World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Cybersecurity of critical infrastructures: Challenges and future perspectives

Tendai Nemure [1,*], Munashe Naphtali Mupa [2], Kelvin Gyimah Agyei [3], Hilton Hatitye Chisora [1], Ken Mudzingwa [1] and Rodney Chiwanga [1]

[1] *Yeshiva University*
[2] *Hult International Business School*
[3] *University of Memphis*
Tendai Nemure, ORCiD: 0009-0009-0303-3864
Munashe Naphtali Mupa, ORCiD: 0000-0003-3509-867X
Kelvin Gyimah Agyei, ORCiD: 0009-0002-6728-9825
Hilton Hatitye Chisora, ORCiD: 0009-0006-5927-4577
Ken Mudzingwa, ORCiD: 0009-0005-1090-6492
Rodney Chiwanga, ORCiD: 0009-0000-2484-883X

World Journal of Advanced Research and Reviews, 2026, 29(03), 870-883

Publication history: Received on 04 February 2026; revised on 10 March 2026; accepted on 13 March 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.29.3.0621

Abstract

Critical infrastructures (CIs) ranging from energy, finance, telecom, healthcare, water, and transport infrastructures form the basis of societal stability and economic consistency for various countries. These CIs themselves are progressing at an unprecedented pace into these new paradigm shifts of cloud computing and virtualization technologies, and Internet of Things (IoT) integration and 5G networks; simultaneously experiencing an ever-expanding set of more complex threats to their cybersecurity. The paper would examine these new trends and outlooks related to critical infrastructure security with knowledge gained from research studies offered by Maglaras et al. (2022) related to this topic and with novel perspectives introduced hereinafter. These trends and outlooks would cover IT/OT integration, vulnerabilities found within traditional infrastructural systems with age factors, unshared visibility with distributed systems infrastructure, and threats posed to these infrastructures with ever-growing supply chains, among others.

Cloud computing, Edge intelligence, artificial intelligence, blockchain, or 5G/6G technologies represent new areas of promising security and exciting areas of potential risks. By providing an overview of case studies reported in recent years related to the energy sector, financial industry, telecommunication industry, and healthcare sector, this paper draws attention to real-life consequences of CI compromise and risks associated with interdependent infrastructure systems. Recommendations provided at the end of this study could focus on developing technical specifications at national or International Governments to adapt and overcome these risks related to critical infrastructure security. It's an interdisciplinary and international challenge to ensure essential infrastructure security.

Keywords: Critical; Cybersecurity; Infrastructure; Perspectives

1. Introduction

Critical infrastructures (CIs) may be defined as systems and infrastructure that support activities of the society to operate, be economically stable, and maintain national security. Such systems involve power grid system, world financial systems, telecommunication infrastructure, transport infrastructure, healthcare infrastructure and so forth that is responsive to the well-being of the society. An example is where these infrastructures were originally made up of isolated systems that were operated manually. On the other hand, due to the fast development of digitalization and

* Corresponding author: Tendai Nemure

interconnectivity technologies such as cloud computing, Internet of Things (IoT), or 5G network communication systems, these infrastructures have been converted into highly interconnected cyber infrastructural systems, which have efficiency and scalability advantages, but which introduce crucial risks related to cyber threats (Lehto, 2022).

There has been a paradigm shift in the nature of the threats that may impact the critical infrastructures in respect of complexity and magnitude. The historical cyber events comprised opportunistic or simple malware with minimal maliciousness. The current cyber threats have progressively employed advanced modalities with insidious tenacity and vast understanding of the ICS operational conditions. The actual impact of CI breaches by cyber-attacks is evident in the high-profile attacks such as those experienced in the ransomware attack of Colonial Pipeline in 2021 which resulted in fuel shortages along the East Coast of America, or in widespread cyber-attacks of power infrastructure in the power grid infrastructure of Ukraine. Not only do these scenarios comment on the vulnerabilities associated with interconnection systems, but can illustrate the effect of the cascades and their implications far beyond what was covered by the compromised infrastructure in the first place.

In particular, in the current case, the article by Maglaras et al. (2022) can provide valuable information about the current research on CI and cybersecurity threats. The discussed paper is a well-organized review of the issues of secure infrastructures with a focus on rapid technological progress that has a direct impact on the managerial activity associated with security. As an example, the current risks and vulnerabilities linked to attack patterns and potential threats provided in the context of this study provide meaningful insights that would be required to design an initial knowledge base in regard to threats presented by cyber risks currently. Above all, research topics demanding specific focus, in particular, infrastructures based on cloud computing infrastructure and 5G/6G technologies, provide the necessary insights required to reach certain goals pertaining to infrastructural security threats residing within the context of the presented analysis of this paper. This paper is intended to take advantage of past research findings that are provided in the analysis of the study on CI and related cyber threats by Maglaras et al. (2022).

2. Overview of Critical Infrastructure Cybersecurity

2.1. Overview of Critical Infrastructure Cybersecurity

Critical Infrastructures (CIs) can be described as basic infrastructure systems that cover essential sectors such as power infrastructure systems, transport systems, water infrastructure systems, telecommunication systems, and healthcare infrastructure systems, among others. Cybersecurity of Critical Infrastructures becomes essential for preserving national security and public safety with growing dependence on computers and other technologies (Jiang et al, 2024). Over the years, there has been a rapid evolution in CI security measures because of advances in computer and communications technologies.

