. The links between them represent conditional dependencies among the variables with their parent nodes, which are ruled and used by the conditional probability tables. The static BN cannot be used to model a time-varying performance system. Therefore, the DBN was based on the hidden Markov model to satisfy the temporal system performance [59]. The DBN is also known as a two-time slice BN because the two-time slices are included in DBN modelling: time slice t and $t + \Delta t$. The discrete-time slice Δt is usually set to be 1. By using the technique of dividing a time duration into a series of time slices, the DBN allows the node attribute variable $X^{t+\Delta t}$ at time slice $t + \Delta t$ to be conditional upon its nodes of parent $Xp_i^{t+\Delta t}$ at the same time slice, as well as i its parents Xp_i^t and its states X_i^t at the previous time slice t.

The DBN is adapted in modelling and quantifying system or network of cyber resilience as shown in Figure 8 that represents the details and the basic structure of DBN. First, each row of nodes simultaneously represents the four cyber resilience performances, where solid angles link the four attribute nodes. The solid angles represent the conditional transition probability between the parent node and the self-node. Then, each column of nodes represents the time-varying states of every cyber resilience performance. The dotted angles between the columns of nodes represent every cyber resilience performance's conditional probability of change. Finally, the diagonal dotted curves represent the conditional probability of change between the self-node at the current time slice and the parent node at the previous time slice.

3.2. Performances of Cyber Resilience

We can explain the performance of cyber resilience by showing the curve relationship between phases and factors as illustrated in Figure 9. The P_{L1} means the system or network typically works with good cyber resilience performance. During a period of cyber-attack, the system offers a more straightforward method of measuring the level of cyber resilience that has been established.

The relationship between cyber resilience and performance is shown in Figure 9. The P_{L2} signifies the minimum performance required by the system and network under any situation. Under P_{L2}, it means that poor performance of a system results in poor performance of its components, leading to degraded performance when attacked in a certain way.

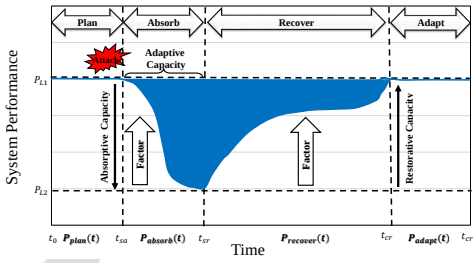


Figure 9: The framework proposes a curve performance for cyber resilience that shows its phases, factors, and capacities.

Understanding that we can accurately measure performance levels between average and baseline is essential. We need a sophisticated quantification model that includes complex systems or networks modelled as nodes in a DBN model to do this. To quantify cyber resilience, measuring $P(t)$ is critical using the phases of cyber resilience to present performances, as detailed in Section 2.1. Although there is a lack of literature that formally describes $P(t)$ or designates a simple system attribute as the quantitative standard of $P(t)$, this paper establishes a clear measurement indicator of $P(t)$. Four phases of cyber resilience determine this and can define time-independent system performances: (1) performance of preparing $P_{prepare}(t)$; (2) performance of absorbing $P_{absorb}(t)$; (3) performance of recovering $P_{recover}(t)$; and (4) performance of adapting $P_{adapt}(t)$, as summarised in Figure 9.

These four phases' performances are influenced directly by the five core cyber resilience factors described in Section 2.3. Meanwhile, a time-dimensional interaction exists between these four performances based on conditional probability. For example, networks A and B provide the same sustained absorbing at time Δt when suffering the same destruction at time t. Still, the performance preparing $P_{prepare}(t)$ on network B is higher than network A at time t. It can be expected that network A will better perform absorbing $P_{absorb}(t + \Delta t)$ than network B when affected by a cyber-attack.

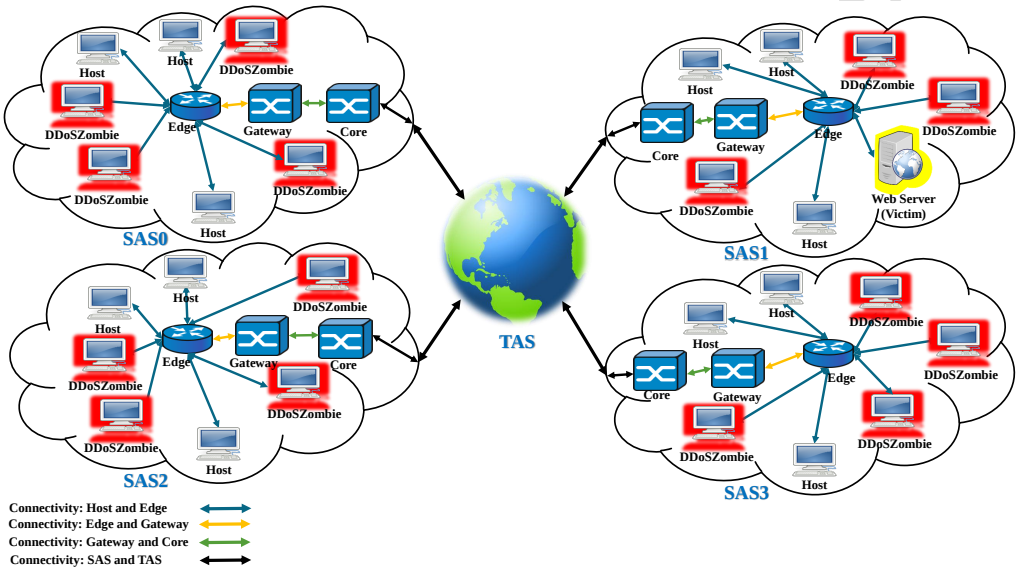


Figure 10: The architecture design of the simulation in the OMNeT++ platform.

3.3. Metrics for Quantifying Cyber Resilience

In order to comprehensively assess the effectiveness of various cyber resilience factors within an organisation's IT infrastructure, it is essential to establish quantification metrics that can provide insights into the system's ability to withstand and recover from cyber-attacks. These metrics offer a structured approach to evaluating the performance of different resilience factors and can guide organisations in prioritising their investments and efforts towards enhancing cyber resilience.

This section presents a set of basic metrics to evaluate the impact and effectiveness of critical cyber resilience factors. By quantifying various aspects of cyber resilience, these metrics enable organisations to understand their resilience posture better and identify improvement areas. This section outlines six essential metrics:

Start attack time (T_{sa}): The start attack time represents the duration between the initiation of a cyber-attack and its detection by the organisation's security systems. It indicates how quickly the organisation can identify and respond to incoming threats, allowing for a prompt initiation of defensive measures.

Start recovery time (T_{rs}): The start recovery time represents the duration between detecting a cyber-attack and initiating the recovery process. It indicates how quickly an organisation can respond to an attack and restore its systems to a functional state.

Complete recovery time (T_{rc}): The complete recovery time measures the duration required for the system to achieve complete restoration after a cyber-attack. It encompasses the entire recovery process, including all necessary actions to recover the system to its pre-attack state.

Absorb duration (D_{absorb}): The absorb duration quantifies the time it takes for the organisation to detect and mitigate the impact of a cyber-attack. It reflects the effectiveness of the organisation's defences and incident response capabilities in minimising the attack's immediate consequences.

Recovery duration ($D_{recovery}$): The recovery duration calculates the time interval between the initiation of the recovery process and the complete restoration of the system. It measures the efficiency of the organisation's recovery efforts in recovering from the attack and returning to normal operations.

Adapt duration (D_{adapt}): The adapt duration evaluates how quickly the organisation can adapt and implement improvements in response to a cyber-attack. It reflects the organisation's agility and ability to learn from past incidents to enhance its resilience against future

threats.

Each of these metrics provides valuable insights into cyber resilience, allowing organisations to identify strengths and weaknesses in their resilience strategies. By tracking and analysing these metrics over time, organisations can continuously improve their cyber resilience posture and better protect their IT infrastructure against evolving threats.

While our primary quantification metric is initially developed for IT infrastructure networks, with appropriate modifications and adaptations, it can be applied to evaluate the cyber resilience of other applications, such as IT networks within cyber-physical systems such as smart grids or microgrids. Collaboration with domain experts, simulation studies, and customisation for CPS contexts are essential to ensure the metric's applicability and effectiveness in these environments.

3.4. Process Steps of CRQF Framework

The Cyber Resilience Quantification Framework (CRQF) presented herein offers a structured methodology for assessing, prioritising, and improving cyber resilience within organisations. Grounded in the understanding that cyber resilience is multifaceted and context-dependent, the framework integrates three fundamental dimensions: the phases of cyber resilience, the capabilities of cyber resilience, and the factors influencing cyber resilience. By incorporating these dimensions into a comprehensive framework, organisations can systematically evaluate their cyber resilience posture, identify areas for improvement, and prioritise strategic initiatives to enhance resilience capabilities.

