Emerging Technologies and Cybersecurity in Critical Information Infrastructure and Industrial Control Systems: An Integrated Cyber Risk Pathway Model

Jennita Rao Appanah Appayya, Sandhya Armoogum, Kaleem Ahmed Usmani
University of Technology, Mauritius, Republic of Mauritius

***Abstract*—The digital transformation of Critical Information Infrastructure (CII) and Industrial Control Systems (ICS) through Industry 4.0 technologies introduces significant cybersecurity challenges. While existing research examines technologies individually, little attention has been given to how their combined adoption reshapes the overall threat landscape. This study presents a Multivocal Literature Review, synthesising evidence from 41 academic and industry sources (January 2010–June 2026) and proposes an Integrated Cyber Risk Pathway Model that traces how technology adoption introduces interconnected vulnerabilities, expands threat actor capabilities, produces cyber-physical impacts, and ultimately defines resilience requirements. Three findings emerge: 1) emerging technologies play a dual role, enhancing operational capability while expanding the attack surface; 2) cyber-attacks have evolved from specialist ICS operations to ecosystem-level compromises exploiting supply chains and shared platforms; 3) the resulting vulnerabilities are systemically interconnected, creating risks that prevention-focused cybersecurity alone cannot fully address. The study argues that protecting modern critical infrastructure requires a shift to resilience-centred strategies supported by governance, secure system design and cross-sector collaboration.**

Keywords*—Critical Information Infrastructure (CII); Industrial Control Systems (ICS); emerging technologies; industry 4.0; IT/OT convergence; cyber resilience; cyber-physical systems; multivocal literature review; integrated cyber risk pathway model

I. Introduction

Critical Information Infrastructure (CII) is the foundation of many services on which modern societies depend. These include energy, water, healthcare, transportation, finance and telecommunications. These sectors rely heavily on Industrial Control Systems (ICS), such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS) and Programmable Logic Controllers (PLCs), to monitor and control physical processes. As these systems support critical services, cyber incidents affecting them can have consequences far beyond financial losses, disrupting public services, endangering safety and, in some cases, threatening national security [1][2].

Over the past decade, CII and ICS environments have undergone rapid digital transformation. Emerging technologies are increasingly being deployed to improve operational efficiency, enable predictive maintenance and support real-time decision-making. At the same time, organisations are integrating Information Technology (IT) and Operational Technology (OT) systems to improve visibility across operations and enable data-driven services. Although these developments deliver significant operational benefits, they also increase connectivity, introduce new dependencies, and expand the potential attack surface available to cyber adversaries [1][3].

Recent cyber incidents demonstrate that the threat landscape has evolved considerably. Earlier attacks, such as Stuxnet [15] and Triton [16], were highly specialised operations that required extensive knowledge of industrial processes and proprietary control systems. Modern attacks, however, increasingly exploit software supply chains, cloud platforms, Internet-facing devices and interconnected digital ecosystems. Consequently, adversaries are able to compromise multiple organisations without directly targeting industrial technologies themselves. This evolution indicates a wider trend - from attacks at the level of individual systems to attacks on interconnected infrastructure, in which vulnerabilities in one part of the digital ecosystem can quickly spread to several critical sectors [2][4].

A growing body of research has examined the cybersecurity implications of emerging technologies in CII and ICS environments. Previous studies have investigated areas such as Artificial Intelligence (AI) enabled systems, Industrial Internet of Things (IIoT) devices, cloud computing, digital twins, 5G networks, and industrial cybersecurity more generally [5][6][7]. These studies provide valuable insights on the security challenges of individual technologies. However, the cybersecurity landscape of modern critical infrastructure is becoming increasingly interconnected. CII operators are no longer adopting these technologies in isolation. Instead, multiple technologies are being integrated across IT and OT environments, creating new technical dependencies, external connections and shared attack surfaces.

This raises an important research problem. When emerging technologies are examined separately, it becomes difficult to understand how their combined adoption changes the overall cyber risk environment of CII and ICS. A vulnerability introduced through one technology may interact with weaknesses in another system, create new opportunities for threat actors, or allow an incident to propagate across interconnected operational environments. These relationships can ultimately result in operational disruption, physical consequences and cascading effects across critical services. There is therefore a need for an integrated perspective that connects technology adoption with vulnerability creation, threat actor capabilities, cyber-physical impacts and the resilience requirements needed to address these risks.

This study therefore addresses this gap by adopting a Multivocal Literature Review (MLR) [8], synthesising evidence from academic publications, government reports, international standards and industry threat intelligence. Rather than reviewing emerging technologies individually, the study examines how they collectively redefine cybersecurity risks within CII and ICS environments. Drawing on this synthesis, this study makes three main contributions. First, it synthesises current evidence on seven emerging technologies, namely AI, IIoT, cloud computing, edge computing, 5G, digital twins and quantum computing, to provide a unified view of how they are reshaping cybersecurity threats in CII and ICS. Second, it introduces an Integrated Cyber Risk Pathway Model that links technology adoption, emerging vulnerabilities, threat actor capabilities, cyber-physical impacts and resilience requirements into a single conceptual framework. Unlike previous research that focuses on particular technologies or isolated threats, the model shows how these interact within the wider digital ecosystem. Third, the study identifies resilience priorities that extend beyond traditional prevention-based cybersecurity, emphasising governance, secure system design, supply chain security and cross-sector collaboration as essential components of protecting modern critical infrastructure. The remainder of this study is organised around five research questions:

- RQ1: What are the main cyber threats affecting CII and ICS?
- RQ2: How are emerging technologies reshaping the cybersecurity landscape?
- RQ3: What new vulnerabilities and attack pathways are being introduced?
- RQ4: What operational, economic, physical and societal impacts arise from these threats?
- RQ5: What resilience strategies are needed to address these emerging challenges?

The findings derived from these questions are then incorporated through the proposed Integrated Cyber Risk Pathway Model, providing a conceptual foundation for understanding how digital transformation is reshaping cybersecurity and resilience in critical infrastructure.

II. Methodology

This study adopts a Multivocal Literature Review (MLR) to investigate the impact of emerging technologies on the cybersecurity landscape of CII and ICS. An MLR combines evidence from both peer-reviewed research and grey literature, making it particularly suitable for cybersecurity research, where emerging threats, vulnerabilities, and defensive practices are frequently documented in government advisories, technical standards, and industry threat intelligence before appearing in academic publications [8]. Fig. 1 summarises the overall methodology adopted in this study.

The review focused on publications from January 2010 to June 2026, covering the period during which Industry 4.0 technologies became increasingly integrated into CII and ICS environments. The literature search was last updated on 30 June 2026; therefore, publications from 2026 represent evidence available up to the search cut-off date rather than the complete publication year.

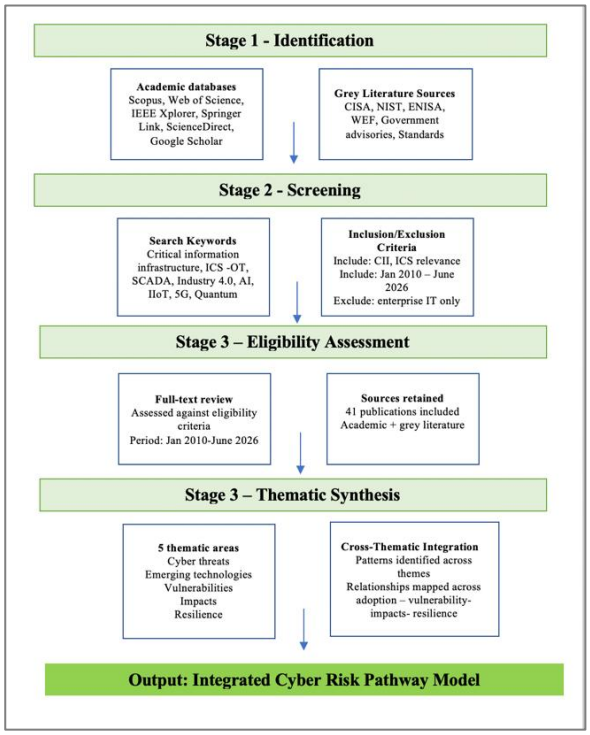

Fig. 1. Multivocal literature review process.