2.1.1. Traditional Security Approaches: Isolation and Obscurity

In the past, ensuring the cybersecurity of critical infrastructure was achieved mainly through physical isolation and managed connectivity. The main idea behind these industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems was to run such systems under secure and isolated networks with air-gapped systems as their primary defense strategy. This defense relied on what was referred to as security through obscurity because these systems relied on technologies and communication protocols not well understood or known outside technical circles.

Air-gapping was an effective means of securing these systems to some degree but it was not foolproof as well. Over time, it became more evident how prone to threats air-gapped systems were, as the impossibility to integrate new technologies, as well as the ease with which they could be remotely controlled, would place them in this networked age as being in the past (Roshanaei, 2021). These industrial systems were increasingly dependent on digital technologies, as well; therefore, there was a necessity of better cybersecurity.

2.1.2. The Shift to Digitalization and Connectivity

Critical infrastructures have extensively evolved over the last few years due to the technological innovations. Critical infrastructure systems have had cloud computing, Internet of Things (IoT) devices and artificial intelligence (AI) integrated into them. At the centre of these developments has been migrating to the cloud due to the fact that a good number of critical infrastructure service providers have been embracing a hybrid cloud system that integrates various infrastructure systems with a combination of the private or public cloud as a way of expanding its computing capacity and control over the dispersed data systems.

In contrast, more modern technologies such as IIoT have transformed businesses such as the energy industry, transport, and production plants. The processes that can be achieved through IIoT can be easily acquired due to the real-time tracking and decision-making that can be achieved. Examples of such innovative approaches can be innovative grid systems that are linked with the energy sector, autonomous transport systems, or artificial intelligence-based telecommunication networks. The implication of such technologies is that CI systems are becoming complicated and have more points of vulnerability to cybercriminal assaults.

Integration of operational technology (OT) systems with traditional IT systems has lowered the difference that existed between the two spheres of activity in the previous past. The wave of virtualization, containerization, and orchestration Systems such as Kubernetes has added more complexity into the security of such modernized environments. The fact that edge computing platforms can process data near the point of its initial creation adds further complexity in terms of decentralized methods of decision making.

2.1.3. Evolving Cybersecurity Frameworks and Standards

Due to the growing interdependence of critical infrastructures and digital systems, the focus has been on the creation of suitable cybersecurity. There are various regulations and policies that are related to assisting CIs with adequate measures of cybersecurity.

As an example, there is the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), which can be used to apply to the cybersecurity on a holistic, dynamic basis. Speaking of which, the North American Electric Reliability Corporation has a set of guidelines that are associated with the critical infrastructure protection (NERC CIP) concerning the condition of cybersecurity of electric grids and the steps required to protect bulk electric power infrastructure against the threat of cyber-attacks.

In the international business community, whilst the ISO 27001 is the standard that determines the best information security management system (ISMS) and the NIS2 Directive by European Union encourages more resilient cybersecurity measures to critical businesses such as the energy, transport and medical industries, these two provide insight into how important yet challenging these two domains can actually be. Maglaras et al. claimed that the gaps in alignment of policy, enforcement coexistence and the flexibility of regulatory systems to adopt swiftly changing technologies can present overwhelming challenges. The necessity to address such issues is even more urgent when such factors as cloud security risks and the increasing 5G/Edge computing technologies are taken into account.

2.1.4. Emerging Cybersecurity Threats and Challenges

As the process of digitalization takes place in the critical infrastructure, the threat situation has changed; hence, new cybersecurity threats come with the appearance of new technologies. The main threat of such technologies might be that they are vulnerable to cyber attacks as more and more CI systems become interconnected. Despite the abundance of advantages of cloud computing and IIoT devices to several industries, they have vulnerabilities that can be exploited by cyber attackers.

Cloud infrastructure risks can be very high and pose a great risk to the security of CI systems in case unauthorized access to important data takes place or inappropriate cloud infrastructure settings. The additional risk can be added by including other third-party cloud service providers, as they should be adequately addressed, taking these dependencies, as well. Cyber threats like weak authentication or compromised communication channels may also create a point of entry because of threats pertaining to IIoT devices, as well.

Supply chain risks: Supply chain risks are also other pertinent risk factors. The supply chains worldwide today have become complex involving third-party suppliers. These third parties may have multiple attack points, or the cyberattacks can have a starting point at the third party suppliers or vendors whose risks to the critical infrastructure can be taken into consideration; therefore, the risk management practices between the vendors must be realized.

3. Threat Landscape and Vulnerabilities in Critical Infrastructures (

3.1. Adversaries Targeting Critical Infrastructures

The threat environment of the critical infrastructures (CIS) is highly diverse and multidimensional, and various malicious actors use these systems with various purposes to support their goal. These bad actors lie between the very sophisticated attackers of the state level and the criminals and between the attackers and the cybercriminals that have

varying plans of attack and intent regarding ugly attacks upon critical infrastructure systems with disruptive or destructive intent (Järvelainen et al, 2025).

3.1.1. Nation-State Actors:

Rivalry inside the nation-state has the potential to become a danger at an accelerating capacity and agency due to geopolitical interests like spying, interference, or disruption of service. The entities of nation-states would tend to be equipped with advanced tools and familiarize themselves with the industry systems. They might choose the industries that are associated with the national security interests such as energy, telecommunications or defense systems.

3.1.2. Cybercriminal Groups:

These cybercrime gangs operate with the main drive of making monetary gain and using different techniques to target critical infrastructure systems. Ransomware attacks, extortion, and stealing sensitive data are among the methods primarily used by these gangs with the aim of affecting infrastructural services, with the goal of demanding a ransom or using sensitive information for money gain.