The framework depicted in Figure 11 consists of various elements that help organisations enhance their cyber resilience capabilities. These elements are chosen based on the organisation's specific needs and are evaluated for their effectiveness in enhancing cyber resilience. The framework follows a phased approach that aligns with the different phases of cyber resilience. The simulation and evolution step is used to measure the effectiveness of cyber resilience. Finally, continuous improvement mechanisms are established to help organisations improve their cyber resilience capabilities.

The CRQF consists of six interconnected process steps, each tailored to address specific aspects of cyber resilience while leveraging insights from the phases, capabilities, and factors of cyber resilience. These steps guide organisations through a structured approach to cyber resilience enhancement, encompassing customisation, risk assessment, resource allocation, phased implementation, simulation and testing, and continuous improvement.

1. Customisation: This initial step involves assessing the organisation's operational environment, business objectives, and risk appetite to tailor the framework to its unique circumstances. By identifying relevant cyber resilience factors aligned with organisational goals and capabilities, organisations can lay the groundwork for effective resilience strategies.

2. Risk assessment: Organisations conduct a comprehensive risk assessment to identify critical assets, vulnerabilities, and potential threats. This process is then used to customise their approach to security. By considering cyber resilience's phases, capabilities, and factors, organisations can prioritise resilience measures that mitigate identified risks and protect essential assets.

3. Resource allocation: With a clear understanding of organisational risks and priorities, resource allocation becomes essential. Organisations must evaluate constraints and allocate resources based on each cyber resilience factor's potential impact and effectiveness. This step ensures optimal resource utilisation and maximises resilience outcomes within available constraints.

4. Phased approach: Recognising that cyber resilience is an ongoing journey; organisations adopt a phased approach to implementation. By prioritising high-impact, low-cost initiatives and gradually expanding resilience capabilities over time, organisations build momentum and demonstrate tangible progress in enhancing their resilience posture.

5. Simulation and testing: Organisations conduct simulations and testing exercises to validate and quantify the effectiveness of cyber resilience measures and preparedness for cyber incidents. Realistic scenarios are employed to assess the organisation's response capabilities across different phases of cyber resilience, enabling organisations to identify weaknesses and refine their strategies accordingly.

6. Continuous improvement: Finally, organisations establish mechanisms for ongoing monitoring, assessment, and adaptation of cyber resilience strategies. Organisations can continuously improve their cyber resilience by reviewing and updating the framework based on emerging threats, lessons learned, and changes in the operational environment.

Through the systematic application of the CRQF, organisations can enhance their cyber resilience capabilities, mitigate risks, and maintain operational continuity in the face of evolving cyber threats. By integrating cyber resilience's phases, capabilities, and factors into a unified framework, organisations can navigate the complexities of the cybersecurity landscape with confidence and resilience.

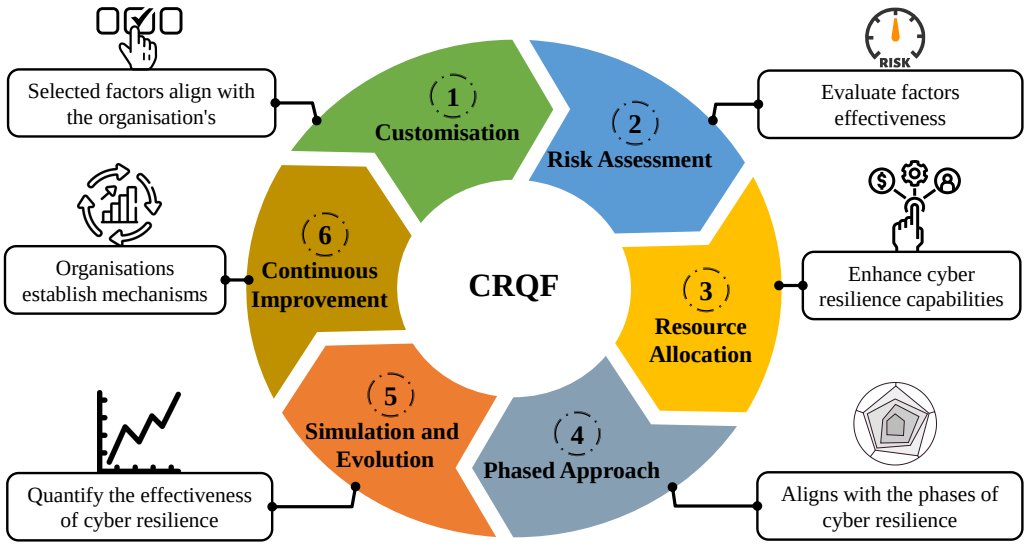


Figure 11: The CRQF framework consists of several process steps that need to be followed in order to quantify and enhance cyber resilience.

4. Simulation Environment and Results

In this section, we introduce the simulation for quantifying cyber resilience. This section explains the setup of the simulation and the modules used in it. The simulation runs in Oracle VirtualBox, an open-source virtual machine. Ubuntu's operating system was installed in the virtual machine to run the simulation. The simulator tool used in this simulation is Objective Modular Network Testbed in C++ (OMNeT++). This simulator requires modules such as INET, ReaSE, SEA++, and NETwork Attacks (NETA). Furthermore, a Linux-based operating system is preferable because it supports Command-Line Interface (CLI) and Graphical User Interface (GUI). The main reason for this simulation is to show how cyber resilience's phases, factors, and capacities affect quantifying cyber resilience, especially the performance of network systems. Figure 10 demonstrates the simulation design.

Our study represents a novel application of existing tools within the context of cyber resilience assessment. While individual tools such as OMNeT++, INET, ReaSE, SEA++, and NETA have been used independently in previous research, our study uniquely combines these tools to create a comprehensive simulation environment tailored to evaluate cyber resilience factors and their impact on system performance.

The novelty of our approach lies in integrating and orchestrating these tools to simulate realistic cyber-attack scenarios, assess the effectiveness of various cyber resilience factors, and quantify the resilience of IT infrastructures under different conditions. By leveraging the capabilities of each tool and integrating them into a cohesive simulation framework, we generated valuable insights into the dynamics of cyber resilience. We provided actionable recommendations for enhancing resilience in complex systems.

Therefore, while the individual tools themselves may not be new, our study's contribution lies in the novel application and combination of these tools to address cyber resilience challenges, ultimately advancing the state-of-the-art in cyber resilience research. We believe this will help elucidate our study's unique contribution in leveraging existing tools within the simulation environment better.

Our work utilised a simulation-based methodology to evaluate the elements contributing to cyber resilience in IT infrastructure networks. Our simulation process was designed with the utmost care, ensuring it was thorough and precise. To ensure the dependability and strength of our discoveries, we carried out sensitivity analyses incorporating multiple parameters and scenarios.

The simulation model was developed based on estab-

lished principles in cyber resilience research, leveraging validated algorithms and inputs derived from both theoretical frameworks and empirical data sources. Multiple scenarios were considered, encompassing different cyber-attacks, network topologies, system configurations, and organisational contexts to capture a broad spectrum of real-world conditions.

Furthermore, we conducted extensive validation and sensitivity analyses to assess the accuracy and stability of the simulation results. This involved comparing the simulated outcomes with available empirical data and testing the model's response to variations in input parameters and assumptions. Sensitivity analyses were performed to identify critical factors influencing the cyber resilience outcomes and evaluate the model's robustness under different conditions.

4.1. Data and Methods

This section provides sample data and methods and an overview of our study's simulation methodology, including details on the experimental design, simulation execution, data collection, and validation procedures. We can make adjustments according to our research's specific details and requirements. We have used a toolset for the offline evaluation of cyber resilience strategies called Policy-driven Resilience Strategy Evaluation Toolset (PReSET) [60]. It integrates the OMNeT++ [61] and the Ponder2 policy framework [62].

It has implemented several policy-controlled instrumented mechanisms as OMNeT++ modules, which run within the simulation and offer cyber resilience functionality, including link monitoring, anomaly detection, and rate-limiting mechanisms. Policies can control their behaviour by setting flags, stopping monitoring sessions, triggering or dropping connections, and finding optimal configurations.

The toolset is extensible and allows the modelling of cyber resilience strategies, facilitates the offline analysis of anomalies and attack behaviours, and permits the evaluation of cyber resilience policies to detect and mitigate cyber-attacks. PReSET can synthesise data describing real network traffic and attack behaviour. Cyber resilience strategies that perform well in PReSET are converting to management patterns, ready for deployment.

