APPENDIX

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

A APPLICATIONS OF CYBER RESILIENCE

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

A.1 Cyber Resilience in Transportation Sector

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

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

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

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

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

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

A.2 Cyber Resilience in Financial Sector

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

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

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

A.3 Cyber Resilience in Power System

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

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

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

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

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

A.4 Cyber Resilience in Supply Chain

Chris and Omera [36] conferred cyber resilience in the supply chain that has received lesser attention than security, cyber risk, and resilience. That may be because, naturally, most experts view IT security as mainly responsible for cyber-related issues. This compartmentalisation of disciplines is the main problem and must be resolved to achieve cyber resilience in the supply chain. They highlighted the significance of cyber resilience in the supply chain. They developed a shared understanding of the theory, definition, and managerial implications of cyber resilience and risk in the supply chain.

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

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

A.5 Cyber Resilience in SCADA Systems

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

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

A.6 Cyber Resilience in Smart Grid

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

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

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

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

To address the consensus problem in networked intelligent grids, especially in MGs subject to multi-layer DoS attacks presented by Ge *et al.* [55]. The authors proposed a unified notion of Persistency-of-Data-Flow (PoDF) to characterize the data unavailability in different information network links and quantify the multi-layer DoS effects on the hierarchical system. The authors provide a sufficient condition for preserving consensus under DoS attacks with the proposed edge-based self-triggered distributed control framework. An online self-adaptive scheme of control parameters is developed to mitigate the conservativeness of offline design against the worst-case attack. The effectiveness of the proposed cyber resilience self-triggered distributed control is verified through representative case studies.

A.7 Cyber Resilience in Communication Networks

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

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

A.8 Cyber Resilience in Healthcare

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

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

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

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

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

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

A.9 Cyber Resilience in ICS

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

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

B LIST OF ACRONYMS

ADS	Active Directory Server	**AI**	Artificial Intelligence
AHP	Analytical Hierarchy Process	**AM**	Additive Manufacturing

ASD	Australian Signals Directorate
B2B	Business 2 Business
B2G	Business 2 Government
BFT++	Byzantine Fault Tolerant++
C2M2	Cybersecurity Capability Maturity Model
CERT	Computer Emergency Response Team
CERT-RMM	Computer Emergency Readiness Team-Resilience Management Model
CIA	Confidentiality, Integrity, and Availability
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technologies
CPS	Cyber-Physical Systems
CRAT	Cyber Resilience Assessment Tool
DREAD	Damage, Reproducibility, Exploitability, Affected, and Discoverability
CREF	Cyber Resilience Engineering Framework
CRI	Cyber Resilience Index
CRF	Cyber Resilience Framework
CRR	Cyber Resilience Review
CSF	Cyber Security Framework
CVE	Common Vulnerabilities and Exposure
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DoD	Department of Defense
DoS	Denial of Service
DREF	Dependability and Resilience Engineering Framework
DS	Dempster Shafer
ENISA	European Union Agency for Cybersecurity
EO 13636	Executive Order 13636
EPS	Electronic Prescribing Server
ETA	Estimated Time of Arrival
ETTR	Event-Trigger Topology Reconfiguration
GENI	Global Energy Network Institute
GUI	Graphical User Interface
HIPAA	Health Insurance Portability and Accountability
ICS	Industrial Control System
ICT	Information and Communications Technologies
ID/PS	Intrusion Detection and Prevention Systems
IDS	Intrusion Detection Systems
IoT	Internet of Things
ISO/IEC 27001	International Organisation for Standardisation/International Electrotechnical Commission 27001
IT	Information Technology
ITS	Intelligent Transportation System
JUMP	Joint User Cyber Mission Planning
MG	Microgrid
MFA	Multi-Factor Authentication
MFH	Mobile Field Hospitals
ML	Machine Learning
NATO	North Atlantic Treaty Organisation
NDN	Named Data Network
NDVCPS	Named Data Vehicular Cyber-Physical Systems
NHS	National Health Service
NIST	National Institute of Standards and Technology
NIST-CSF	National Institute of Standards and Technology (NIST) Cybersecurity Framework
NoSQL	Not Only SQL
NSCC	Non-Stop Customs Clearance
NVD	National Vulnerability Database
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OES	Operators of Essential Services
OT	Operational Technology
OWASP	Open Web Application Security Project
PAS	Patient Administration System
PASTA	Process for Attack Simulation and Threat Analysis
PC	Personal Computer

PLCs	Programmable Logic Controllers
PoDF	Persistency-of-Data-Flow
PPD 21	Presidential Policy Directive 21
PMU	Phasor Measurement Unit
RL	Reinforcement Learning
RMM	Resilience Management Model
SA	Situational Awareness
SCADA	Supervisory Control And Data Acquisition
SDLC	Software Development Life Cycle
SDL	Security Development Lifecycle
SDN	Software-Defined Networking
SIEM	Security Information and Event Management
SMEs	Small and Medium-sized Enterprises
S/MIME	Secure/Multipurpose Internet Mail Extensions
SSH	Secure Shell
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege
TMT	Threat Modelling Tool
VANET	Vehicular Adhoc Network
VAST	Visual, Agile, and Simple Threat
VCPS	Vehicular Cyber-Physical Systems
WEF	World Economic Forum