3.1.3. Insider Threats:

Threats of insiders are of the malicious, compromised, and careless employees and may be a significant threat to critical infrastructure organizations. The insiders may be very dangerous since they may easily circumvent the traditional security systems since they have an authorization to access sensitive systems or other valuable assets.

3.1.4. Hacktivists and Ideologically Motivated Actors:

Other ideologically-oriented groups such as hacktivists might attack CIs with an aim of achieving an ideological agenda. Such attacks are not complex comparative to ones whose goal is to disrupt a country or a criminal group; however, they can be devastating due to their tendency to target critical infrastructure to drive a point or get noticed by people.

3.2. Evolving Capabilities of Threat Actors

The abilities of malicious entities targeting critical infrastructure systems have improved beyond recognition over the years. In particular, with more advanced malware available to malicious entities, they now get to benefit from attack kits and tools of exploitation that were previously only at the expertise level of more skilled attackers.

3.3. Common Attack Vectors in Critical Infrastructure

There exist many types of attack vectors that can target critical infrastructure; these can target either IT or OT systems or even a combination of these two types of systems. There exist human factors among these types of attack vectors.

3.3.1. Phishing and Social Engineering:

Phishing attacks can still rank among the top initial access vectors used in critical infrastructure environments. Attackers commonly resort to using social engineering techniques with the aim of tricking specific employees into disclosing particular types of information or installing malicious software.

3.3.2. Supply Chain Attacks:

There has been an increase in supply chain attacks whereby the attackers target software or hardware suppliers to compromise the organization's trust in these suppliers and gain access to systems indirectly.

3.3.3. Cloud and Virtualized Environments:

Cloud systems and virtualization infrastructures can face problems like misconfiguration in terms of unsecured APIs or relaxed access controls. A malicious actor could use these vulnerabilities to pivot from the cloud into more valuable systems on the infrastructure.

3.3.4. Zero-Day Vulnerabilities in ICS

OT Systems and Industrial Control Systems (ICS) are the most common victims of zero-day attacks since most industrial devices will have outdated firmware or software that cannot be fixed or updated with ease. Such vulnerabilities may act as entry points or access points to systems by attackers or other evil-minded forces.

3.3.5. Ransomware Attacks:

The ransomware attacks on critical facilities have been on the rise and particularly in healthcare facilities, logistics infrastructure and other facilities like power. As a rule, such attacks include financial motives, and the attackers will require some money to restore access.

3.4. Sector-Specific Vulnerabilities in Critical Infrastructure

Critical infrastructure consists of sectors that present dissimilar varieties of risks depending upon their technologies and operations. Such risks may be connected with the technologies or regulations within the field, and so on.

3.4.1. Energy Sector:

All these allow stating that the energy industry has been moving towards autonomous system control and remote access systems that may develop vulnerabilities in control systems. The IoT communications of insecure devices are enormous because the trend of smart meters and Distributed Energy Resources (DERs) has introduced myriads of devices.

3.4.2. Financial Sector:

The growing use of cloud-based transaction processing systems and online banking systems has presented an exposure to weaknesses related to the abuse of APIs, credential theft, and the hacking of payment systems. It may lead to the loss of major economies, in addition to the violation of security and interruption with services.

3.4.3. Telecommunications Sector:

There are threats of telecommunication infrastructure that are specific to 5G implementation and virtualization. Network slicing may have weaknesses, software-defined networking (SDN), as well as protocols like SS7 and Diameter, which may give malicious actors loopholes to exploit or interfere with telecommunicating networks.

3.4.4. Transportation and Smart Cities:

The transportation networks and smart city infrastructure, which highly depends on the technologies of IoT sensors and networks of control units connected with one another, can be easily attacked when it comes to CAN bus networks or autonomous vehicles. Attackers can get easily involved in these networks due to the connections they make as a result of interconnectedness.

3.4.5. Healthcare Sector:

Healthcare sector may encounter the requirements connected with the outdated healthcare devices, the deficiency of network separation, and the expansion of remote patient monitoring devices. These issues may result in numerous risks and turn healthcare infrastructures into the object of interest of cybercriminals who want to obtain or interfere with healthcare information and services.

3.5. The Threat of Advanced Persistent Threats (APTs)

Advanced Persistent Threats (APTs) are among the significant threats that are strategic to the critical infrastructure since these actors are connected to stealthy and persistent activities that may reside within the target systems without being detected in significant durations of time.

3.5.1. Tactics, Techniques, and Procedures

There are many complicated strategies, Techniques, and Procedures that APTs usually use to penetrate and gain presence in networks. The methods used include spear-phishing attacks to privilege escalation to even bespoke malware that can bypass the standard security measures.

3.5.2. Targeted Sectors:

The APTs focus on various critical infrastructure industries such as power grid systems, water facilities and telecommunication infrastructure. These operations have been able to disrupt physical operations, undermine functions, and costly damage crucial infrastructure systems.

3.5.3. Needs - Detection and Response:

Due to the nature of APTs, monitoring, detection capabilities and response systems are critical in securing critical infrastructure. The necessity of APT activity detection and response capabilities allows making sure that the threat of such well-trained threats can be reduced significantly.