INET framework [63] is an open-source model library working under the OMNeT++ simulation environment. It provides students and researchers with many protocols, agents and other communication network models. ReaSE [64] is a tool module for creating a realistic environment. It considers traffic patterns, topology generation, and attack traffic. SEA++ [65] is a framework module that extends from OMNeT++ and INET to evaluate cyber-attacks impact on networks, systems and applications in a user-friendly way. NETA [66] is a framework module built on OMNeT++ simulator and INET framework. NETA intended to become a practical framework module for students and researchers focused on the network security field to apply cyber-attacks.

Simulation methodology: The study used the PReSET software tool to evaluate the impact of various factors on cyber resilience through simulation methodology. PReSET is a comprehensive simulation platform designed explicitly for assessing cyber resilience in complex systems. It allows for creating dynamic cyber environments, manipulating system parameters, and analysing resilience under various scenarios.

Experimental design: The simulation study was conducted in a controlled environment, where different scenarios were simulated to assess the resilience of cyber systems under varying conditions. The experimental design consisted of four steps: scenario development, input parameters, simulation execution, and data collection.

1. Scenario development: Multiple simulation scenarios were developed based on the factors identified in the cyber resilience framework proposed in this study. These cyber resilience factors included system complexity, network topology, added resources, preconfiguration, and buffering-supported factors. Once the configuration of each factor with the specific edge or network is complete, the next stage involves simulating to generate the system performance results for each factor separately.

Simulation scenarios are designed to evaluate the performance of attack detection mechanisms with different traffic types. The nodes of the simulated topology are configured to generate honest, attack, and flash traffic at a specific duration. The scenario simulated was a DDoS attack based on the set of programs Tribe Flood Network [64]. All our simulations generate some traffic networks and create attacks. The victim is a web server named "Web Server", which ranks SAS1 as the victim. We simulate and execute in the absence and presence of an attack detection mechanism.

2. Input parameters: Input parameters for each simulation scenario were defined, including the characteristics of the cyber system, the configuration of network elements, and the behaviour of human actors within the system. These parameters were varied systematically to

evaluate their impact on cyber resilience.

3. Simulation execution: The scenarios were executed using the PReSET toolkit, with each scenario run multiple times to account for variability and randomness in system behaviour. The simulation environment was monitored throughout the execution to collect data on system performance, resilience metrics, and other relevant variables.

4. Data collection: Data generated during the simulation runs were collected and analysed to assess the resilience of the cyber systems under different conditions. Several key performance indicators were measured to assess the system's efficiency in countering cyber threats and disruptions. These metrics included system uptime, response time, and recovery capability. The system's effectiveness in mitigating potential cyber risks was gauged by evaluating these parameters.

4.2. Validation and Sensitivity Analysis

We conducted thorough validation and sensitivity analysis to ensure the accuracy and dependability of our simulation results. Validation is a process that involves comparing the output of a simulation model with real-world data or theoretical models. This helps to determine how accurate the simulation is. Furthermore, we conduct a sensitivity analysis to evaluate the effectiveness and reliability of the simulation results, especially when input parameters and assumptions are altered or modified.

This analysis helps us understand how sensitive the results are to changes in the used variables. This evaluation helps assess the accuracy and precision of the simulation model and make informed decisions based on the outcomes. It is important to acknowledge certain limitations of the simulation study. While PReSET provides a powerful platform for assessing cyber resilience, the accuracy of the simulation results may be influenced by factors such as simplifications in the model, assumptions made during scenario development, and the representativeness of the simulated cyber environment.

In the simulation process, the last stage is generating data analysis output for each factor of cyber resilience. This output helps to quantify the level of cyber resilience. It is essential to understand the effectiveness of each factor and make informed decisions on the best approach to enhance cyber resilience. The results of this stage provide valuable insights to decision-makers in different industries, such as finance, manufacturing, and healthcare.

We conducted one simulation run for each factor; our experimental design involved developing multiple scenarios within each factor to explore different variations and configurations. Each scenario represented specific conditions or parameters relevant to the evaluated factor. These scenarios were carefully designed to cover a broad spectrum of potential cyber resilience scenarios, allowing us to assess the factor's robustness across various contexts.

While conducting only one simulation run per factor is limited, it is essential to emphasise that our study focused on understanding the relative impact of each factor and its variations on cyber resilience. By systematically varying the parameters within each factor and evaluating their effects on system performance, we gained valuable insights into the factors that most significantly influence cyber resilience.

Additionally, while we conducted a comprehensive analysis within the scope of our study, we acknowledge that there may be opportunities for further exploration and refinement in future research. Our study provides a solid foundation for understanding the fundamental relationships between cyber resilience factors and system performance, paving the way for more extensive investigations and iterations in subsequent studies.

In summary, while we conducted one simulation run for each factor, our experimental design allowed us to explore multiple variations and configurations within each factor, comprehensively assessing their impact on cyber resilience. Our approach effectively balances the need for rigour and efficiency in simulation-based research while laying the groundwork for future exploration and refinement.

The summary of the simulation results of cyber resilience in terms of time ($Seconds$) presented in Table 6 and in terms of percentage (%) shown in Table 7. The data shown in Tables 6 and 7 includes multiple measurements that are used to evaluate cyber resilience factors. A detailed explanation of these metrics is in Section 3.2. These metrics are obtained from simulations or analytical models designed to test the effectiveness of different cyber resilience factor configurations.

In Table 6, the time taken for each cyber resilience factor to respond to a cyber-attack is measured and presented in seconds. This information can be used to determine which factors are more effective in responding to cyber-attacks and which ones need improvement. In Table 7, the results of the analysis are presented in terms of percentage, allowing for a comparison of the effectiveness of each cyber resilience factor. The percentage values indicate the proportion of successful responses to cyber-attacks for each factor. This information can be used to identify the most effective cyber resilience factors and prioritise their implementation in IT infrastructure.

Table 6: **The performance analysis of cyber resilience factors in terms of time (seconds).**

Factors of Cyber Resilience		Start Attack (Sec)	Start Recovery (Sec)	Complete Recovery (Sec)	Plan / Prepare Duration (Sec)	Absorb Duration (Sec)	Recovery Duration (Sec)	Adapt Duration (Sec)
Managing Complexity		40	65.5	125.5	40	25.5	60	34.5
Add Resources		40	58	119	40	18	61	41
Network Topology	**Mesh**	40	45.5	114.5	40	5.5	69	45.5
	Tree	40	45.5	55	40	5.5	9.5	105
	Star	40	45.5	55	40	5.5	9.5	105
	Ring	40	45.5	55	40	5.5	9.5	105
Pre-configuration		40	55.5	148	40	15.5	92.5	12
Buffering Supported		40	55.5	115	40	15.5	59.5	45

Table 7: **A comparative analysis of cyber resilience factors in terms of percentage (%).**

Factors of Cyber Resilience		Plan / Prepare Duration (Sec)	Plan / Prepare (%)	Absorb Duration (Sec)	Absorb (%)	Recovery Duration (Sec)	Recovery (%)	Adapt Duration (Sec)	Adapt (%)	Overall (%)
Managing Complixity		40	100	25.5	21.57	60	15.83	34.5	34.78	43.05
Add Resources		40	100	18	30.56	61	15.57	41	29.27	43.85
Network Topology	**Mesh**	40	100	5.5	100	69	13.77	45.5	26.37	60.04
	Tree	40	100	5.5	100	9.5	100	105	11.43	77.86
	Star	40	100	5.5	100	9.5	100	105	11.43	77.86
	Ring	40	100	5.5	100	9.5	100	105	11.43	77.86
Pre-configuration		40	100	15.5	35.48	92.5	10.27	12	100	61.44
Buffering Supported		40	100	15.5	35.48	59.5	15.97	45	26.67	44.53

In the comparative analysis of cyber resilience factors, the pre-configuration factor stands out with the highest overall cyber resilience score of 61.44%. This factor excels in planning and adaptation, achieving perfect scores of 100%, but it faces significant challenges in absorption (35.48%) and recovery (10.27%). Conversely, the buffering supported factor, with an overall score of 44.53%, demonstrates strengths in planning (100%) and adaptation (44.53%) but requires substantial improvement in absorption (35.48%) and recovery (15.97%) capabilities. Managing complexity and adding resources factors share similar overall scores at approximately 43%, highlighting the need for comprehensive enhancements across phases. Network topology factors, including mesh (60.04%), tree (77.86%), star (77.86%), and ring (77.86%), excel in planning and absorption but struggle with recovery and adaptation, with scores ranging from 11.43% to 26.37%.

The similarity in observed values across different network topologies, such as tree, star, and ring, could be due to several factors, including simulation parameters, model complexity, the effectiveness of defence mechanisms, and random variability. The simulation parameters, such as attack intensity, duration, and defence mechanisms, could influence the results. Similar cyber resilience outcomes may result if these parameters are constant across different network topologies.