Academic literature was retrieved from Scopus, Web of Science, IEEE Xplore, SpringerLink, ScienceDirect and Google Scholar using a combination of keywords. Examples include Critical Information Infrastructure, Industrial Control Systems, Operational Technology, SCADA security, cyber resilience, Industry 4.0, AI, IIoT, cloud computing, edge computing, 5G, digital twins and quantum computing.

The review focuses on seven emerging technologies: AI, IIoT, cloud computing, edge computing, 5G, digital twins and quantum computing. These technologies were selected to provide coverage of major technological developments influencing connectivity, automation, data-driven operations, distributed computing and long-term cryptographic security within CII and ICS environments. The scope was intentionally limited to allow these technologies and their cybersecurity implications to be examined within a common analytical framework. Other relevant developments, including blockchain, distributed ledger technologies and autonomous industrial systems, were not examined in detail and therefore fall outside the scope of this review. Their exclusion does not mean that they are unimportant to CII and ICS cybersecurity, but that they are additional areas that could be incorporated in future extensions of the analysis.

To complement the academic literature, grey literature was collected from internationally recognised organisations, such as the Cybersecurity and Infrastructure Security Agency (CISA) [9], National Institute of Standards and Technology (NIST) [10], European Union Agency for Cybersecurity (ENISA) [11], International Society of Automation (ISA) [12] and the World Economic Forum (WEF) [13]. These sources were selected

because they provide current threat intelligence, technical guidance and policy recommendations that are highly relevant to the rapidly evolving cybersecurity landscape of critical infrastructure [8].

Given the inclusion of grey literature, the quality and credibility of non-peer-reviewed sources were also considered. These sources were assessed based on the authority of the issuing organisation, relevance to CII and ICS cybersecurity, timeliness of the information, transparency of the evidence presented, and consistency with other available sources. Priority was given to publications from recognised government agencies, standards bodies, international organisations and established cybersecurity organisations involved in critical infrastructure security or threat analysis. Industry sources were mainly used to provide information on recent cyber incidents, emerging threat activity and operational developments that may not yet be widely covered in academic literature. Peer-reviewed studies were used more comprehensively to support theoretical and conceptual arguments. The use of grey literature was, where possible, considered in the light of evidence from other independent sources. This approach helped to balance the timeliness of grey literature and the methodological rigour of academic research.

The literature selection followed four stages: identification, screening, eligibility and inclusion. Publications were included if they addressed cybersecurity issues relating to CII or ICS, examined one or more of the selected emerging technologies, or discussed cyber threats, vulnerabilities, resilience or significant cyber incidents affecting critical infrastructure. Studies focusing exclusively on conventional enterprise IT environments and that are not relevant to CII or ICS were excluded. Following the screening process, 41 publications were retained for detailed analysis. The characteristics of these publications are summarised in Table I.

TABLE I. CHARACTERISTICS OF PUBLICATIONS INCLUDED IN THE MULTIVOCAL LITERATURE REVIEW

No.	Author / Organisation, Year	Main Focus	Technology / Theme	Main RQ	Contribution to Pathway Model
1	Asghar, Hu & Zeadally, 2019 [1]	Security issues and challenges in ICS	ICS, IT/OT	RQ1, RQ2, RQ3	Determines the baseline risks, weaknesses, and increasing exposure of ICS due to digitalisation.
2	Hemsley & Fisher, 2018 [2]	Historical evolution of ICS cyber incidents	ICS threats	RQ1, RQ4	Establishes the relationship between an attack and the operational and physical consequences.
3	Katsikas et al.(2020) [3]	Computer security concepts and emerging environments	Digital transformation	RQ2	Affirms the connection between evolving security needs and technology adoption.
4	CISA, 2021 [4]	SolarWinds supply-chain compromise	Supply chain	RQ1, RQ3, RQ4	Demonstrates how trusted third-party dependencies can compromise an ecosystem.
5	Axon et al.(2022) [5]	Cybersecurity capability gaps in IIoT	IIoT	RQ2, RQ3	Demonstrates how connected industrial devices increase the attack surfaces
6	Raval et al., 2024 [6]	Critical infrastructure attacks and AI security	AI, CII	RQ1–RQ3	Connects the use of AI to new dangers, weaknesses, and defensive needs
7	Abraham et al., 2025 [7]	ICS cybersecurity using modelling, digital twins and ML	AI, digital twins	RQ2, RQ3, RQ5	Supports the advantages and security dependencies of intelligent industrial technologies
8	Langner, 2011 [14]	Analysis of Stuxnet	ICS malware	RQ1, RQ4	Demonstrates how direct physical harm can be caused by cyber manipulation
9	Cherepanov & Lipovsky, 2017 [15]	Industroyer attack	ICS malware, energy	RQ1, RQ4	Demonstrates how specialised malware is directly interfering with electrical infrastructure.
10	Pinto, Dragoni & Carcano, 2018 [16]	TRITON attack on Safety Instrumented Systems	ICS/ Safety Instrumented Systems (SIS)	RQ1, RQ4	Shows how industrial safety devices can be compromised digitally.
11	ESET Research, 2022 [17]	Industroyer2 attack	ICS malware, energy	RQ1, RQ4	Demonstrates how threats against operational technologies are still evolving.
12	Hunter, 2020 [18]	EKANS ransomware targeting ICS/OT	OT ransomware	RQ1, RQ3	Shows how ransomware is migrating from traditional IT to operational settings.
13	FBI/CISA/HHS, 2024 [19]	ALPHV/BlackCat ransomware	Ransomware	RQ1, RQ4	Demonstrates how ransomware is causing disruption across critical sectors.
14	CISA, 2016 [20]	Mirai and IoT botnets	IoT/IIoT	RQ1–RQ3	Illustrates how insecure connected devices become distributed attack infrastructure.
15	Easterly & Fanning, 2023 [21]	Colonial Pipeline ransomware	IT/OT convergence	RQ1, RQ4	Illustrates how physical operations can be shut down due to an IT compromise.
16	HHS, 2023 [22]	KillNet DDoS attacks	DDoS, multi-sector CII	RQ1, RQ4	Demonstrates a coordinated disruption that has an impact on different critical sectors.
17	FBI/CISA/NSA/EPA/INCD, 2023 [23]	Exploitation of PLCs in water systems	PLC, ICS	RQ1, RQ3, RQ4	Demonstrates the use of default login credentials and operational assets exposed to the internet.
18	CISA, 2024 [24]	Threats against communications infrastructure	Telecom, Advanced Persistent Threat (APT)	RQ1, RQ3	Demonstrates state-linked exploitation of interconnected communications infrastructure.