4. Key Challenges Identified by Maglaras et al. (2022)

There exist significant challenges related to the protection and resilience of essential infrastructures (CIs) that are discussed in an article by Maglaras et al. (2022). These challenges can be viewed from multiple angles, depending on technological or human factors, or other system dependencies related to these infrastructures. Below are these significant challenges divided into various points:

4.1. Interdependence of Critical Infrastructure Sectors

Interconnected or interdependent critical infrastructures pose a significant challenge to their management. It can be noted that different infrastructural areas such as energy services, telecommunication infrastructure, transport infrastructure, and healthcare infrastructure are interlinked with each other and form complicated networks whereby an unavailability or disruption in one particular infrastructure can cause consequences or linkages with other infrastructural networks and areas like telecommunication services; hence, if there were cyber attacks on the power infrastructure targeting telecommunication networks supporting finances, logistics, and healthcare emergencies directly related to those networks could occur.

4.2. Convergence of Information Technology (IT) and Operational Technology (OT)

The other urgent issue arising when considering the protection of critical infrastructure relates to the integration of IT and OT systems. While IT systems were conceptualized with emphasis on management and security related to data and networks, respectively, OT systems were designed with a focus on real-time operational control and associated safety factors. These two systems were traditionally separated for strategic purposes related to safety and security concerns. The increased necessity to combine the IoT-based devices and cloud computing with the ICS necessitates a more global approach to the protection of these systems, where the IT and OT systems are not looked at as distinct entities, but the areas of overlap concerning the protection of the infrastructure. The focus on management and security of networks of the IT systems may interfere with the OT systems due to the ability of IT-based security services, such as encrypting and firewalling, to hamper the efficiency of operational systems.

4.3. Legacy Systems and Their Vulnerabilities

Another major threat to CI security is the use of old legacy systems. The current technologies, such as programmable logic controller (PLC) and industrial sensor devices were invented several decades ago and no one has considered security at that time when cyberattacks did not exist or were only in their early phases. These systems are also many years old with various communications protocols that are not supported and updated with new technologies as CI security systems need updates to remain secure, and cannot be connected with security systems due to lack of computational power to execute various security tools. These systems can easily fall prey to cyberattacks to access CIs because of their weaknesses and lack updated security protocols to stay secure.

4.4. Cybersecurity Workforce Shortage

The lack of qualified information security experts has been an enduring problem that has heightened weaknesses in critical infrastructure systems. In ensuring ICS and OT system security, specialized knowledge not only in security but also related to these technologies and processes under which the systems operate is necessary. The lack of such expertise makes it difficult for companies to fill positions in their security departments adequately. The problem of lack of knowledge among IT security professionals has been heightened by growing system complexity that requires specialized knowledge to handle and protect it. There will be an ever-growing gap between the needed expertise and those who offer these services, with the increasing automation of critical infrastructure systems.

4.5. Limited Visibility and Monitoring Capabilities

While critical infrastructure systems become more dispersed with multi-cloud systems, Edge computing devices, or IoT-based systems, managing visibility throughout the system becomes more challenging to achieve. Difficulties posed by dispersed infrastructure systems and devices/technologies used could cause challenges when aggregating data needed to monitor every aspect of critical infrastructure systems. It could lead to situations where cyberattacks occur undetected for extended periods of time before identification because these systems can create gaps where cyberattacks

can occur without monitoring, while hiding behind dispersed systems like multi-cloud systems or Edge computing devices. These problems would be mitigated by enhancement of monitoring systems and integration with security systems to a greater extent.

4.6. Supply Chain and Data Governance Risks

One more threat that has emerged due to the globalisation of hardware and software supply chains concerns the protection of critical infrastructure. Third-party suppliers, to which essential systems of infrastructure are often administratively related or trusted, provide possible attack points. These suppliers might be attacked by attackers to add vulnerabilities or malicious code to the supply chain leading to compromised infrastructure systems. Moreover, increasingly significant numbers of critical infrastructure systems are producing large volumes of sensitive data, which are stored in cloud environments; the associated issues are those associated with data governance. Sufficient data protection measures are required to avert unauthorized access cases and corresponding data security measures of the critical infrastructure system.

5. Emerging Technologies in CI Security

As the reliance on digital technologies as one of the most critical infrastructures (CIs) grows, the cybersecurity environment is changing fast. The capabilities of critical infrastructure systems and the risks of such systems are increasingly being shaped by new technologies such as cloud computing, edge computing, 5G/6G networks, artificial intelligence (AI), machine learning (ML), blockchain, and zero trust architecture (ZTA). On the one hand, these technologies offer opportunities to become more efficient and more resilient to risks, on the other hand, they are also risky and should be dealt with appropriately. These technologies are now going to be described.

5.1. Cloud and Edge Computing in CI Security

5.1.1. Cloud Computing: Opportunities and Risks

Cloud computing is now a crucial component of the contemporary CI systems since it assists in utilizing scalable resources in a very reliable manner to process, store, and analyze the data. Scaling of large volumes of business data under real-time analysis as well as the ability to remotely manage resources enhances efficiency in the fields of the energy industry, transport industry, and utility industry when utilizing CI systems.

Although the increased use of cloud services comes with numerous security risks associated with cloud computing, the multi-tenant aspect of cloud computing tends to create innumerable risks that could lead to threats within these systems. Some of these risks connected with cloud computing consist of unauthorised access to infrastructure environments that contain vital data that could pose different threats.

5.1.2. Edge Computing: Reducing Latency, Increasing Risk

Edge computing can hence be utilized with cloud computing to offer real-time processing and decision-making closer to where the action or event is taking place i.e. at the edge or near the network and near machines or sensor devices on the factory floor or other facilities. Industries like manufacturing, health and autopilot cars may need edge computing urgently.

Conversely, there is the growing amount of devices at the edge of the network which may be in exposed or uncontrolled surroundings that may present a security risk. These devices may either not have proper security measures or even fall to bodily attacks as they do not have strict security measures to protect these devices against being exploited by either the cybercriminals or the malicious states.