The complexity of the simulation model and its ability to accurately capture the nuances of each network topology could also impact the results. If the model can differentiate between the resilience capabilities of different topologies, it may yield similar performance metrics. The effectiveness of defence mechanisms implemented in each network topology could play a significant role.

If the defence mechanisms are equally effective across different topologies, similar resilience outcomes may result despite structural differences. Finally, random variability inherent in simulations could also contribute to the observed similarities. Fluctuations in the simulation outcomes due to stochastic elements may mask the expected differences between topologies.

4.3. Manage Complexity Factor of Cyber Resilience

Figure 12 describes the testing results that display significant differences between baseline cyber resilience and managing complex IT infrastructure performance. The graph outcome IT infrastructure's better cyber resilience and faster-starting recovery at 65.5 seconds. The complex IT infrastructure factor of cyber resilience performed better to complete the comeback in around

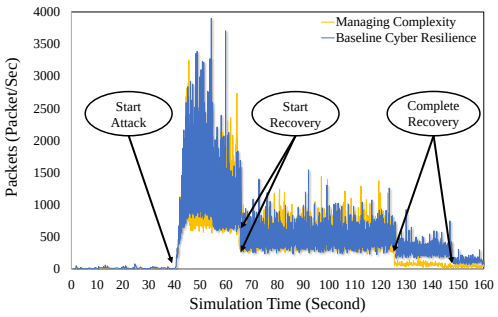


Figure 12: The manage complexity factor will affect the cyber resilience quantification compared with baseline cyber resilience.

125.5 seconds, faster than baseline cyber resilience and regular IT infrastructure.

The start recovery duration of 65.5 seconds suggests that the organisation has mechanisms to detect cyber-attacks and initiates the recovery process quickly. This indicates a proactive approach to monitoring and incident response, enabling the organisation to mitigate the attack's impact promptly. The relatively short complete recovery duration of 125.5 seconds implies that the organisation has efficient recovery processes, resources, and expertise. The organisation can effectively restore the system to its acceptable level, minimising any disruption to business operations.

The absorb duration of 25.5 seconds indicates that the organisation has strategies to mitigate the immediate effects of a cyber-attack promptly. This suggests the presence of practical measures such as intrusion detection systems, firewalls, or threat intelligence tools to block or filter malicious traffic. The relatively short recovery duration of 60 seconds implies that the organisation has efficient recovery processes, resources, and automation tools to expedite the restoration of the system. This helps to minimise downtime and reduce potential financial and reputational losses.

Furthermore, the results indicate that managing complexity is crucial to cyber resilience. The duration obtained from the simulation provides insights into the time it takes from a DDoS attack to recover and the overall duration of the different phases. This information can help organisations understand the relationship between system complexity and cyber resilience.

Overall, the managing complexity factor results indicate that the organisation has taken steps to effectively manage the complexities of its IT infrastructure when responding to cyber-attacks. The prompt start of the recovery process, efficient complete recovery, and quick absorption of the attack's impact highlight the organisation's preparedness and effectiveness in dealing with complex cyber threats. The relatively short recovery duration suggests a proactive approach in restoring operations and enhancing cyber resilience.

The managing complexity factor achieves an overall cyber resilience score slightly below that of the buffering supported factor, at 43.05%. It excels in planning / preparing (100%) but encounters substantial challenges in the absorption phase (21.57%). This lower percentage in absorption underscores the difficulties it faces in effectively managing complex cyber-attacks. Additionally, its recovery (15.83%) and adaptation (34.78%) scores suggest significant room for improvement, emphasising the necessity of adapting a comprehensive approach to cyber resilience. It is important to address weaknesses in absorption, recovery, and adaptation despite a strong foundation in preparation.

4.4. Add Resource Factor of Cyber Resilience

Figure 13 illustrates the simulation results that indicate some significant distinction between the baseline cyber resilience performance and the configuration of the add resource factor of cyber resilience, such as the dependency of the links. The result demonstrated that the start recovery at 58 seconds is the same for the baseline cyber resilience method and adding resources. However, the added resource factor of cyber resilience performed better for completing recovery at 119 seconds which is faster than baseline cyber resilience.

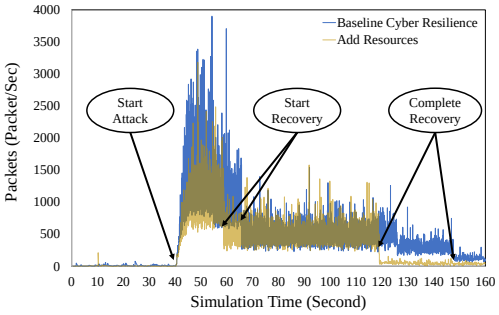


Figure 13: The added resources factor will affect the cyber resilience quantification compared with baseline cyber resilience.

The recovery phase starts at 58 seconds for the additional resources factor, and complete recovery is achieved at 119 seconds. The absorb phase lasts 18 seconds, the recovery phase lasts 61 seconds, and the adaptation phase takes 41 seconds. These durations reflect the impact of adding additional resources on the system's ability to recover and restore standard functionality.

The add resources factor shares a similar overall score with the managing complexity factor, indicating a comparable level of cyber resilience. It is excellent at planning and preparing (100%), but its absorption rate is only 30.56% and its recovery rate is only 15.57%. These percentages highlight the imperative of maintaining its response and recovery capabilities to enhance overall cyber resilience effectively. It is essential to prioritise addressing vulnerabilities during response and recovery to establish a stronger cyber resilience strategy, regardless of the initial level of preparedness.

The results related to adding resources highlight the importance of allocating sufficient resources to enhance cyber resilience. The duration obtained from the simulation provides insights into the time required to recover from a DDoS attack when additional resources are allocated. We emphasise the significance of resource allocation in cyber resilience. Adequate human, financial, and technological resources are essential for mitigating cyber-attack impact and ensuring a timely recovery. By quantifying the effect of adding resources on cyber resilience, organisations can make informed decisions regarding resource allocation and prioritise investments in areas critical for cyber resilience enhancement.

4.5. Network Topology Factor of Cyber Resilience

Figure 14 demonstrates the practical results that indicate the powerful performance of cyber resilience with the tree, star, and ring network topologies configuration. The graph showed that the tree, star, ring, and mesh network topologies started recovery at 45.5 seconds. The mesh network topology performed very slowly to complete the recovery at 114.5 seconds. The results show how different network configurations impact cyber resilience, with the mesh topology being particularly demonstrative.

The results for the network topology factor indicate the impact of different network configurations on cyber resilience. The mesh topology demonstrates a longer recovery process, starting at 45.5 seconds and completing at 114.5 seconds. It has a longer recovery duration of 69 seconds, which might be due to the complexity of the mesh network. On the other hand, the tree, star, and ring topologies show faster recovery times, starting at 45.5 seconds and completing within 55 seconds. The recovery duration for these topologies is shorter and takes around 9.5 seconds compared with a mesh topology. However, the adaption duration is longer for the tree, star, and ring topologies, indicating a need for more time to learn from the attack and implement improvements.

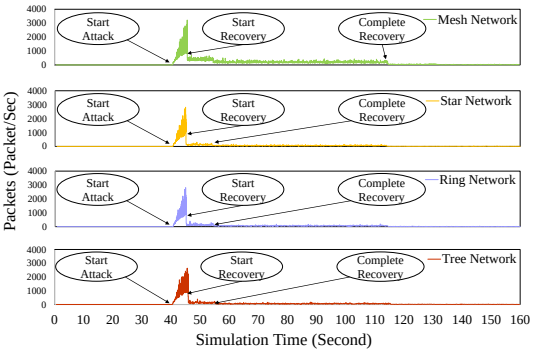


Figure 14: The network topology will affect the cyber resilience quantification compared with baseline cyber resilience.

We extensively investigate the impact of network topology on cyber resilience. The numerical values obtained from the simulation help assess the effectiveness of different network structures in responding to DDoS attacks. Mesh topologies, characterised by complex interconnections, exhibit longer recovery duration than other topologies. While mesh topologies offer redundancy and distributed processing capabilities, they may require more time to recover from an attack due to intricate interdependencies.

The network topology factors collectively exhibit high scores in planning / preparing and absorption phases, ranging from 60.04% to 77.86%. These scores suggest robust initial defences and incident detection capabilities. However, they all reveal notable weaknesses in the recovery (ranging from 11.43% to 26.37%) and adaptation phases, indicating the imperative to enhance resilience against prolonged cyber-attacks and adapt to evolving attacks. Improving the recovery and adaptation of network topologies is essential for strengthening cyber resilience. Focusing on addressing vulnerabilities in this area should be a top priority.