19	Dragos, 2026 [25]	Attack against Polish distributed energy infrastructure	Energy/OT	RQ1, RQ4	Shows how cyber risks extend to distributed and interconnected energy assets.
20	FBI/CISA, 2024 [26]	BlackSuit/Royal ransomware	Ransomware	RQ1, RQ4	Demonstrates the dangers of ransomware in the manufacturing, medical, and utility industries.
21	CYFIRMA, 2025 [27]	Jaguar Land Rover cyberattack	Manufacturing	RQ1, RQ4	Demonstrates how interconnected IT systems can create significant operational interruption.
22	Itron/SEC, 2026 [28]	Cyber compromise involving CII technology supplier	Supply chain	RQ1, RQ3	Illustrates third parties and the supply chain access to CII operators.
23	Cilluffo, 2025 [29]	Chinese Typhoon cyber campaigns	Nation-state threats, CII	RQ1, RQ3	Demonstrates state-sponsored exploitation of connected infrastructure.
24	NIST NCCoE, 2023 [31]	5G cybersecurity	5G	RQ2, RQ3, RQ5	Demonstrates new security considerations arising from virtualised and highly connected networks.
25	Kravchik, Biggio & Shabtai, 2021 [32]	Poisoning attacks against cyberattack detectors	AI/ML	RQ2, RQ3	Demonstrates manipulation of training data and loss of trust in AI-enabled monitoring.
26	Gokkaya, Aniello & Halak, 2025 [33]	Software supply-chain attacks and mitigations	Supply chain	RQ3, RQ5	Indicate how third-party dependency acts as a major pathway for systemic compromise.
27	Sharma, 2025 [34]	Cloud misconfiguration and breaches	Cloud computing	RQ2, RQ3	Demonstrates how configuration and privilege-related exposure are caused by cloud adoption.
28	ENISA, 2021 [35]	Growth of supply-chain attacks	Supply chain	RQ1, RQ3	Supports the transition from attacks targeting individual organisations to ecosystem compromise.
29	Waterfall Security Solutions, 2025 [36]	OT attacks producing physical consequences	OT, IT/OT	RQ1, RQ4, RQ5	Connects operational and physical repercussions to attacks originating from IT.
30	DHS, 2021 [37]	Preparation for post-quantum cryptography	Quantum computing	RQ2, RQ3, RQ5	Identifies long-term cryptographic exposure and the need for migration planning.
31	NIST, 2024 [38]	Post-quantum cryptography standards	Quantum computing	RQ2, RQ5	Supports post-quantum readiness as a present resilience requirement.
32	Obasuyi, 2023 [39]	Convergence of edge, 5G and cloud security	Edge, 5G, cloud	RQ2, RQ3	Illustrates how the adoption of many technologies results in interconnected attack surfaces.
33	Palleti et al., 2021 [40]	Cascading effects of cyberattacks on interconnected CI	Interdependencies	RQ4, RQ5	Provides direct evidence for the cascading and systemic impact stage of the model.
34	Erukude, Marella & Veluru, 2026 [41]	AI-driven cybersecurity threats	AI	RQ1, RQ3	Demonstrates new offensive threats connected to threat capabilities enabled by AI.
35	Center for Security and Emerging Technology, 2024 [42]	AI security in critical infrastructure	AI, CII	RQ2, RQ3, RQ5	Connects the need for resilience and CI risk management with the adoption of AI.
36	Järveläinen et al., 2025 [43]	Cybersecurity resilience of critical infrastructure	Cyber resilience	RQ5	Enhances the capacity for organisational and dynamic resilience.
37	Kott & Linkov, 2019 [44]	Cyber resilience of systems and networks	Cyber resilience	RQ5	Gives a theoretical foundation for anticipating, enduring, reacting, and recovering.
38	Claroty, 2024 [47]	Business impact of CPS security incidents	CPS/OT	RQ4	Demonstrates the operational and financial effects of cyber-physical incidents.
39	EuRepoC [49]	NotPetya cyber incident	Supply chain/systemic risk	RQ1, RQ4	Illustrates how an attack can widely propagate beyond the initially compromised organisation.
40	World Bank, 2025 [50]	Economic costs of cyber incidents	Economic impact	RQ4	Supports the evaluation of both direct and indirect economic effects.
41	DNI, 2024 [51]	Nation-state cyber threats	Geopolitical/CII threats	RQ1, RQ4	Supports national-security and societal dimensions of CII cyber risk

Rather than analysing each publication independently, the selected literature was examined through thematic and conceptual synthesis. The evidence was first organised around the five research questions that guided this study. The results were then compared across publications to identify recurrent patterns and relationships between these themes.

To strengthen the consistency of the synthesis, evidence from the selected sources was examined in relation to the five research questions and grouped according to recurring concepts identified across the literature. These included cyber threats, emerging technologies, vulnerabilities and attack pathways, cyber-physical impacts, and resilience requirements. Relationships identified across the reviewed sources were then compared to determine how developments in one area influenced another. Particular attention was given to the progression from technology adoption to vulnerability creation, the exploitation of these vulnerabilities by threat actors, the resulting operational and cyber-physical consequences, and the resilience measures proposed in response. Findings were supported through comparison across peer-reviewed studies, government publications and industry evidence rather than relying on individual sources. This iterative synthesis provided the analytical basis for consolidating the recurring relationships into the five stages of the Integrated Cyber Risk Pathway Model.

The final stage of the review involved integrating these recurring relationships into a single conceptual representation. Instead of creating another taxonomy of technologies or threats, the aim was to develop a broader understanding of how digital transformation is changing the nature of cyber risk in interconnected CII and ICS environments. This process resulted

in the development of the Integrated Cyber Risk Pathway Model, which connects technology adoption, vulnerability creation, threat actor exploitation, cyber-physical impacts, and resilience requirements.

III. The Evolving Cyber Threat Landscape

A. From Attacks on Individual Systems to Exploiting Ecosystems

The cyber threat landscape for CII and ICS has evolved significantly over the last fifteen years. Earlier attacks mainly targeted specific industrial processes by exploiting vulnerabilities in proprietary control systems. But with time, the nature and scope of these attacks have changed. Cyber threat actors are now targeting the entire digital ecosystem around critical infrastructure, including software supply chains, cloud platforms, Internet-facing devices, and third-party service providers. This is due to the convergence of IT and OT, where vulnerabilities outside traditional industrial environments can affect physical assets through ICS [2][4]. Several key incidents illustrate how these threats have evolved. For example, the 2010 Stuxnet attack [14] was a milestone in industrial cybersecurity, demonstrating that malicious programs could be tailored to affect physical equipment in ICS environments. Subsequent attacks, such as Industroyer [15], Triton [16], and attacks on the Ukrainian power grid [17], revealed that sophisticated adversaries with an understanding of industrial protocols and engineering processes could effectively target OT systems [2],[16]. These incidents indicated that cyber-attacks could cause physical disruption, not just affect digital assets.

From around 2020 onwards, this evolution entered a new phase. Rather than directly attacking industrial systems, threat actors increasingly exploited vulnerabilities in the wider digital ecosystem that supports critical infrastructure operations. The SolarWinds [4] compromise exemplifies this shift by demonstrating how a single software supply chain attack could simultaneously provide access to thousands of organisations, including operators of critical infrastructure. Likewise, ransomware campaigns such as EKANS [18] and BlackCat [19], together with attacks targeting Internet-facing operational assets, demonstrate that adversaries no longer require detailed knowledge of ICS environments to disrupt critical services. Instead, they exploit trusted software, cloud services, remote access solutions and poorly secured IT infrastructure as entry points into operational environments [4][18].

This evolution reflects an important change in attacker strategy. Earlier attacks were mainly focused on compromising individual industrial assets through direct manipulation of operational technologies, whereas contemporary attacks tend to exploit the interconnected relationships between organisations, software platforms and supply chains. With the acceleration of digital transformation, cybersecurity of CII can no longer be viewed in isolation from an individual organisation. Instead, the resilience of critical infrastructure is increasingly dependent on the security of the wider digital ecosystem in which it is embedded.

Table II provides a summary of major cyber incidents between January 2010 and June 2026, illustrating the evolution of cyber threats affecting CII and ICS. The table does not list isolated events, but instead highlights the transition from highly specialised attacks on ICS to broader ecosystem compromises that exploit shared digital platforms, interconnected technologies, and third-party dependencies.