5.2. Telecommunications Infrastructures: 5G and 6G Networks

5.2.1. 5G Networks: A Double-Edged Sword for Security

The deployment of 5G networks brings forth new risks and possibilities with regard to CI security. 5G networks make extensive use of virtualization techniques, network slicing, and software-defined networks (SDNs). These tools not only lead to more flexible and efficient infrastructure but also create new threats like signaling attacks, problems with slice isolation, and those posed by virtualized network functionalities (VNFs).

The decentralized architecture of 5G networks raises the number of points at which attackers could gain access, making it necessary to implement individual security measures. In particular, ultra-low latency on 5G networks ensures real-

time control of distant or autonomous systems like smart grids and intelligent transport networks. Although this capability benefits critical infrastructure services like smart grids and intelligent transport networks, it raises risks of threats like cyberattacks against those systems that were meant to offer protection.

5.2.2. 6G: The Future of Secure Communication

Future Developments The advent of 6G will result in more novel developments as far as connectivity is concerned with the introduction of features like AI-native networking, quantum secure communications, and ultra-reliable low-latency communications (URLLC). These may reshape CI systems and introduce entire new categories of applications, including autonomous manufacturing and real-time monitoring of critical infrastructure systems.

However, as the degree of progression relating to 6G communications is also posed, come new security threats, including that which pertains to the ability of quantum computing to effectively de-crypt most current types of cryptography. It will then turn out to be supreme to make sure communications networks are compatible enough to endure the advancement as they approach CI systems security at 6G communications.

5.3. Artificial Intelligence and Machine Learning in CI Security

5.3.1. AI/ML for Anomaly Detection and Predictive Security

The use of AI and machine learning is transforming the use of CI-based cybersecurity through more active and independent measures toward securing computer infrastructure. AI-based anomaly systems can analyze the high amount of telemetry data to identify subtle changes in system activity that may initiate a possible security threat.

Machine learning algorithms can be used to forecast equipment breakdowns, spot internal threats, and automatically react to security incidents with faster response times for remedying emerging security threats.

5.3.2. Adversarial Machine Learning: New Risks

Although there are advantages brought about by AI/ML systems, these systems also offer risks with vulnerabilities associated with artificial intelligence and machine learning that did not previously exist or were more difficult to access before these systems were introduced. Adversaries using adversarial machine learning to mislead machine learning models and/or training datasets with malicious purposes can result in risks associated with the creation or misuse of false positives or even threats associated with infrastructure systems related to these AI/ML systems.

5.4. Blockchain for Infrastructure Security

The potential benefits of blockchain to secure CI could therefore arise from the distributed ledger system that blockchain offers. For instance, blockchain can benefit smart grids to record transactions while ensuring that these transactions cannot be forged and that they can be viewed openly. These applications have benefits provided that blockchain can actually provide these functionalities effectively and satisfactorily.

Despite such advantages, though, there are also factors that may slow the implementation of blockchain with CI systems. These are issues such as scalability with blockchain technologies, consuming a lot of power with blockchain systems, and incompatibility issues between various blockchain systems. Addressing these issues will assist in accessing the complete advantages of blockchain in ensuring the security of critical infrastructure systems.

5.5. Zero Trust Architecture (ZTA) in CI Security

5.5.1. The Shift from Perimeter-Based to Zero Trust Security

Zero Trust Architecture (ZTA) represents an unprecedented change of mindset among the companies regarding the issue of security threats and protection. In the example, whereas standard security models rely upon trusting devices and individuals within a network or systems outside the network yet within trust zones that form part of the network architecture, Zero Trust Architecture does not trust anyone or anything both within and outside the network architecture or systems.

Zero Trust Architecture can substantially reduce the risks of lateral movement in a network environment in critical infrastructure situations and reduce the extent to which an attack can be caused before it can spiral out of control. Deployment of Zero Trust Architecture However in OT infrastructures where the devices are sensitive to time or systems with strict time responses or issues, deployment of Zero Trust Architecture must be done with cautious consideration not to disrupt critical processes within the mission.

6. Future Perspectives and Research Directions

The landscape of Critical Infrastructures (CIs) cybersecurity is rapidly growing with advancements in technologies and increased intelligence of cyber threats. For the future, CIs' cybersecurity would need more focus on resilience-based design methodologies with advanced threat intelligence and specific security models for new technologies such as cloud computing, 5G networks, and AI-based systems. The following sections will discuss important areas of research and development related to CIs' cybersecurity.

6.1. Resilience-Driven Design Principles

"In moving CI cybersecurity into the future," an important area of focus will be found under the development of more resilient infrastructures that can safely operate under the assumption that they will inevitably be compromised." Writing in 2022, Maglaras et al., explain that "cybersecurity system design with resilience objectives in mind becomes more important." Resilient system designs will offer "continuity of service while under attack." They must "incorporate concepts such as redundancy or automatic fail-over functionalities and self-healing." A promising method for achieving more resilient systems will be found using "digital twins," or virtual copies of real systems that can model "cyber physical system interactions." These digital models can "help forecast consequences of cyber incidents allowing system defenders to make proactive efforts to maximize defense plans."

6.2. Improving Threat Intelligence Sharing

With growing global and more complex threats against CIs, there is a need to enhance the sharing of threat intelligence among governments, industries, and other global entities. There are challenges associated with sharing threat intelligence due to concerns related to privacy and legal constraints, among others, that limit the efficient sharing of threat intelligence for timely reaction to threats. There is a need for research to overcome these hurdles and find ways to share threat intelligence while preserving privacy. AI analysis of threats can aid in processing large amounts of threat intelligence for rapid identification of threats.