The mesh network topology demonstrates a commendable overall cyber resilience score of 60.04%. This topology excels in the planning / preparing phase

(100%) and absorption phase (100%), indicating a robust initial defence and incident detection capability. In these phases, the mesh network provides extensive redundancy and multiple paths for data to travel, enhancing its ability to absorb and detect threats effectively. However, its weaker points lie in the recovery (13.77%) and adaptation (26.37%) phases, suggesting vulnerabilities in terms of bouncing back from cyber-attacks and adapting to evolving threats. To improve overall cyber resilience, focusing on recovery and adaptation strategies within the mesh network topology is crucial.

The tree network topology shares a higher cyber resilience score of 77.86% with star and ring topologies. It excels in both the planning / preparing and absorption phases, achieving perfect scores (100%). This suggests that the tree topology offers robust initial defences and efficient cyber-attack detection capabilities. However, the tree topology reveals a substantial weakness in the recovery (100%) and adaptation (11.43%) phases. While it can effectively mitigate and detect threats initially, it needs help in terms of recovering from attacks and adapting to evolving cyber-attacks. In order to strengthen its overall ability to withstand cyber-attacks, it is crucial to implement strategies that focus on improving recovery and adaptability.

Similar to the tree network topology, the star network topology demonstrates a high overall cyber resilience score of 77.86%. During the planning and preparation stages, it achieves perfect scores of 100% and is highly effective at absorption. This indicates strong initial defences and effective threat detection capabilities. However, it also exhibits notable weaknesses in the recovery (100%) and adaptation (11.43%) phases. The star topology appears effective at the beginning of an attack, but it struggles with recovering from incidents and adjusting to new cyber-attacks. To improve its overall cyber resilience, it is important to implement better recovery and adaptation strategies.

The ring network topology shares the same high overall cyber resilience score of 77.86% as the tree and star topologies. The scores achieved in the planning, preparation, and absorption phases are flawless with a perfect 100%. This demonstrates the robustness of the initial defences and the effectiveness of the attack detection capabilities. Similar to other topologies, this particular system encounters significant challenges during the recovery phase, with a success rate of only 100%. Additionally, it also faces notable weaknesses during the adaptation phase, with a success rate of 11.43%. This highlights the need to improve recovery and adaptation strategies within the ring network topology to enhance its overall cyber resilience.

On the other hand, tree, star, and ring topologies recover relatively faster due to their hierarchical or centralised structures but may be more susceptible to single points of failure. Organisations can leverage these insights to design and implement network topologies that align with their specific resilience requirements. Reliability, scalability, fault tolerance, and recovery time objectives can be considered when selecting the appropriate network topology to improve cyber resilience.

4.6. Pre-configuration Factor of Cyber Resilience

Figure 15 defines the testing results that indicate some significant distinction between the enabled and disabled pre-configuration factors of cyber resilience. The graph shows different start recoveries for the enabled and disabled pre-configuration factors. This shows that the enabled pre-configuration is more potent for cyber resilience and can start and complete comeback faster than the disabled pre-configuration. Likewise, the disabled pre-configuration factor is incapable of reconfiguring and continues to be affected by cyber-attacks. Enabling pre-configuration improves the system's performance with a start recovery time of 55.5 seconds and a total recovery time of 148 seconds, compared to disabled pre-configuration for cyber resilience.

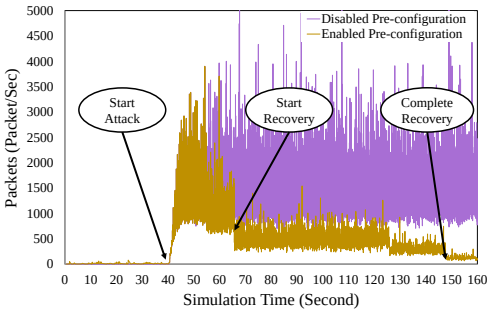


Figure 15: The enabled and disabled IT infrastructure pre-configuration will affect cyber resilience quantification performance.

The results for the pre-configuration factor show that the system takes 55.5 seconds to start the recovery process after the cyber-attack. It then requires 148 seconds to achieve complete recovery, which is longer than other factors. The absorb duration of 15.5 seconds suggests that the system has some measures to mitigate the attack's impact. However, the recovery duration of 92.5 seconds indicates that it takes significant time to restore

the system to its accepted state. The shorter adaption of 12 seconds suggests that the system can quickly learn from the attack and implement improvements.

These results highlight the importance of pre-configuring the IT infrastructure to improve cyber resilience. The start recovery time of 55.5 seconds suggests that the system initiates the recovery process relatively quickly. However, the whole recovery time of 148 seconds indicates that achieving full recovery takes considerable time. This longer recovery duration might be due to factors such as the complexity of the IT infrastructure or the extent of the damage caused by the cyber-attack. The absorb duration of 15.5 seconds suggests that the system has some measures to mitigate the attack's impact.

The pre-configuration factor exhibits the highest overall cyber resilience score, reaching 61.44%. This factor particularly excels in the planning/preparing phase, achieving a perfect score of 100%, signifying a strong foundation for proactive cyber-attack mitigation. Additionally, its high score in adaptation (100%) underscores its readiness to evolve and respond to changing threat landscapes. However, this factor encounters challenges in the absorption (35.48%) and recovery (10.27%) phases, indicating the need for substantial improvements in effectively absorbing and recovering from cyber-attacks. While it lays a solid groundwork for preparation and adaptation, there is a clear call for enhancing its resilience in mitigating and recovering from cyber-attacks.

4.7. Buffering Supported Factor of Cyber Resilience

Figure 16 shows the experimental results that indicate some substantial difference between the baseline cyber resilience performance and the configuration of the buffering-supported factor of cyber resilience. The result indicates that the buffering support started recovery at 55.5 seconds and completed the comeback at 115 seconds. However, the baseline cyber resilience method performed lower than the buffering-supported cyber resilience, which created the rally at 65 seconds and took more time for complete recovery at 148 seconds.

Conversely, the buffering-supported factor results show that the system starts the recovery process at 55.5 seconds and achieves complete recovery within 115 seconds. The absorb duration of 15.5 seconds suggests that the system effectively mitigates the attack's impact. The recovery duration of 59.5 seconds indicates that restoring the system takes an average time. The adaption duration of 45 seconds suggests that the system requires significant time to learn from the attack and implement improvements.

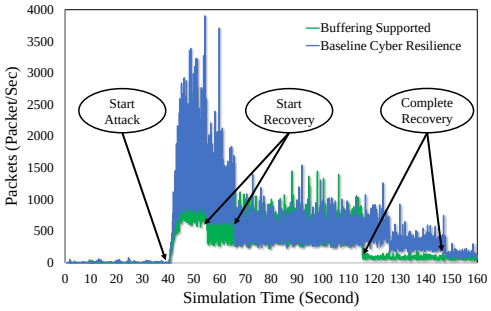


Figure 16: The buffering supported will affect the cyber resilience quantification compared with baseline cyber resilience.

The recovery duration of 59.5 seconds implies that the system can restore its normal operations within a moderate amount of time. This duration might be influenced by factors such as the efficiency of recovery processes, backup system availability, or the affected components' complexity. Interestingly, the relatively longer adaption duration of 45 seconds suggests that the system requires more time to learn from the attack and implement improvements. This signifies that the organisation takes a more thorough approach to analyse the attack, conduct post-incident reviews, and implement measures to enhance cyber resilience in the future.

The buffering supported factor demonstrates a moderate level of cyber resilience, with an overall score of 44.53%. It particularly shines in planning / preparing (100%) and adaptation (44.53%), signifying a solid foundation for readiness and adaptability. Nevertheless, it faces challenges in absorption (35.48%) and recovery (15.97%), highlighting the necessity of bolstering its capabilities to respond to and recover from cyber-attacks effectively. Enhancing overall cyber resilience requires not only initial preparedness and adaptability but also addressing vulnerabilities in response and recovery.

4.8. Significant Findings

The following findings offer valuable insights into the effectiveness of different factors influencing cyber resilience. Managing complexity is crucial as it can make controlling cyber-attacks more challenging. Therefore, strategies that help manage complexity are vital in enhancing overall resilience. Different network topologies like star, mesh, tree, and ring affect resilience differently.

Choosing the proper topology is essential for improving network and system resilience. Adding redundant resources increases the system's ability to withstand and recover from attacks. Resource allocation is also a significant factor in improving cyber resilience. Pre-configured infrastructure enables swift restoration and adaptation, which is beneficial in the face of cyber-attacks. Automated restoration processes are critical for improving overall resilience. Furthermore, buffering and caching functions can help improve data availability and access during attacks, significantly contributing to faster recovery and adaptation. By examining these factors in detail, we can understand their importance in enhancing cyber resilience. Organisations can improve their resilience against cyber threats by focusing on the most impactful strategies.