TABLE II. Major Cyber Incidents Illustrating the Evolution of the CII/ICS Threat Landscape (2010–2026)

Year	Threat Name	Targeted Sector	Type of Attack	Impact
2010	Stuxnet [14]	Nuclear, energy	ICS Malware	Physical damage to centrifuges
2016	Industroyer [15]	Energy	ICS Malware	Electricity disruption
2016	Mirai [20]	Telecom	IIOT DDOS	Domain Name System (DNS) disrupted
2017	Triton/Trisis/Hatman [16]	Energy – Oil, gas	ICS Malware	Safety Instrumented Systems (SIS) compromised
2020	SolarWinds [4]	Energy, Utilities, Telecom	Supply chain Malware	Over 18,000 organisations affected
2021	Colonial Pipeline [21]	Energy – Oil	Ransomware	Fuel disruption across 17 states
2022	Sandworm /Industroyer 2 [17]	Energy – electrical	Malware	Power outages and supply disruptions across several areas in Ukraine.
2022	KillNet [22]	Health, energy, defense	DDOS malware	Disruptions to health, energy, and defense sectors across NATO countries
2023	Cyber Av3ngers [23]	Water	Intrusion and malware attack	Aliquippa water authority booster station disabled via default credentials.
2024	Blackcat/ALPHV [19]	Health	Intrusion attack and ransomware	Healthcare services were disrupted
2024	Salt Typhoon [24]	Telecom	APT	Major U.S and global telecom operators compromised.
2025	Electrum [25]	Energy – Power grid	Ransomware	Distributed renewable energy sites and combined heat and power (CHP) plants across Poland compromised.
2025	BlackSuit (Royal) [26]	Manufacturing, Health, Utilities	Malware	Telecontrol and protection functions disrupted
2025	Scattered Spider and HellCat [27]	Manufacturing	Ransomware	Shutting down of global IT infrastructure at Jaguar Land Rover
2026	Itron [28]	Energy, Water	Supply chain Malware	The attack allowed cyber threat actors to gain access to the networks of CII operators.

B. Emerging Vulnerabilities in Digitally Connected CII

The growing adoption of emerging technologies has introduced new categories of vulnerability that differ from those traditionally associated with isolated ICS. Rather than existing independently, these vulnerabilities reinforce one another, creating multiple pathways through which attackers can move from digital systems into operational environments. Five recurring vulnerability categories were identified through the literature review.

1) Growing attack surfaces from connected devices: The rapid adoption of IIoT devices, edge computing platforms and 5G-enabled sensors has led to an exponential increase in the number of connected assets in CII. While these technologies help to improve operational visibility and provide real-time monitoring, many devices still use default credentials, run obsolete firmware, or have limited security features. As a result, each new connected device becomes a potential attack vector. Large botnets such as Mirai [20] and Flax Typhoon [29] have shown how insecure connected devices can be used to attack critical infrastructure without directly targeting ICS [30][31].

2) Risks to data integrity in intelligent systems: As AI and digital twins increasingly enable operational monitoring, predictive maintenance and decision-making within CII, they pose new challenges for data integrity. Unlike traditional cyber-attacks, which aim to disrupt a system's availability, AI-enabled environments are often targeted for data integrity compromises. Techniques such as data poisoning can manipulate the information used to train or operate AI models, reducing their ability to detect malicious activity or leading operators to make incorrect decisions [32]. As organisations become more dependent on intelligent systems, maintaining trustworthy data becomes as important as protecting the systems themselves.

3) Cloud and supply chain dependencies: Cloud computing has become a vital component of digital transformation, allowing organisations to better manage geographically distributed infrastructure. However, greater reliance on cloud platforms and third-party software also creates new dependencies that extend beyond organisational boundaries. Misconfigurations, excessive privileges and software supply chain compromises have become common attack vectors, as demonstrated by the SolarWinds incident and numerous cloud security breaches [33][34]. These dependencies indicate that the security of critical infrastructure increasingly relies on organisations outside the operator's direct control.

4) Weak IT-OT segmentation: Historically, OT systems were physically separated from enterprise IT systems. Today, however, increasing integration between these environments allows cyber incidents originating in IT networks to affect physical operations. According to the OT Cyber Threat Report 2025, by Waterfalls Security Solutions [36], most recent cyber incidents resulting in physical consequences have originated from compromised IT environments rather than direct attacks on industrial control systems. Strengthening IT–OT segmentation therefore remains one of the most effective measures for reducing cyber-physical risk.

5) Preparing for the post-quantum era: Although practical quantum attacks have not yet materialised, the transition towards quantum computing presents a long-term cybersecurity challenge for CII. Current cryptographic algorithms used to secure communications may eventually become vulnerable, enabling adversaries to exploit a "harvest now, decrypt later" strategy. Consequently, planning for post-quantum cryptography should be viewed as a present resilience priority rather than a distant technical concern [37][38].

Although these vulnerability categories are discussed separately, they rarely occur in isolation. Connected devices increase the number of possible entry points, cloud platforms create external dependencies, AI systems rely on trusted data, and IT-OT convergence enables attacks to propagate beyond operational boundaries. These vulnerabilities combine to create a growing, interconnected risk environment in which weaknesses in one component can increase risks in others. Understanding these relationships is key to investigating how emerging technologies collectively are transforming cybersecurity in CII and ICS, as discussed in the next section.

IV. Emerging Technologies and Cyber Risk Dynamics

The adoption of emerging technologies is significantly changing the operational makeup of CII and ICS environments in ways that are more than just increasing efficiency. While these technologies enable automation, real-time monitoring and data-driven decision-making, they also change the nature of cyber risk by introducing new dependencies, expanding connectivity and increasing the complexity of digital ecosystems. They do not necessarily introduce new threats, but rather alter how existing threats emerge, propagate, and impact critical infrastructure. This review has identified three broad technological shifts that collectively revolutionise the cybersecurity environment: increased connectivity, the proliferation of operational intelligence, and long-term uncertainty surrounding cryptography.

A. Connectivity Technologies: Expanding the Attack Surface

The first transformation is enabled by technologies that improve connectivity between operational environments. IIoT, 5G, and edge computing allow industrial assets, sensors, controllers and enterprise systems to be continuously connected with each other. These technologies enable better operational visibility, predictive maintenance and decentralised decision-making, which are all the hallmarks of Industry 4.0 initiatives [5][39].

But more connectivity also means a larger attack surface for cyber intrusion. With each connected sensor, gateway, or edge device, there is an increased attack surface available to adversaries. Unlike traditional industrial environments that were largely isolated from external networks, modern CII increasingly relies on distributed devices that often operate outside secure network boundaries.

Many of these devices have limited computational resources, infrequent software updates and inconsistent security controls, making them attractive targets for attackers.

The expanding deployment of wireless communication and virtualised network services further complicates security. For example, vulnerabilities in 5G network slicing or edge nodes may allow attackers to move laterally across interconnected environments and impact multiple operational systems. Therefore, the cybersecurity challenge is no longer limited to protecting individual devices but extends to securing a highly connected digital ecosystem.

B. Intelligent Technologies: Shifting the Focus from Availability to Trust

The second transformation is driven by technologies that increasingly support operational decision-making. AI, digital twins and cloud computing enable operators to process large volumes of operational data, optimise industrial processes and detect anomalies more efficiently than traditional approaches [7]. These technologies also introduce a different category of cyber risk. Traditionally, cybersecurity in industrial environments focused primarily on maintaining system availability and protecting systems from unauthorised access. As organisations become more dependent on these technologies, the integrity and reliability of data become equally important. If attackers manipulate sensor readings, poison AI training data, or compromise digital models, operational decisions may become unreliable even when the underlying systems continue to function normally [6].

Cloud computing reinforces this challenge by creating additional dependencies on external service providers. Cloud platforms improve scalability and operational flexibility. However, they also centralise critical services and increase the dependency on third-party software, making supply chain security one of the major components of cyber resilience [41][42]. These technologies, together, are transforming cybersecurity by not only protecting system availability, but also ensuring the trustworthiness of operational data, algorithms and digital services.