6.3. Security Frameworks for Cloud and Edge Computing

There is an increasing need for secure computing frameworks for cloud and edge computing scenarios set up in CI environments. It should emphasize research related to devising cloud security controls for multi-cloud environment management and virtualization of industrial networks at the edges. These security controls would require addressing specific challenges of cloud infrastructure related to joint responsibility models set up at the cloud infrastructure level to ensure that particular security specifications were explicitly established at the cloud setup level. Additionally, techniques related to the analysis of firmware integrity, container secure environment setup, or management of secure cloud-based distributed network flows would significantly determine secure cloud system evolution at computing edges.

6.4. Securing Next-Generation Telecommunications Infrastructure

With the increasing momentum of 5G and 6G networks rolling out, securing sixth-generation telecommunication networks would soon become an essential topic of study and research. Future research would need to focus on techniques that would help enhance slice isolation on sixth-generation networks so that multiple virtual networks running on the same infrastructure can stay protected from other virtual networks that share the infrastructure with them. Securing O-RAN (Open Radio Access Networks) would also become important because O-RANs offer greater versatility to networks, but at the cost of threats to these networks because of their openness and versatility. Also, with sixth-generation computing taking over, classical cryptography would soon face threats related to computing power; hence, quantum cryptography would become necessary for secure communications.

6.5. Integrating Cyber and Physical Security

Cyber and physical security integration is set to become more important with more applications of cyber-physical systems (CPS) taking place in critical areas like power production and consumption, transport networks, and healthcare systems. There will always need to be comprehensive risk management models taking into account consequences related to CPS incidents that can affect systems either virtually or in real life. There will need to be more emphasis on research and development associated with CPS simulation tools and response mechanisms when incidents occur that can increase preparedness and response abilities related to these systems.

6.6. Human Factors and Organizational Dynamics

Human factors pose considerable challenges to CI cybersecurity efforts. Workers can either represent the weakest link in the security system or be part of the strongest defense system. It is essential to conduct research studies related to improving security culture and designing efficient training programs to minimize human factors leading to security incidents associated with CI systems (Volk, 2024). There should also be research studies conducted related to improving human/workers' collaboration with machines or computer systems to increase efficiency at defense systems associated with CI cybersecurity. It can be expected that more intelligent infrastructures will demand improved human oversight systems to stay safe and secure against cyber threats.

6.7. . Addressing the Cybersecurity Workforce Shortage

The lack of skilled cybersecurity personnel globally can be considered a significant impediment to improving CI cybersecurity. To bridge this human resource gap, future research should instead focus on tools and systems with the ability to supplement human expertise. Decision-support systems that can offer real-time guidance and recommendations for response can significantly boost the efficiency of performing these cybersecurity operations. Additionally, artificial intelligence and machine learning can be applied to automate mundane operations and allow human cybersecurity experts to concentrate on more complex problems that require human expertise (Malatji et al, 2022). Increased access to education and training programs for more workers to gain expertise can greatly benefit future preparedness to deal with cybersecurity threats.

7. Case Studies and Real-World Examples

The absence of expert cybersecurity workers can be regarded as one of the factors that significantly hinder efforts to enhance CI cybersecurity systems. To remedy this human resource challenge, future studies should focus on tools or systems with capacities to complement human expertise. Decision-support systems with real-time guiding abilities can significantly enhance efficiency when carrying out these processes associated with supporting computer infrastructure security systems (Yigit et al, 2024). Additionally, artificial intelligence and machine learning can be used to automate basic processes so that human cybersecurity experts can focus on solving complex problems that need human expertise. More education and training programs can significantly aid future preparedness to confront threats associated with computer infrastructure security systems.

7.1. The 2015 Ukraine Power Grid Attack

The issue of a lack of human resources can be viewed among those factors that significantly affect efforts geared at enhancing CI cybersecurity systems. In addressing human resource challenges associated with these systems, future research studies should focus on systems with capabilities that can complement human knowledge or expertise. Decision-support systems with real-time guidance capabilities can significantly boost efficiency when implementing these processes required to facilitate computer infrastructure security systems. On top of that, artificial intelligence systems can provide solutions to automatically execute basic processes so that human computer infrastructure security experts can focus on addressing problems requiring human knowledge or expertise (Aghazadeh Ardebili et al, 2024). More efforts related to education and training programs can significantly help with preparedness for future challenges associated with computer infrastructure security systems.

The cyber attack caused a city-wide blackout that left hundreds of thousands of residents without power for several hours. The attack demonstrated the weaknesses found in IT/OT integration and showed problems such as unsegmented networks and remote access tools to be of particular concern. It was also evident how these types of cyber attacks can cause disruptions to primary services with indirect effects on operations in critical infrastructure environments. The attack remained active despite solving the initial problem of access to the infrastructure environment.

7.2. Telecommunications Attacks on 5G Infrastructure

Telecommunication networks were exposed to cyber threats not only because of the increase in malicious cyber attackers, but also due to the evolution of 5G networks. The major case that was reported involved virtual network function attacks related to 5G signaling and traffic control management functionalities (Toledano, 2024). Cyber threats were associated with loopholes inherent in orchestration layers, virtual machines with incorrect configurations, and insecure APIs; these posed threats to telecommunication services. Cyber threats were not only associated with telecommunication protocols like SS7/Diameter but also with features of 5G networks.