Our evaluation demonstrates how the proposed factors can affect cyber resilience quantification. Thus, our factors of cyber resilience quantification will help propose a CRQF that offers to quantify and can accommodate the IT Infrastructure cyber resilience demands of various network configurations.

These results provide insights into the time the system or network takes to recover from a cyber-attack and the duration of different phases within the framework. Each factor and topology demonstrates varying start recovery times, total recovery times, absorb duration, recovery duration, and adapt duration. These metrics help to assess the system's resilience and the effectiveness of different factors and topologies in responding to cyber-attacks.

We only provide a comprehensive summary of its impact on cyber resilience with specific values for managing complexity factors. However, the other elements and network topologies highlight the significance of adding resources, pre-configuration, and buffering support in reducing recovery time and enhancing cyber resilience.

Organisations can use these results to identify areas for improvement and allocate resources based on the relative importance of each factor and topology within their specific IT infrastructure. Organisations can strengthen their security posture and response capabilities by understanding their cyber resilience levels and the impact of cyber attacks.

5. Conclusion and Future Directions

In this study, we have investigated the cyber resilience of IT infrastructure networks and systems to propose a quantification framework called the CRQF. We have discussed the various phases of cyber resilience and put forth five factors contributing to the resilience of IT infrastructure networks and systems. We evaluated the proposed factors by simulating the framework process and implementing cyber resilience by generating traffic networks using DDoS zombie attacks. Our evaluation results demonstrate the framework's effectiveness in guiding the analysis of cyber resilience in IT infrastructure networks and systems.

The examination process carried out in this research has important implications for IT infrastructure operators and technical experts. It provides valuable insights into the architecture of their networks and systems, enabling them to enhance their resilience against cyber-attacks. By understanding the five proposed factors and applying the CRQF, operators and experts can make informed decisions to bolster the security and robustness of their IT infrastructure. Many potential research directions can be summarised for the CRQF outlined in Figure 17.

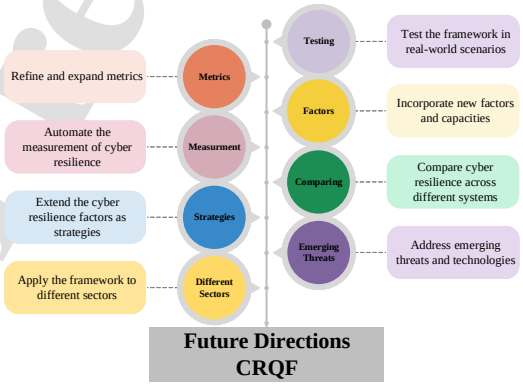


Figure 17: Future research directions for the CRQF framework.

Overall, this research contributes to the cyber resilience field by presenting a comprehensive framework and highlighting the essential factors that influence the resilience of IT infrastructure networks and systems. Further research is needed to develop advanced factors, techniques, and strategies to enhance cyber resilience and protect critical information systems from cyber-attacks.

One important next step in this work would be to test the developed framework in real-world scenarios. This could involve conducting case studies or simulations of cyber-attacks and measuring the system's resilience using the developed metrics. Testing the framework this way would validate its effectiveness in quantifying cyber resilience and identify any areas needing refinement

or modification.

As the framework is tested and used, it may become apparent that specific metrics could be more helpful and effective in measuring cyber resilience. Thus, another potential avenue for future work would be to refine the metrics to ensure that they accurately capture the relevant factors and capacities of cyber resilience. This could involve modifying existing metrics or developing new ones to capture the nuances of cyber resilience better.

Incorporating new factors and capacities into the framework as the cybersecurity landscape evolves is also an important consideration for future work. This could involve adding new metrics or modifying existing ones to reflect the cyber-attacks changing nature. The framework can remain relevant and effective in measuring cyber resilience by staying up-to-date with emerging threats and vulnerabilities.

Automating the measurement of cyber resilience is another potential area for future work. The framework and metrics developed in this research could help organisations develop automated tools that help organisations monitor their cyber resilience over time. These tools could be integrated into existing cybersecurity platforms or be developed as standalone products to help organisations stay ahead of emerging threats.

Comparing the cyber resilience of different systems, such as organisations or IT infrastructures, is another potential application of the framework and metrics. By doing so, it would be possible to identify best practices and areas for improvement in cyber resilience. This could help organisations benchmark their resilience against their peers and identify areas where they may fall behind.

Future research could focus on refining the metrics within each dimension of cyber resilience identified in the framework. This may involve specifying data sources, measurement methods, and indicators relevant to each metric. Additionally, guiding data collection strategies and tools would facilitate organisations in assessing their accurate cyber resilience posture effectively.

We believe collaboration with industry stakeholders and practitioners could offer valuable insights into implementing the framework's practical challenges and opportunities. Researchers can ensure that the developed metrics align closely with organisational needs and operational realities by incorporating their feedback and expertise.

While this work lays a foundation by identifying key dimensions of cyber resilience, further refinement and specificity in developing metrics are warranted to support organisations in assessing their cyber resilience posture accurately.

Extending the proposed cyber resilience factors as strategies is an important area of future work. This can involve exploring additional factors that can contribute to resilience and developing strategies to address each of these factors. For example, one possible extension area could be the development of strategies to address the human factor in cyber resilience.

While the proposed framework includes factors such as network topology and IT infrastructure preconfiguration, it does not explicitly address the role of employees and human behaviour in cyber resilience. Developing strategies to address this factor, such as training employees in cybersecurity best practices and creating a culture of security awareness, could significantly improve overall resilience.

Another extension area could be the development of strategies to address emerging threats and technologies. As the threat landscape continues to evolve, it will be necessary to assess the framework and identify areas for improvement continually. This could involve incorporating new factors into the framework, such as using artificial intelligence and machine learning in cyber-attacks and developing strategies to address these emerging threats. Extending the proposed cyber resilience factors as strategies can help organisations stay ahead of the evolving threat landscape and continually improve their resilience against cyber-attacks.

Finally, the framework could be applied to different sectors beyond the initial sector it is developed. This could help identify sector-specific challenges and opportunities for improving cyber resilience. For example, the framework for critical infrastructure, finance, healthcare, or government would help identify sector-specific vulnerabilities and help organisations develop more targeted strategies for improving their cyber resilience.

List of Acronyms

BN	Bayesian Network
CLI	Command-Line Interface
CRQF	Cyber Resilience Quantification Framework
CPS	Cyber-Physical Systems
DBN	Dynamic Bayesian Network
DDoS	Distributed Denial of Service

IDS	Intrusion Detection Systems
GUI	Graphical User Interface
NAS	National Academy of Sciences
NETA	NETwork Attacks
OMNeT++	Objective Modular Network Testbed in C++
PReSET	Policy-driven Resilience Strategy Evaluation Toolset
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information and Event Management
SOC	Security Operations Centre
STS	Socio-technical Systems

References

[1] I. B. M. Security, "IBM: Cost of a data breach report," *Computer Fraud Security*, 2023, ISSN: 1361-3723. DOI: 10.1016/s1361-3723(21)00082-8. [Online]. Available: https://www.ibm.com/downloads/cas/E3G5JMBP.

[2] J. Singh *et al.*, *Resilient risk based adaptive authentication and authorization (RAD-AA) framework*. Springer Nature Singapore, 2024, vol. 1075 LNEE, pp. 371–385, ISBN: 9789819950904. DOI: 10.1007/978-981-99-5091-1_27.

[3] A. Kott and I. Linkov, "To improve cyber resilience, measure it," *IEEE*, vol. 54, no. 2, pp. 80–85, 2021, ISSN: 15580814. DOI: 10.1109/MC.2020.3038411.

[4] A. K. Ligo *et al.*, "How to measure cyber-resilience of a system with autonomous agents: Approaches and challenges," *IEEE Engineering Management Review*, vol. 49, no. 2, pp. 89–97, 2021, ISSN: 19374178. DOI: 10.1109/EMR.2021.3074288.

[5] S. M. Alhidaifi *et al.*, "A Survey on cyber resilience: Key strategies, research challenges, and future directions," *ACM Computing Surveys*, 2024. DOI: 10.1145/3649218.

[6] A. Kott *et al.*, "Mathematical modeling of cyber resilience," *Proceedings - IEEE Military Communications Conference MILCOM*, vol. 2022-Novem, pp. 849–854, 2022. DOI: 10.1109/MILCOM55135.2022.10017731. eprint: 2302.04413.