C. Quantum Computing: a Future Threat with Present-Day Implications

Unlike the technologies discussed above, quantum computing is not yet impacting day-to-day industrial operations. Its significance lies in its capacity to compromise the cryptographic foundations that protect digital communications in CII and ICS environments. Current public-key cryptographic algorithms, including Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), are expected to become vulnerable to sufficiently powerful quantum computers [38].

Although practical quantum attacks remain some years away, adversaries may already be collecting encrypted information for future decryption using a “harvest now, decrypt later” strategy [37][38]. Given that many industrial systems remain operational for decades, preparing for post-quantum cryptography has become a strategic resilience issue rather than simply a future technical challenge.

D. A Common Pattern Across Emerging Technologies

While the seven technologies examined in this review differ in purpose and maturity, they exhibit a common pattern. Each technology provides significant operational benefits, but also introduces new types of cyber exposure. Connectivity technologies expand the attack surface, intelligent technologies increase dependence on trusted data and digital services, while quantum computing challenges the long-term security of existing cryptographic mechanisms. These technologies therefore do not create isolated cybersecurity problems. Rather, they collectively reshape how cyber risks emerge and propagate across interconnected CII and ICS environments.

V. Cyber-Physical Impacts of Emerging Technologies on CII and ICS

A. Operational and Economic Impacts

The increasing digitalisation of CII and ICS has significantly increased the operational and financial consequences of cyber incidents. Unlike traditional enterprise IT environments, disruptions to critical infrastructure can interrupt essential services such as electricity generation, water treatment, healthcare delivery and transportation. Even when OT systems is not directly compromised, attacks on supporting IT systems can force operators to suspend critical processes as a precautionary measure, leading to substantial operational disruption.

The Colonial Pipeline [21] ransomware incident demonstrated that a cyberattack targeting enterprise IT systems could trigger the shutdown of operational infrastructure because of concerns over the safe management of pipeline operations. Similarly, attacks against manufacturing facilities, healthcare organisations and utility providers have resulted in prolonged service interruptions, delayed production and significant financial losses.

The 2025 OT Cyber Threat Report [36] states that multiple cyber incidents per year have quantifiable physical operational impacts, with some cases resulting in losses of several million to hundreds of millions of dollars. Another study found that nearly half of the critical infrastructure organisations surveyed had experienced cyber-physical incidents resulting in financial losses exceeding US$500,000, indicating that economic impacts of cyberattacks are beyond system recovery costs [47]. Furthermore, studies of major incidents such as NotPetya [49] demonstrate that indirect supply chain disruption often exceeds the direct cost of the original attack, thereby increasing economic losses across interconnected organisations [50].

These examples indicate that cyber incidents impacting CII are no longer limited to technical failures. Rather, they increasingly disrupt operational continuity, interrupt essential services and cause economic consequences that propagate across interdependent supply chains.

B. Physical, Safety and Societal Impacts

A significant characteristic of cyber incidents affecting CII and ICS is their ability to produce physical consequences.

Incidents targeting industrial environments may affect equipment, industrial processes and public safety, as compared to cyber-attacks against traditional IT systems. Consequently, cybersecurity within critical infrastructure is closely linked to operational resilience and the protection of human life.

Historical incidents illustrate this distinction clearly. Stuxnet demonstrated that malware could manipulate industrial equipment to cause physical damage, while Triton specifically targeted Safety Instrumented Systems (SIS), highlighting that cyber-attacks can deliberately compromise mechanisms designed to protect people and industrial facilities. More recently, attacks on water treatment facilities and energy operators have demonstrated that relatively simple vulnerabilities, such as exposed remote access services or default credentials, may create opportunities for attackers to interfere with critical processes [16][23].

The societal impact of these events extends beyond the organisations concerned. Interruptions to electricity, healthcare, telecommunications or water supply can rapidly affect businesses, government services and the daily lives of citizens. Furthermore, the increasing involvement of nation-state actors in targeting critical infrastructure introduces geopolitical dimensions that encompass cybersecurity beyond organisational risk management and into national security and economic stability [51].

C. Cascading and Systemic Impacts

Perhaps the most significant consequence of digital transformation is the increasing potential for cyber incidents to cascade across interconnected infrastructures. Modern CII sectors are no longer isolated systems but form part of a wider ecosystem connected through shared communication networks, cloud platforms, software suppliers and operational dependencies. Consequently, a disruption affecting one organisation or sector may trigger secondary effects across multiple critical services.

Research on interconnected critical infrastructure consistently demonstrates that cyber incidents can produce cascading failures, in which disruption spreads through technical, organisational, and supply-chain dependencies rather than remaining confined to the original target [40]. For example, failures within the electricity sector may affect telecommunications, transportation, healthcare and financial services, while compromises of widely used software platforms or cloud service providers can simultaneously expose thousands of organisations, as demonstrated during the SolarWinds incident.

These systemic effects challenge many traditional cybersecurity approaches, which primarily focus on protecting individual organisations. As digital transformation deepens inter-sectoral interconnections, cyber resilience must increasingly consider the wider ecosystem in which critical infrastructure operates. Protecting one organisation is no longer sufficient if vulnerabilities in trusted suppliers, cloud providers, or interconnected services can cause widespread disruption.

VI. An Integrated Pathway Model for Understanding Cyber Risk Transformation in CII and ICS

The literature reviewed in this study reveals a consistent pattern beyond individual technologies or isolated cyber incidents. While emerging technologies, cyber threats, vulnerabilities, and resilience have been examined independently in previous studies, little attention has been paid to how these elements interact to reshape cyber risks in CII and ICS. Bringing these relationships together reveals that digital transformation does not simply introduce new technologies; it changes the pathways through which cyber risks emerge, propagate and ultimately affect critical services.

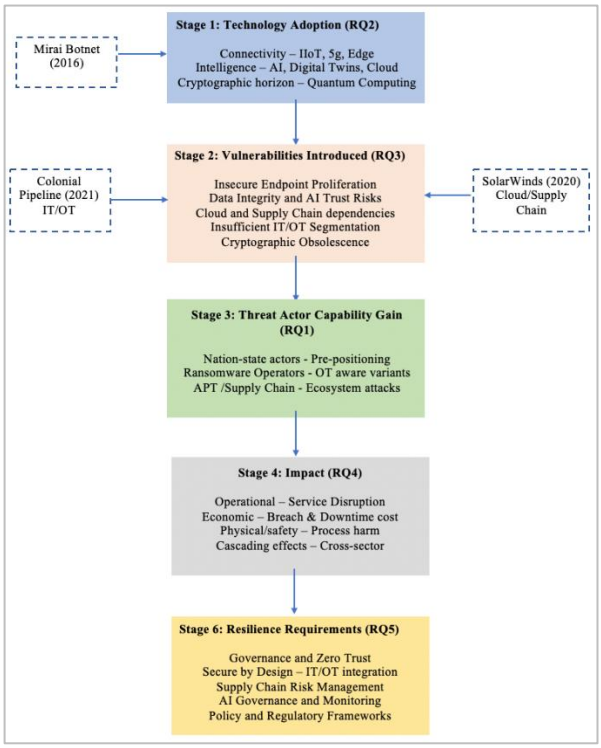

Fig. 2. Integrated cyber risk pathway model illustrating the relationship between the different stages.

Fig. 2 presents an Integrated Cyber Risk Pathway Model that synthesises these relationships. The model illustrates cyber risk as a progressive process that begins with technology adoption, creates new forms of exposure, expands opportunities for cyber threat actors and results in operational, physical and societal consequences. These consequences, in turn, redefine the resilience capabilities required to protect modern critical infrastructure.

A. Stage 1: Technology Adoption

The pathway starts with the growing adoption of Industry 4.0 technologies. These technologies are being deployed to improve operational efficiency, enable predictive maintenance, improve situational awareness and allow for more autonomous industrial processes [1][3].