7.3. Cloud-Related Breach in the Financial Sector

The growing dependence of the financial industry on cloud infrastructure has brought with it novel risks, especially those related to APIs, third-party systems, and distributed transaction systems. It's telling that a significant breach took place when a prominent fintech company's sensitive customer information was compromised because of an improper setup of their cloud-based storage solution. Hackers were able to target this vulnerability to gain access to customers' personally identifiable information.

This particular case brought into focus the need for robust access management and audit abilities not only when using the cloud but also when using third-party cloud services for carrying out valuable operations like money transfers (Baseri et al, 2024). It was found that due to an improper configuration of a workload on the cloud service, there was unbridled access to vast amounts of data, resulting in penalties and loss of public trust.

7.4. Ransomware Attack on Healthcare Systems

Healthcare infrastructure has been increasingly attacked given the importance of its service offerings and tendency to rely on networks of medical equipment. A significant example of this was when a hospital's IT infrastructure was attacked using ransomware; hackers were able to encrypt the IT infrastructure, such as patients' records and medical equipment (Riggs et al, 2023). The effect was that surgeries were delayed and patients had to be referred elsewhere because medical services were not available.

It exposed how unsegmented or inadequately protected access to IT and operational technologies can result in life-threatening consequences when medical equipment becomes antiquated or when there is a lack of backup and disaster recovery capabilities in healthcare delivery institutions (Dawson et al, 2021). For that reason, healthcare delivery institutions with an urgent need for access to essential data or system access qualify to be primary ransomware targets because these entities can afford to pay ransoms with the urgent need to restart access to critical systems or services.

8. Recommendations

8.1. Adopting Zero Trust Security Principles

An essential technical recommendation for CI cybersecurity is implementing a so-called zero trust (ZT) model of security on a wide scale. Zero trust implies that internal and external networks are under constant attack and hence need rigorous authentication checks on every individual and every network access attempt. Some basic criteria of such models consist of least privilege access and monitoring processes.

For operational technology (OT) environments, micro-segmentation can help reduce lateral movement risks within networks or confine breach impact. By implementing granulated access management for critical assets with micro-segmentation techniques, breaching incidents can be restricted before they can cause damage to more sensitive areas of infrastructure (Lewis, 2006). Other than this, CI service providers can ensure their cloud infrastructures adhere to secure-by-default principles of access control audits, encrypting sensitive workloads on clouds, and securely managing APIs to reduce risks due to their possible weaknesses.

8.2. Strengthening Regulatory Frameworks and International Cooperation

At the policy level, it is evident that sufficient regulatory framework and tools are needed, which would make CI entities comply sufficiently with regulations regarding the Cybersecurity Standards to reduce risks. Optimal underpinning level of Cybersecurity measures would be realized through improvement of best practices like the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), ISO 27001 and industry sector standards like the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP).

The NIS2 Directive of the EU provides a blueprint of the modernization of the regulations based on the aspects of mandatory reporting of the incidents, enhanced risk analysis, and supply chain priorities. It should also be internally collaborative to facilitate information sharing and collaborate to respond in the event of international cyber threats. International security requirements might be developed to ensure that certain emerging technologies such as cloud computing, edge computing, and 5G networks remain on their toes and have sufficient security systems that are in accordance with the advancements against threats.

8.3. Investing in Workforce Development and Operational Readiness

The most serious concern involving CI and cybersecurity systems is associated with the absence of skills among IT employees in the field of industrial control systems (ICS) or other OT systems. This loophole needs to be found and sealed to ensure efficient security of infrastructure systems. Until the present, training and educational interdisciplinary knowledge that would give the workers experience in handling the constantly increasing cyber threats can bridge this gap.

In addition, authorities must conduct routine operations like red teaming exercises, penetration testing, and tabletop exercises to determine the effectiveness of security measures and incident-related response operations. Such exercises can also easily spot weak points in the defense infrastructure and level of preparedness of entities in a manner that it is possible to take actions before an attack can happen. Besides that, the processes in managing vendor risk should be enhanced with comprehensive research of third-party suppliers and focus on security provisions in the contracts that are regulatory compliant.

8.4. Enhancing Visibility and Monitoring Across Hybrid Environments

With the increasing complexity in terms of the hybrid infrastructure systems, this calls on enhancement, as to the visibility and monitoring of such systems. The implementation of centralized monitoring systems that have the ability to gather logs and telemetry data, and alerts related to various environments including cloud, edges, IoT devices, and OT systems, is needed. These monitoring systems may be of great benefit in case they are connected with analytics tools based on artificial intelligence.

Besides this, backup and disaster recovery related measures should be enhanced such that continuity of services can be guaranteed in case of ransomware or system crash. These systems must be better off being isolated and not vulnerable to cyber threats such that in case of an attack by ransomware or failure of the system, it can be prevented. Restoration of the system is possible at a greater rate.

8.5. Fostering Proactive Resilience and Continuous Adaptation

The struggle to achieve security of critical infrastructures requires the proactive nature that not only focuses on security, but much more. It involves active initiatives of CI facilities to concentrate on core activities involved in the establishment of resilience that facilitate the infrastructural systems to continue functioning despite incidences of breach of security.

Threats continuously change and in this case all organizations need to embrace a dynamic model in respect to cyber threats as they can continuously enhance their preparations to cyber threats with the assistance of new intelligence or new technologies that may create vulnerabilities.

9. Conclusion

The infrastructures of critical infrastructures are the backbone of the contemporary modern world and support or otherwise foundations to important services such as power grid infrastructure, financial systems, healthcare infrastructure, telecommunication systems, and transport infrastructure. As these industries revolutionize at a dizzying pace using new technologies such as cloud computing, Internet of Things gadgets, and well-developed connectivity networks, they are put at an unprecedented risk of cyber attacks.

The identified difficulties expressed by Maglaras et al. (2022) indicate the intricacy of safeguarding the contemporary CIs. The reason is that interdependencies have risks that are introduced systematically; and at the same time, IT/OT convergence is breaking the traditional definition of security. The current infrastructural systems, invisibility, and shortage of skills complicate the security of such systems. Conversely, emerging technologies such as cloud computing, Edge intelligence, and 5G/6G communications networks and analysis conducted using AI-powered systems are both dangerous and promising. New approaches to securing these technologies are needed, moreover, cyber and physical security spheres should be more closely integrated.

The future action plan would then aim at resilience, collaboration and defense based on intelligence. The architecture of resilience by design, better exchange of threat intelligence, stricter cloud and 5G security policies would assist in preparing the infrastructural systems to be ready against future threats. Besides that, a greater emphasis on human elements would raise the overall readiness of CI service providers to cyber threat.

Protecting critical infrastructures is not merely an IT dilemma to nations, but IT necessity across the world. The continuously growing risks linked with cyberattacks imply that the protection of the critical infrastructural services will be associated with active governmental and IT-related measures and activities at the national and international levels. Through this, societies are able to shield their critical systems and infrastructural foundation against escalating dangers relating to progressive as well as a constantly growing cyberattacks.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Aghazadeh Ardebili, A., Lezzi, M., & Pourmadadkar, M. (2024). Risk Assessment for Cyber Resilience of Critical Infrastructures: Methods, Governance, and Standards. Applied Sciences, 14(24), 11807. https://www.mdpi.com/2076-3417/14/24/11807?.

[2] Baseri, Y., Chouhan, V., & Ghorbani, A. (2024). Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure. arXiv preprint arXiv:2404.10659. https://arxiv.org/abs/2404.10659?.

[3] Cybersecurity in Critical Infrastructures: A Contemporary Review (2024) — a peer review of recent threat trends, defenses, sector-specific vulnerabilities (energy, transport, healthcare), and gaps in standardization. https://journaljsrr.com/index.php/JSRR/article/view/2868?.

[4] Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. Land Forces Academy Review, 26(1), 69-75. https://sciendo.com/pdf/10.2478/raft-2021-0011.

[5] Järveläinen, J., Dang, D., Mekkanen, M., & Vartiainen, T. (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), 2479546. https://www.tandfonline.com/doi/pdf/10.1080/12460125.2025.2479546?.

[6] Jiang, Y., Jeusfeld, M. A., Mosaad, M., & Oo, N. (2024). Enterprise architecture modeling for cybersecurity analysis in critical infrastructures—A systematic literature review. International Journal of Critical Infrastructure Protection, 46, 100700. https://www.sciencedirect.com/science/article/pii/S1874548224000416?.

[7] Lehto, M. (2022). Cyber-attacks against critical infrastructure. In Cyber security: Critical infrastructure protection (pp. 3-42). Cham: Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-030-91293-2_1.

[8] Lewis, J. A. (2006). Cybersecurity and critical infrastructure protection. Center for Strategic and International Studies, 9, 18. http://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/0601_cscip_preliminary.pdf.

[9] Maglaras, L. A., Kim, K. H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., ... & Cruz, T. J. (2018). Cyber security of critical infrastructures. Ict Express, 4(1), 42-45. https://www.mdpi.com/1424-8220/22/14/5105?.

[10] Maglaras, L. A., Kim, K. H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., ... & Cruz, T. J. (2022). Cyber security of critical infrastructures. Ict Express, 4(1), 42-45. https://www.sciencedirect.com/science/article/pii/S2405959517303880.

[11] Malatji, M., Marnewick, A. L., & Von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. Information & Computer Security, 30(2), 255-279. https://www.emerald.com/ics/article/30/2/255/111698/Cybersecurity-capabilities-for-critical?.

[12] Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., ... & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. Sensors, 23(8), 4060. https://www.mdpi.com/1424-8220/23/8/4060?.

[13] Roshanaei, M. (2021). Resilience at the core: critical infrastructure protection challenges, priorities and cybersecurity assessment strategies. Journal of Computer and Communications, 9(8), 80-102.

[14] Toledano, S. A. (2024). Critical Infrastructure Security: Cybersecurity lessons learned from real-world breaches. Packt Publishing Ltd.

https://books.google.com/books?hl=en&lr=&id=2a4FEQAAQBAJ&oi=fnd&pg=PP1&dq=Cybersecurity+in+Critical+Infrastructures+(2023)+%E2%80%94+general+discussion+of+CI+systems%E2%80%99+vulnerability+across+sectors+(energy,+transport,+water,+telecom)+and+growing+threat+landscape.&ots=KK1Hp4dCAp&sig=FtaZTiba3ELdYtXgB495Iyq7cFw.

[15] Volk, M. (2024). A safer future: Leveraging the AI power to improve the cybersecurity in critical infrastructures. Electrotechnical Review/Elektrotehniski Vestnik, 91(3). https://ev.fe.uni-lj.si/3-2024/Volk.pdf.

[16] Yigit, Y., Ferrag, M. A., Sarker, I. H., Maglaras, L. A., Chrysoulas, C., Moradpoor, N., & Janicke, H. (2024). Critical infrastructure protection: Generative AI, challenges, and opportunities. arXiv preprint arXiv:2405.04874. https://arxiv.org/abs/2405.04874?.