[7] T. Aoyama *et al.*, "Studying resilient cyber incident management from large-scale cyber security training," *2015 10th Asian Control Conference: Emerging Control Techniques for a Sustainable World, ASCC 2015*, pp. 1–4, 2015. DOI: 10.1109/ASCC.2015.7244713.

[8] F. Björck *et al.*, "Cyber resilience – Fundamentals for a definition," in *Advances in Intelligent Systems and Computing*, vol. 353, 2015, pp. 311–316, ISBN: 9783319164854. DOI: 10.1007/978-3-319-16486-1_31.

[9] R. Ayoub *et al.*, "Cyber resilience in the digital age implications for the GCC region," *EY & World Government Summit*, 2017.

[10] P. Institute and IBM, "The third annual study on the cyber resilient organization: Asia-pacific," Tech. Rep., 2018. [Online]. Available: https://www.bankinfosecurity.com/whitepapers.php?wp_id=5002&preview=inactive_whitepaper#dynamic-popup.

[11] B. Cassottana *et al.*, "Resilience analysis of cyber-physical systems: A review of models and methods," *Risk Analysis*, pp. 1–21, 2023, ISSN: 15396924. DOI: 10.1111/risa.14089.

[12] S. Jiang *et al.*, "A quantitative framework for network resilience evaluation using dynamic bayesian network," *Computer Communications*, vol. 194, no. October 2020, pp. 387–398, 2022, ISSN: 1873703X. DOI: 10.1016/j.comcom.2022.07.042.

[13] A. Marino and E. Zio, "A framework for the resilience analysis of complex natural gas pipeline networks from a cyber-physical system perspective," *Computers and Industrial Engineering*, vol. 162, p. 107 727, 2021, ISSN: 03608352. DOI: 10.1016/j.cie.2021.107727. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0360835221006318.

[14] L. Das *et al.*, *Measuring smart grid resilience: Methods, challenges and opportunities*, 2020. DOI: 10.1016/j.rser.2020.109918. [Online]. Available: https://doi.org/10.1016/j.rser.2020.109918.

[15] N. U. I. Hossain *et al.*, "A framework for modeling and assessing system resilience using a bayesian network: A case study of an interdependent electrical infrastructure system," *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 62–83, Jun. 2019, ISSN: 18745482. DOI: 10.1016/J.IJCIP.2019.02.002.

[16] N. Yodo and P. Wang, "Resilience modeling and quantification for engineered systems using Bayesian networks," *Journal of Mechanical Design, Transactions of the ASME*, vol. 138, no. 3, 2016, ISSN: 10500472. DOI: 10.1115/1.4032399.

[17] S. Hosseini *et al.*, "A general framework for assessing system resilience using Bayesian networks: A case study of sulfuric acid manufacturer," *Journal of Manufacturing Systems*, vol. 41, pp. 211–227, 2016, ISSN: 02786125. DOI: 10.1016/j.jmsy.2016.09.006. [Online]. Available: http://dx.doi.org/10.1016/j.jmsy.2016.09.006.

[18] N. Yodo and P. Wang, *Engineering resilience quantification and system design implications: A literature survey*, 2016. DOI: 10.1115/1.4034223.

[19] R. Francis and B. Bekera, *A metric and frameworks for resilience analysis of engineered and infrastructure systems*, 2014. DOI: 10.1016/j.ress.2013.07.004. [Online]. Available: http://dx.doi.org/10.1016/j.ress.2013.07.004.

[20] E. D. Vugrin and J. Turgeon, "Advancing cyber resilience analysis with performance-based metrics from infrastructure assessments," *IGI Global*, no. 505, 2014.

[21] B. Todorovic *et al.*, "Resilience and evolution - angola banking survey," *University of Belgrade*, vol. 9, no. 1, pp. 41–45, 2016. DOI: 10.1007/978-94-024-1123-2.

[22] D. Bodeau and R. Graubart, "Cyber resilience metrics : Key observations," *MITRE*, no. 16, pp. 1–10, 2016.

[23] O. Lemeshko *et al.*, "Cyber resilience approach based on traffic engineering fast reroute with policing," *CEUR Workshop Proceedings*, vol. 2923, 2021, ISSN: 16130073.

[24] O. Lemeshko *et al.*, "Redundancy cyber resiliency technique based on fast rerouting under security metric," *2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020 - Proceedings*, 2021. DOI: 10.1109/PICST51311.2020.9468072.

[25] C. Onwubiko, "Focusing on the recovery aspects of cyber resilience," *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020*, 2020. DOI: 10.1109/CyberSA49311.2020.9139685.

[26] V. Tzavara and S. Vassiliadis, "Tracing the evolution of cyber resilience: a historical and conceptual review," *International Journal of Information Security*, 2024, ISSN: 16155270. DOI: 10.1007/s10207-023-00811-x. [Online]. Available: https://doi.org/10.1007/s10207-023-00811-x.

[27] A. Mentges *et al.*, "A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures," *International Journal of Disaster Risk Reduction*, vol. 96, no. February, p. 103 893, 2023, ISSN: 22124209. DOI: 10.1016/j.ijdrr.2023.103893.

[28] D. I. Christine and M. Thinyane, "Socio-technical cyber resilience: A systematic review of cyber resilience management frameworks," in *Springer*, Springer, Cham, 2022, pp. 573–597, ISBN: 978-3-031-15420-1. DOI: 10.1007/978-3-031-15420-1_28.

[29] E. Bellini *et al.*, "Cyber resilience meta-modelling: The railway communication case study," *Electronics (Switzerland)*, vol. 10, no. 5, pp. 1–26, Mar. 2021, ISSN: 20799292. DOI: 10.3390/electronics10050583.

[30] I. Linkov *et al.*, "Resilience metrics for cyber systems," *Environment Systems and Decisions*, vol. 33, no. 4, pp. 471–476, 2013, ISSN: 21945411. DOI: 10.1007/s10669-013-9485-y.

[31] M. Thinyane and D. Christine, "SMART citizen cyber resilience (SC2R) ontology," 2020. DOI: 10.1145/3433174.3433617.

[32] P. M *et al.*, "Cyber resilience and response," Tech. Rep., 2018, pp. 1–45.

[33] J. R. C. Nurse, *Cyber resilience: What is it and how do we get it?* [Online]. Available: https://crestresearch.ac.uk/comment/nurse-cyber-resilience/ (visited on 06/22/2023).

[34] Brianna Keys *et al.*, "A framework for assessing cyber resilience," *World Economic Forum*, pp. 1–55, 2016. [Online]. Available: http://bloustein.rutgers.edu/wp-content/uploads/2016/05/2016_WEF.pdf.

[35] EY, "Insights on governance, risk and compliance Achieving resilience in the cyber ecosystem," Tech. Rep., 2014.

[36] D. J. Bodeau *et al.*, "Cyber resiliency engineering overview of the architectural assessment process," *Procedia Computer Science*, vol. 28, pp. 838–847, 2014, ISSN: 18770509. DOI: 10.1016/j.procs.2014.03.100.

[37] E. Alvarenga *et al.*, "Cyber resilience for the Internet of Things: Implementations with resilience engines and attack classifications," pp. 1–16, 2022. DOI: 10.1109/TETC.2022.3231692.

[38] A. El Korchi, "Survivability, resilience and sustainability of supply chains: The COVID-19 pandemic," *Journal of Cleaner Production*, vol. 377, no. May, p. 134 363, 2022, ISSN: 09596526. DOI: 10.1016/j.jclepro.2022.134363.

[39] E. B. Connelly *et al.*, "Features of resilience," *Environment Systems and Decisions*, vol. 37, no. 1, pp. 46–50, Mar. 2017, ISSN: 21945411. DOI: 10.1007/s10669-017-9634-9.

[40] D. Bodeau and R. Graubart, "Structured cyber resiliency analysis methodology (SCRAM)," *MITRE CORP MCLEAN VA*, no. 16, p. 13, 2016.

[41] S. Hosseini *et al.*, "A review of definitions and measures of system resilience," *Reliability Engineering and System Safety*, vol. 145, pp. 47–61, Jan. 2016, ISSN: 09518320. DOI: 10.1016/J.RESS.2015.08.006. [Online]. Available: http://dx.doi.org/10.1016/j.ress.2015.08.006.

[42] S. Hosseini and K. Barker, "Modeling infrastructure resilience using Bayesian networks: A case study of inland waterway ports," *Computers and Industrial Engineering*, vol. 93, pp. 252–266, Mar. 2016, ISSN: 03608352. DOI: 10.1016/J.CIE.2016.01.007. [Online]. Available: http://dx.doi.org/10.1016/j.cie.2016.01.007.