All technologies provide significant operational benefits, but the combined adoption fundamentally alters the architecture of CII and ICS. Industrial environments are becoming increasingly connected, data-driven, and dependent on external digital services. As a result, the nature of cybersecurity challenges has evolved from securing individual systems to managing risks in an interconnected digital ecosystem.

B. Stage 2: Vulnerability Creation

Digital transformation inevitably introduces new forms of exposure. The literature reviewed in this study identified five recurring vulnerability categories: expanding attack surfaces, data integrity risks, cloud and third-party dependencies, weak IT–OT segmentation and emerging cryptographic challenges. Importantly, these vulnerabilities should not be viewed as independent security issues. They reinforce one another. For example, IIoT devices increase the number of internet-connected assets, cloud computing introduces external dependencies, AI systems rely on trustworthy data, while IT–OT convergence creates pathways through which attacks originating in enterprise networks can affect physical operations. Together, these vulnerabilities create a highly interconnected risk environment in which weaknesses in one domain can amplify risks elsewhere [32][36].

C. Stage 3:Threat Actor Exploitation

These vulnerabilities provide cyber threat actors with new opportunities to compromise critical infrastructure. The review shows that attacker behaviour has evolved alongside digital transformation. Earlier attacks generally required specialist knowledge of industrial processes and proprietary control systems. More recent attacks increasingly exploit software supply chains, cloud services, internet-facing assets and trusted third-party relationships to gain access to operational environments [4][18].

Consequently, the capabilities of threat actors are no longer determined solely by their understanding of industrial systems. Increasingly, attackers exploit weaknesses created by digital integration, allowing them to compromise critical infrastructure without directly attacking industrial technologies themselves. This explains the growing prevalence of ransomware, supply chain compromises and attacks targeting interconnected digital services.

D. Stage 4: Cyber-Physical Impacts

When vulnerabilities are successfully exploited, the consequences surpass the loss of information. Unlike traditional enterprise environments, cyber incidents affecting CII and ICS can disrupt physical processes, interfere with the delivery of essential services and cause cascading effects across interconnected sectors.

The review identified four general types of impacts: operational disruption, economic loss, physical and safety consequences, and systemic or cascading failures. These impacts are closely related. For example, a compromise of an enterprise IT network may disrupt industrial operations, leading to financial losses, interruption of public services, and wider societal consequences. As digital interdependencies increase, the likelihood that failures will propagate across multiple sectors also increases [40][36].

E. Stage 5: Resilience Requirements

The final stage of the pathway recognises that preventing every cyber-attack is unrealistic. Instead, resilience therefore involves the ability to anticipate, withstand, respond to and recover from cyber incidents while maintaining essential services.

The literature consistently highlights governance, secure-by-design principles, IT-OT integration, supply chain security, continuous monitoring and cross-sector collaboration as key resilience capabilities. Importantly, these capabilities address different stages of the pathway rather than functioning as isolated security controls. Resilience should be viewed as a system-wide capability that reflects the interconnected nature of modern CII and ICS.

VII. Discussion

A. Advancing an Integrated Perspective of Cyber Risk

The findings of this review suggest that the cybersecurity of CII and ICS can no longer be understood by examining individual technologies or isolated cyber incidents. While previous studies have made important contributions by investigating the security implications of AI, IIoT, cloud computing, digital twins, 5G and other emerging technologies, they have generally addressed these technologies separately. In practice, however, CII operators are adopting several of these technologies simultaneously, creating an increasingly interconnected digital ecosystem in which vulnerabilities, threats and impacts are closely related [6][43]. The Integrated Cyber Risk Pathway Model developed in this study brings these relationships together into a single conceptual framework. Instead of viewing cyber-attacks as isolated technical events, the model demonstrates how digital transformation progressively reshapes cyber risk. The adoption of emerging technologies creates new forms of exposure; these vulnerabilities provide opportunities for cyber threat actors, successful attacks produce cyber-physical and societal impacts, and those impacts redefine the resilience capabilities required to protect essential services. This perspective is consistent with studies showing that cyber incidents increasingly propagate across interconnected infrastructures rather than remaining confined to individual organisations [40].

The model also reinforces a broader shift in cybersecurity research. Traditional approaches have largely focused on preventing unauthorised access and protecting individual assets. While these objectives remain important, they are no longer sufficient for digitally connected critical infrastructure. Modern CII environments operate as complex socio-technical systems in which cloud platforms, software supply chains, operational technologies and external service providers are tightly interconnected. As a result, resilience depends not only on protecting individual components but also on understanding how disruptions propagate across the wider ecosystem. This systemic perspective aligns with the growing body of cyber resilience literature, which argues that resilience should be viewed as an organisational and system-level capability rather than simply a collection of technical security controls [43][44].

B. Implications for Research and Practice

This review has implications for both researchers and practitioners. From a research perspective, the Integrated Cyber Risk Pathway Model provides a conceptual foundation for future empirical studies examining the relationships between technology adoption, emerging vulnerabilities and cyber resilience. Most existing studies investigate these topics independently, making it difficult to explain how digital transformation influences the overall cybersecurity posture of CII and ICS. The proposed model offers a structured framework that can be validated using longitudinal cyber incident data, sector-specific case studies, or quantitative resilience assessments.

From a practical perspective, the model encourages organisations to move beyond technology-specific security measures towards a more integrated understanding of cyber risk. Decisions relating to AI adoption, cloud migration, IIoT deployment or IT–OT integration should not be evaluated independently. This is because each decision can influence vulnerabilities in other parts of the digital ecosystem. Consequently, resilience planning should incorporate governance, secure system design, supply chain risk management and cross-sector collaboration as complementary rather than independent activities.

Although the pathway model is intended to provide a cross-sector perspective, its individual stages should be interpreted in the context of the sector in which it is applied. CII sectors differ in their operational environments, technology dependencies, threat exposure and potential consequences of disruption. For example, energy infrastructure may focus on availability and integrity of operational technologies and prevention of cascading disruptions. Healthcare settings must consider continuity of clinical services, protection of sensitive information and the increasing reliance on interconnected medical systems. Water infrastructure might be especially vulnerable to risks of remote-access control systems, legacy operational technologies and physical process manipulation. Therefore, the route from technology adoption to vulnerability, exploitation, impact and resilience applies across CII sectors, but the importance of individual vulnerabilities, threat scenarios and resilience measures may vary according to sector-specific characteristics. The model should therefore be viewed as a common analytical structure that can be adapted to the operational and risk context of individual CII sectors.

The model also has relevance for policymakers and regulators. As governments continue to promote digital transformation across critical sectors, cybersecurity policies should increasingly recognise the interconnected nature of modern infrastructure. Regulatory initiatives such as the NIS2 Directive [45], the Critical Entities Resilience Directive (CER) [46] and the Cyber Resilience Act (CRA) [48] represent significant progress by promoting stronger governance and supply chain security. However, the findings of this review suggest that future policy development should place greater emphasis on systemic risk, cross-sector dependencies and coordinated resilience planning.

C. Limitations of the Study

This Study Has Certain Limitations that Should Be Acknowledged. First, the Findings Are Based on a Multivocal Literature Review, Which Combines Peer-reviewed Research with Grey Literature. Although This Approach Is Well Suited to Cybersecurity Research Because Many Emerging Threats Are First Reported by Government Agencies and Industry Organisations, the Quality and Level of Evidence Across Sources Are Not Always Consistent [8].

Second, the Integrated Cyber Risk Pathway Model is a conceptual framework derived from evidence synthesis and has not yet been empirically validated. While the relationships represented in the model are supported by the literature reviewed, future research should examine whether these relationships are consistently observable in real-world CII and ICS environments. One approach would be to analyse documented cyber incidents and map the available evidence against the five stages of the model: technology adoption, vulnerability creation, threat actor exploitation, cyber-physical impacts and resilience requirements. Sector-specific case studies in areas such as energy, healthcare and water could then be used to examine whether the nature and strength of these relationships vary across different operational environments. As the evidence base develops, quantitative indicators could also be defined for individual stages of the pathway to support more systematic assessment of the relationships between technology adoption, cyber exposure, incident impacts and resilience outcomes. These approaches would provide a basis for progressively testing and refining the proposed model.

Third, the review examines seven emerging technologies. Other developments that may have cybersecurity implications for CII and ICS, such as blockchain, distributed ledger technologies and autonomous industrial systems, are not examined. As the integration of these technologies into critical infrastructure evolves, they should be considered in future extensions of the review.

Finally, the study adopts a cross-sector perspective and therefore does not provide a detailed comparative analysis of individual CII sectors. Differences in operational environments, technology dependencies, threat exposure and resilience priorities across sectors such as energy, healthcare, water, telecommunications and manufacturing may influence how individual stages of the proposed pathway manifest in practice. Future sector-specific studies could therefore apply and validate the model within individual CII domains to determine how these relationships vary across operational contexts. Despite these limitations, the study provides an integrated perspective on how emerging technologies collectively reshape cyber risk and resilience within critical infrastructure, while providing a foundation for future empirical and theoretical research.

VIII. Conclusion

The rise of emerging technologies is transforming the cybersecurity landscape of CII and ICS in ways that go beyond the introduction of new technologies or attack vectors. The fast pace of digital transformation is resulting in increasingly complex cybersecurity challenges, with vulnerabilities emerging not only from individual systems but also from

interactions among technologies, organisational processes, and digital dependencies. This shift calls for a broader understanding of cyber risk, considering the complexity of modern critical infrastructure.

This study addresses this challenge by synthesising evidence from academic research, government publications and industry threat intelligence to examine how emerging technologies collectively influence cybersecurity in CII and ICS. Instead of analysing technologies, vulnerabilities, threat actors and resilience as separate topics, the study combined these perspectives into an Integrated Cyber Risk Pathway Model that explains how cyber risk develops from technology adoption through to cyber-physical impacts and resilience needs. By bringing these relationships together, the framework provides a comprehensive view that complements existing technology-specific and threat-specific research.

Results also indicate that securing critical infrastructure requires a shift from siloed security measures to resilience strategies that recognise the interconnected nature of today's digital ecosystem. As organisations increasingly integrate AI, cloud computing, IIoT, edge computing and other Industry 4.0 technologies into operational environments, cybersecurity cannot be addressed solely through technical controls. Effective protection increasingly depends on governance, secure system design, supply chain assurance and collaboration across organisations and sectors. Building resilience, therefore, requires understanding not only where vulnerabilities exist but also how they interact and propagate across interconnected systems.

However, the present study has some limitations. The Integrated Cyber Risk Pathway Model presented is a synthesis of existing evidence and has not been empirically tested. In addition, the review adopts a cross-sector perspective and focuses on seven emerging technologies. Sector-specific differences and other technological developments are not examined in detail.

Future research should therefore focus on the empirical validation and further refinement of the proposed model. Documented cyber incidents could be mapped against its five stages to examine whether the relationships identified through the literature are consistently observable in practice. Sector-specific case studies across areas such as energy, healthcare and water could further determine how vulnerability profiles, threat actor behaviour, cyber-physical impacts and resilience priorities vary across different operational environments. Future extensions of the review could also consider other emerging developments, including blockchain and distributed ledger technologies and increasingly autonomous industrial systems. Also, as the model matures, quantitative indicators may be developed for its individual stages to support a more systematic assessment of cyber risk transformation and resilience in CII and ICS environments.

The Integrated Cyber Risk Pathway Model provides a basis for understanding how cyber risk is changing in critical infrastructure through technological transformation and increasing interconnectedness. The model connects the adoption of technology, vulnerabilities, exploitation by threat actors, cyber-physical consequences, and resilience needs. It provides a foundation for future empirical research and offers practitioners and policymakers a systematic perspective to ponder cybersecurity risks within the framework of ongoing digital transformation.

IX. Declaration of Generative AI

The authors declare that Generative AI was not used for the preparation and writing of this research study.

References

[1] Asghar, M.R., Hu, Q. and Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. Computer Networks, [online] 165, p.106946. doi:https://doi.org/10.1016/j.comnet.2019.106946.

[2] Hemsley, K. and Fisher, R. (2018). A History of Cyber Incidents and Threats Involving Industrial Control Systems. Critical Infrastructure Protection XII, pp.215–242. doi:https://doi.org/10.1007/978-3-030-04537-1_12.

[3] Katsikas, S., Frédéric Cuppens, Cuppens, N., Costas Lambrinoudakis, Christos Kalloniatis, Mylopoulos, J., Antón, A., Stefanos Gritzalis, Meng, W. and Furnell, S. (2020). Computer Security. Springer.

[4] CISA (2021). Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organisations | CISA. [online] Cybersecurity and Infrastructure Security Agency CISA. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a.

[5] Axon, L., Fletcher, K., Stolz, M., Kaafarani, A.E. and Creese, S. (2022). Emerging Cybersecurity Capability Gaps in the Industrial Internet of Things: Overview and Research Agenda IIoT Capability Gaps. Digital Threats: Research and Practice, 3(4). doi:https://doi.org/10.1145/3503920

[6] Raval, K.J., Jadav, N.K., Rathod, T., Tanwar, S., Vimal, V. and Yamsani, N. (2024). A survey on safeguarding critical infrastructures: Attacks, AI security, and future directions. International Journal of Critical Infrastructure Protection, [online] 44, p.100647. doi:https://doi.org/10.1016/j.ijcip.2023.100647.

[7] Abraham, D., Erceylan, G., Gkioulos, V. and Houmb, S.H. (2025). Towards enhanced cybersecurity in industrial control systems: a systematic review of context-based modeling, digital twins, and machine learning approaches. International Journal of Information Security, 24(6). doi:https://doi.org/10.1007/s10207-025-01158-1.

[8] Garousi, V., Felderer, M. and Mäntylä, M.V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Information and Software Technology, 106, pp.101–121. doi:https://doi.org/10.1016/j.infsof.2018.09.006.

[9] Cybersecurity & Infrastructure Security Agency (2020). CISA. [online] Cisa.gov. Available at: https://www.cisa.gov/.

[10] NIST (2025). National Institute of Standards and Technology. [online] NIST. Available at: https://www.nist.gov/.

[11] Enisa (2016). ENISA. [online] Europa.eu. Available at: https://www.enisa.europa.eu/.

[12] isa.org. (n.d.). International Society of Automation. [online] Available at: https://www.isa.org/.

[13] WEF (2023). The World Economic Forum. [online] World Economic Forum. Available at: https://www.weforum.org/.

[14] Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security & Privacy Magazine, 9(3), pp.49–51. doi:https://doi.org/10.1109/msp.2011.67.

[15] Cherepanov, A. and Lipovsky, R. (2017). Industroyer: Biggest threat to industrial control systems since Stuxnet. [online] WeLiveSecurity. Available at: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/.

[16] Pinto, A., Dragoni, Y. and Carcano, A. (2018). TRITON: The First ICS Cyber Attack on Safety Instrument Systems Understanding the Malware, Its Communications and Its OT Payload. [online] Available at: https://i.blackhat.com/us-18/Wed-August-8/us-18-Carcano-TRITON-How-It-Disrupted-Safety-Systems-And-Changed-The-Threat-Landscape-Of-Industrial-Control-Systems-Forever-wp.pdf.

[17] ESET Research (2022). Industroyer2: Industroyer reloaded. [online] WeLiveSecurity. Available at: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.

[18] Hunter, B. (2020). EKANS Ransomware: A Malware Targeting OT ICS Systems | FortiGuard Labs. [online] Fortinet Blog. Available at: https://www.fortinet.com/blog/threat-research/ekans-ransomware-targeting-ot-ics-systems.

[19] FBI, CISA, and HHS (2024) #StopRansomware: ALPHV Blackcat. [online]. Available at: https://www.hhs.gov/sites/default/files/aa23-353a-stopransomware-alphv-blackcat-update.pdf.

[20] CISA (2016). Heightened DDoS Threat Posed by Mirai and Other Botnets | CISA. [online] www.cisa.gov. Available at: https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets.

[21] Easterly, J. and Fanning, T. (2023). The attack on Colonial Pipeline: What we've learned & what we've done over the past two years. [online] Cybersecurity and Infrastructure Security Agency. Available at: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

[22] HC3 Analyst Note Level II Level III Level IV Non-Trauma Unknown Number of HPH Organizations by Trauma Level Allegedly Targeted by KillNet DDoS Attack on 28JAN2023 (n=91). (2023). Available at: https://www.hhs.gov/sites/default/files/202304051200-killnet-analyst-note-tlpwhite.pdf.

[23] IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities. (2023). [online] Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Environmental Protection Agency (EPA), and the Israel National Cyber Directorate (INCD). Available at: https://www.cisa.gov/sites/default/files/2023-12/aa23-335a-irgc-affiliated-cyber-actors-exploit-plcs-in-multiple-sectors-1.pdf.

[24] CISA (2024). Enhanced Visibility and Hardening Guidance for Communications Infrastructure | CISA. [online] Cybersecurity and Infrastructure Security Agency CISA. Available at: https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure.

[25] https://www.dragos.com/danielle-gauthier (2026). Poland Power Grid Attack Targets Distributed Energy Facilities. [online] Dragos.com. Available at: https://www.dragos.com/blog/poland-power-grid-attack-electrum-targets-distributed-energy-2025.

[26] #StopRansomware: BlackSuit (Royal) Ransomware. (2023). [online] *https://www.cisa.gov*. Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA). Available at: https://www.cisa.gov/sites/default/files/2024-08/aa23-061a-stopransomware-blacksuit-royal-ransomware_4.pdf.

[27] CYFIRMA. (2025). Investigation Report on Jaguar Land Rover Cyberattack - CYFIRMA. [online] Available at: https://www.cyfirma.com/research/investigation-report-on-jaguar-land-rover-cyberattack/.

[28] Sec.gov. (2026). 8-K. [online] Available at: https://www.sec.gov/Archives/edgar/data/780571/000119312526175249/d125229d8k.htm [Accessed 30 Jun. 2026].

[29] Frank J. Cilluffo (2020). Code Red: A Guide to Understanding China's Sophisticated Typhoon Cyber Campaigns. [online] McCrary Institute for Cyber and Critical Infrastructure Security, Auburn University. Available at: https://mccraryinstitute.com/app/uploads/2025/10/McCrary-Institue-Code-Red-Release-Ready.pdf.

[30] Asimily. (2026). The Top Internet of Things (IoT) Cybersecurity Breaches in 2026. [online] Availab2le at: https://asimily.com/blog/the-top-internet-of-things-iot-cybersecurity-breaches-in-2026/.

[31] 5G Cybersecurity. (2023). [online] National Cybersecurity Center of Excellence (NCCoE), National Institute of Standards and Technology. Available at: https://www.nccoe.nist.gov/sites/default/files/2023-01/5g-cybersecurity-fact-sheet.pdf.

[32] Kravchik, M., Biggio, B. and Shabtai, A. (2021). Poisoning attacks on cyber attack detectors for industrial control systems. Proceedings of the 36th Annual ACM Symposium on Applied Computing. doi:https://doi.org/10.1145/3412841.3441892.

[33] Gokkaya, B., Aniello, L. and Halak, B. (2025). Software supply chain: A taxonomy of attacks, mitigations and risk assessment strategies. Journal of Information Security and Applications, [online] 97, p.104324. doi:https://doi.org/10.1016/j.jisa.2025.104324.

[34] Sharma, S. (2025). Cloud Misconfiguration: The #1 Cause of Data Breaches 2025 | Fidelis Security. [online] Fidelis Security. Available at: https://fidelissecurity.com/threatgeek/threat-detection-response/cloud-misconfigurations-causing-data-breaches/.

[35] ENISA (2021). Understanding the increase in Supply Chain Security Attacks. [online] ENISA. Available at: https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks.

[36] Team, W. (2025). 2025 OT Cyber Threat Report – OT attacks with physical consequences. [online] Waterfall Security Solutions. Available at: https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/2025-threat-report-ot-cyberattacks-with-physical-consequences/

[37] www.dhs.gov. (n.d.). Preparing for Post-Quantum Cryptography: Infographic | Homeland Security. [online] Available at: https://www.dhs.gov/publication/preparing-post-quantum-cryptography-infographic.

[38] NIST (2024). NIST Releases First 3 Finalized Post-Quantum Encryption Standards | NIST. [online] NIST. Available at: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[39] Obasuyi, T. (2023). Edge Computing, 5G, and Cloud Security Convergence: Strengthening USA's Critical Infrastructure Resilience. International Journal of Computer Applications Technology and Research (IJCATR), [online] 12(9), pp.17–31. Available at: https://ijcat.com/archieve/volume12/issue9/ijcatr12091003 [Accessed 3 Feb. 2026].

[40] Palleti, V.R., Adepu, S., Mishra, V.K. and Mathur, A. (2021). Cascading effects of cyber-attacks on interconnected critical infrastructure. Cybersecurity, [online] 4(1). doi:https://doi.org/10.1186/s42400-021-00071-z.

[41] Erukude, S.T., Marella, V.C. and Veluru, S.R. (2026). AI-Driven Cybersecurity Threats: A Survey of Emerging Risks and Defensive Strategies. Lecture Notes in Networks and Systems, pp.185–197. doi:https://doi.org/10.1007/978-3-032-10783-1_14.

[42] Center for Security and Emerging Technology. (2024). Securing Critical Infrastructure in the Age of AI | Center for Security and Emerging Technology. [online] Available at: https://cset.georgetown.edu/publication/securing-critical-infrastructure-in-the-age-of-ai/.

[43] Järveläinen, J., Dang, D., Mekkanen, M. and Tero Vartiainen (2025). Towards a framework for improving cyber security resilience of critical infrastructure against cyber threats: a dynamic capabilities approach. Journal of Decision Systems, 34(1). doi:https://doi.org/10.1080/12460125.2025.2479546.

[44] Kott, A. and Linkov, I., eds. (2019). Cyber Resilience of Systems and Networks. Cham: Springer International Publishing. doi:https://doi.org/10.1007/978-3-319-77492-3.

[45] European Commission (2023). Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) | Shaping Europe's digital future. [online] digital-strategy.ec.europa.eu. Available at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

[46] European Commission - European Commission. (2026). Enhancing EU resilience: A step forward to identify critical entities for key sectors. [online] Available at: https://ec.europa.eu/commission/presscorner/detail/it/ip_23_3992.

[47] Claroty. (2024). The Global State of CPS Security 2024: Business Impact of Disruptions. [online] Available at: https://claroty.com/resources/reports/the-global-state-of-cps-security-2024-business-impact-of-disruptions.

[48] European Commission. "EU Cyber Resilience Act | Shaping Europe's Digital Future."*Digital-Strategy. Ec.Europa.Eu*, 10 Dec. 2024, Available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

[49] EuRepoC: European Repository of Cyber Incidents. (n.d.). Major Cyber Incident: NotPetya. [online] Available at: https://eurepoc.eu/publication/major-cyber-incident-notpetya/.

[50] Belen (2025). A Review of the Economic Costs of Cyber Incidents. [online] World Bank. Available at: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099092324164536687

[51] DNI (2024). 2024 annual threat assessment of the US intelligence community. [online] Available at: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf [Accessed 7 Jan. 2026].