[43] E. D. Vugrin *et al.*, "A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane," *Process Safety Progress*, vol. 30, no. 3, pp. 280–290, Sep. 2011, ISSN: 10668527. DOI: 10.1002/PRS.10437.

[44] S. Hosseini *et al.*, "Conceptualization and measurement of supply chain resilience in an open-System context," *IEEE Transactions on Engineering Management*, pp. 1–16, 2020, ISSN: 15580040.

[45] A. A. Ganin *et al.*, "Operational resilience: Concepts, design and analysis," *Scientific Reports*, vol. 6, 2016, ISSN: 20452322. DOI: 10.1038/srep19540.

[46] T. Welsh and E. Benkhelifa, "On resilience in cloud computing: A survey of techniques across the cloud domain," *ACM Computing Surveys*, vol. 53, no. 3, 2020, ISSN: 15577341. DOI: 10.1145/3388922.

[47] A. Kott and I. Linkov, "Fundamental concepts of cyber resilience: Introduction and overview," in *Cyber Resilience of Systems and Networks*, 2019, p. 471, ISBN: 978-3-319-77491-6. DOI: 10.1007/978-3-319-77492-3.

[48] M. Jafarian *et al.*, "Resilient identification of distribution network topology," *IEEE Transactions on Power Delivery*, vol. 36, no. 4, pp. 2332–2342, 2021, ISSN: 19374208. DOI: 10.1109/TPWRD.2020.3037639. eprint: 2011.07981.

[49] M. R. Awal *et al.*, "Architecture and network-on-chip implementation of a new hierarchical interconnection network," *Journal of Circuits, Systems and Computers*, vol. 24, no. 2, 2015, ISSN: 02181266. DOI: 10.1142/S021812661540006X.

[50] D. Fan *et al.*, "A modified connectivity link addition strategy to improve the resilience of multiplex networks against attacks," *Reliability Engineering and System Safety*, vol. 221, no. December 2021, p. 108 294, 2022, ISSN: 09518320. DOI: 10.1016/j.ress.2021.108294.

[51] D. R. Keppler *et al.*, "Experimentation and implementation of BFT++ cyber-attack resilience mechanism for cyber physical systems," *ACM Transactions on Cyber-Physical Systems*, 2024, ISSN: 2378-962X. DOI: 10.1145/3639570.

[52] K. Paridari *et al.*, "A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 113–128, 2018, ISSN: 15582256. DOI: 10.1109/JPROC.2017.2725482.

[53] T. Xie *et al.*, "Attack resilience of cache replacement policies," *Proceedings - IEEE INFOCOM*, vol. 2021-May, no. 6, pp. 2433–2447, 2021, ISSN: 0743166X. DOI: 10.1109/INFOCOM42981.2021.9488697.

[54] K. W. Lee *et al.*, "Improving the resilience of content distribution networks to large scale distributed denial of service attacks," *Computer Networks*, vol. 51, no. 10, pp. 2753–2770, 2007, ISSN: 13891286. DOI: 10.1016/j.comnet.2006.11.025.

[55] N. Fairburn *et al.*, *Beyond murphy's law: Applying wider human factors behavioural science approaches in cyber-Security resilience: An applied practice case study discussing approaches to assessing human factors vulnerabilities in cybersecurity systems*. Springer International Publishing, 2021, vol. 12788 LNCS, pp. 123–138, ISBN: 9783030773915. DOI: 10.1007/978-3-030-77392-2_9.

[56] G. Giacomello and G. Pescaroli, "Managing human factors," in *Cyber resilience of systems and networks*, January, Springer International Publishing, 2019, ISBN: 9783319774923. DOI: 10.1007/978-3-319-77492-3.

[57] R. van der Kleij and R. Leukfeldt, *Cyber resilient behavior: Integrating human behavioral models and resilience engineering capabilities into cyber security*. Springer International Publishing, 2020, vol. 960, pp. 16–27, ISBN: 9783030204877. DOI: 10.1007/978-3-030-20488-4_2.

[58] O. Kammouh *et al.*, "Probabilistic framework to evaluate the resilience of engineering systems using Bayesian and dynamic Bayesian networks," *Reliability Engineering and System Safety*, vol. 198, no. March 2019, p. 106 813, 2020, ISSN: 09518320. DOI: 10.1016/j.ress.2020.106813.

[59] N. Yodo *et al.*, "Predictive resilience analysis of complex systems using dynamic bayesian networks," *IEEE Transactions on Reliability*, vol. 66, no. 3, pp. 761–770, 2017, ISSN: 00189529. DOI: 10.1109/TR.2017.2722471.

[60] A. Schaeffer-Filho *et al.*, "PReSET: A toolset for the evaluation of network resilience strategies," *Proceedings of the 2013 IFIP/IEEE International Symposium on Integrated Network Management, IM 2013*, pp. 202–209, 2013.

[61] *OMNeT++ Discrete Event Simulator*. [Online]. Available: https://omnetpp.org/ (visited on 04/08/2023).

[62] K. Twidle *et al.*, "Ponder2: A policy system for autonomous pervasive environments," *Proceedings of the 5th International Conference on Autonomic and Autonomous Systems, ICAS 2009*, pp. 330–335, 2009. DOI: 10.1109/ICAS.2009.42.

[63] *INET framework - INET Framework*. [Online]. Available: https://inet.omnetpp.org/ (visited on 04/08/2023).

[64] T. Gamer and M. Scharf, "Realistic simulation environments for IP-based networks," 2009. DOI: 10.4108/icst.simutools2008.3079.

[65] M. Tiloca *et al.*, "SEA++: A framework for evaluating the impact of security attacks in OMNeT++/INET," in *Innovations in Communication and Computing*, Springer, 2019, pp. 253–278. DOI: 10.1007/978-3-030-12842-5_7.

[66] L. Sánchez-Casado *et al.*, "NETA: Evaluating the effects of NETwork attacks. MANETs as a case study," in *Advances in Security of Information and Communication Networks*, vol. 381 CCIS, 2013, pp. 1–10, ISBN: 9783642405969. DOI: 10.1007/978-3-642-40597-6_1.

Saleh Mohamed AlHidaifi completed his master’s in computer security and Forensics from the University of Bedfordshire in the United Kingdom in 2014. He is pursuing a PhD in Cyber Security and Cyber Resilience from Glasgow University. His research interests include Artificial Intelligence, Computer Forensics, Information Security, Network Security, and 5G Communication Security. Since 2005, he has worked with the Muscat Municipality of Oman's Muscat Government as a Senior Information Security Professional.

Muhammad Rizwan Asghar is an Associate Professor at the Surrey Centre for Cyber Security (SCCS) at the University of Surrey, United Kingdom. He is also an Honorary Academic in the School of Computer Science at the University of Auckland in New Zealand. He received his PhD degree from the University of Trento, Italy in 2013. As part of his PhD programme, he was a Stanford Research Institute (SRI) Fellow at SRI International, California, USA. He obtained his MSc degree in Computer Science and Engineering - Information Security Technology from the Eindhoven University of Technology (TU/e), The Netherlands in 2009 and carried out his research as a Master Thesis Student at the Ericsson Research Eurolab, Germany. His research interests include cyber resilience, privacy, cyber security, and access control.

Imran Shafique Ansari received a B.Sc. degree in Computer Engineering from King Fahd University of Petroleum and Minerals (KFUPM) in 2009 (with First Honors) and M.Sc. and PhD degrees from King Abdullah University of Science and Technology (KAUST) in 2010 and 2015, respectively. Since August 2018, he has been a Lecturer (Assistant Professor) at the University of Glasgow, Glasgow, UK. Before this, from November 2017 to July 2018, he was a Lecturer (Assistant Professor) with the Global College of Engineering and Technology (GCET) (affiliated with the University of the West of England (UWE), Bristol, UK). From April 2015 to November 2017, he was a Postdoctoral Research Associate (PRA) with Texas A&M University at Qatar (TAMUQ). From May 2009 through Aug. 2009, he was a visiting scholar with Michigan State University (MSU), East Lansing, MI, USA, and from Jun. 2010 through Aug. 2010, he was a research intern with Carleton University, Ottawa, ON, Canada. Dr. Ansari has authored/co-authored 100+ journal and conference publications. His current research interests include free-space optics (FSO), satellite communications, underwater communications, physical layer secrecy issues, and reconfigurable intelligent surfaces / intelligent reflective surfaces (RIS / IRS), among others.

Imran_Ansari_Author_Photo

Click here to access/download;Author Photo;Imran_Ansari_Author_Photo.tif

Rizwan_Asghar_Author_Photo

Click here to access/download;Author Photo;Rizwan_Asghar_Author_Photo.tif

Saleh_AlHidaifi_Author_Photo

Declaration of interests

☒ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☐ The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: