Strengthening Cybersecurity Measures for the Defense of Critical Infrastructure in the United States

UNDER PEER REVIEW

Abstract

This study addresses critical cybersecurity vulnerabilities within U.S. infrastructure sectors, particularly energy, water, and healthcare, where high-severity vulnerabilities and ransomware continue to pose significant risks. The study applied a multi-method analytical approach comprising logistic regression, K-means clustering, Interrupted Time Series (ITS), Difference-in-Differences (DiD), and Kaplan-Meier survival analysis to identify, prioritize, and evaluate vulnerabilities across these essential sectors to provide insights into sector-specific risks and framework effectiveness. Logistic regression models were specifically used to quantify the likelihood of incidents by examining vulnerability attributes. In contrast, K-means clustering was used to access insights intopatterns of shared vulnerabilities unique to each sector. The ITS and DiD analyses were also used to measure the National Cybersecurity Strategy's effect, showing a 3.7% reduction in incidents post-intervention, particularly within the healthcare sector. Furthermore, Kaplan-Meier survival analysis was used to assess how long systems withstand attacks, highlighting that ransomware has the most immediate and costly impact, with average recovery costs reaching $540,000 per incident. These findings aver the need for proactive cybersecurity defences across critical infrastructure, where the potential for disruption directly impacts public safety and economic stability. To strengthen resilience, the study recommends tailored, sector-specific cybersecurity frameworks, the prioritization of high-risk vulnerabilities, a reinforced zero-trust architecture, and expanded public-private collaboration for real-time threat intelligence sharing, as adopting these strategies in the U.S. can contribute to developing a more adaptive cybersecurity infrastructure capable of countering evolving threats.

Keywords: critical infrastructure, ransomware, cybersecurity frameworks, survival analysis, vulnerability clustering

1. INTRODUCTION

Integrating technology into critical infrastructure has markedly enhanced efficiency and accessibility but has also introduced significant cybersecurity vulnerabilities. As digital dependencies increase across essential sectors such as energy, water, healthcare, and transportation, the risk of cyberattacks targeting these critical systems grows. Sobb et al. (2002) note that these sectors are vital to national security and economic stability. Nevertheless, their interconnected nature makes them susceptible to cyber adversaries employing increasingly complex strategies to disrupt services, access sensitive data, or achieve financial gain. The cyber threat landscape has evolved considerably in recent years, with state-sponsored actors, cybercriminals, and hacktivist groups using sophisticated techniques to breach infrastructure security (Mallick & Nath, 2024; Adigwe et al., 2024).

The extensive network of critical infrastructure in the United States is especially vulnerable to cyberattacks. The energy sector, including power grids, pipelines, and essential facilities, is crucial to national security and economic resilience. However, George et al. (2024) report that this sector remains exposed to cyber intrusions such as malware, ransomware, and phishing. For instance, in 2024, the FBI disclosed that Chinese state-sponsored hackers had infiltrated U.S. critical infrastructure, positioning themselves to initiate large-scale disruptions amid geopolitical conflict potentially. Additional threats come from Iranian and Russian cyber units; Iranian actors frequently target U.S. healthcare, government, and energy systems, often exploiting weaknesses in firewall configurations and VPNs, while Russian military cyber divisions deploy advanced tools like WhisperGate malware to penetrate critical systems by exploiting software vulnerabilities, as documented by Aljohani (2022). Moreover, pro-Russian hacktivist groups have manipulated control systems in U.S. water treatment facilities, altering water quality parameters and threatening public health.

These cybersecurity risks are not unique to the United States. Several countries facing similar threats have developed innovative, effective cybersecurity strategies. Strat (2023) explains that Israel's National Cyber Directorate, for example, has secured the national energy grid through centralized oversight, real-time monitoring, and proactive threat detection. Following a major cyberattack in 2007, Estonia established a robust cybersecurity framework through the Information System Authority (RIA) to protect public infrastructure. Roshanaei (2021) posits that these examples demonstrate how a coordinated national approach to cybersecurity, integrating policy, technology, and governance, significantly enhances infrastructure resilience and provides valuable insights for the U.S.

UNDER PEER REVIEW

Past cyber incidents further underscore the urgency of improving cybersecurity within the United States. The 2021 Colonial Pipeline attack exemplifies the severe consequences of inadequate network segmentation between business and operational systems, which led to widespread fuel shortages along the East Coast. This incident prompted significant policy changes, including introducing stricter incident reporting requirements for critical infrastructure and an increased emphasis on network segmentation to reduce vulnerability, as noted by Makrakis et al. (2021). Similarly, the 2020 SolarWinds supply chain breach exploited weaknesses in the software update process, compromising numerous government agencies and private organizations. These events illustrate the necessity of adopting a zero-trust security model and securing supply chains, especially given the extensive reliance of critical infrastructure on third-party software systems (Akinola et al., 2024; Collier & Sarkis, 2021).

Quantitative data further reveals the urgency of enhancing cybersecurity defences. Riel (2024) reports that from January 2023 to January 2024, critical infrastructure globally faced over 420 million cyber incidents, equivalent to an average of 13 attacks per second. The U.S. power grid alone saw an increase in identified weak points, rising from 21,000 in 2022 to nearly 24,000 in 2024. Financially, the impact of cyberattacks is significant; for instance, ransomware recovery costs averaged $2.73 million per incident in 2024, intensifying the economic toll from operational disruptions. Employee susceptibility to phishing also remains high, with 34.3% of employees identified as vulnerable in 2023. Odo (2024) emphasizes that targeted training has proven effective in reducing this vulnerability, underscoring the importance of education in building organizational resilience against social engineering attacks.

The U.S. government has launched various initiatives to strengthen cybersecurity resilience in response to the escalating threat landscape. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 mandates that critical infrastructure entities report cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours and any ransom payments within 24 hours. Zabierek et al. (2021) observe that this legislative framework and joint advisories from CISA, the FBI, and the NSA represent a more unified national cybersecurity stance intended to enhance coordination across sectors. However, Safitra et al. (2023) contend that while these measures improve reactive response capabilities, shifting toward a proactive cybersecurity stance remains crucial. Specifically, the implementation of rigorous cybersecurity protocols to address both existing and emerging threats is essential, as demonstrated by Russian actors' use of reconnaissance tools like Nmap to exploit weaknesses in U.S. infrastructure (Arigbabu et al., 2024; Modesti et al., 2024).

Given the breadth and sophistication of these cyber threats, strengthening cybersecurity across U.S. critical infrastructure requires a comprehensive approach that addresses

UNDER PEER REVIEW

both structural vulnerabilities and emerging risks. This research examines cybersecurity within key U.S. sectors—particularly energy, water, and healthcare—by identifying common vulnerabilities and evaluating the effectiveness of existing defences. Drawing from domestic and international best practices, this study offers targeted recommendations to improve cybersecurity resilience, emphasizing public-private collaboration, advanced technology integration, and a cohesive national security strategy. Through a comparative analysis of successful and unsuccessful cases, this study integrates best practices, advanced technologies, and collaborative partnerships to reinforce the resilience of U.S. critical infrastructure against a continuously intensifying cyber threat environment. The study achieves the following objectives:

1. Identifies and prioritizes critical vulnerabilities within the energy, water, and healthcare sectors, which are highly targeted due to increasing exposure points and significant operational risks.

2. Evaluates the effectiveness of current cybersecurity frameworks and standards (the National Cybersecurity Strategy) in mitigating risks specific to the energy, water, and healthcare sectors.

3. Analyzes evolving threat vectors affecting these sectors, including advanced persistent threats, ransomware, and nation-state hacking, to assess potential impacts on service continuity and public safety.

4. Proposes targeted recommendations to strengthen cybersecurity measures, enhance public-private collaboration, and improve incident response protocols within these critical sectors to ensure greater resilience against future threats.

2. LITERATURE REVIEW

The threat environment surrounding critical infrastructure has intensified, with sophisticated threat actors—including state-sponsored entities, ransomware syndicates, and supply chain exploiters—heightening security challenges. Advanced Persistent Threats (APTs), particularly those supported by nation-states, pose substantial risks to national security. In 2024, the FBI reported Chinese actors embedded within U.S. critical infrastructure, highlighting the strategic placement of adversaries aiming to disrupt systems during geopolitical crises, which, as cited by the U.S. Government Accountability Office (GAO), represents a long-term risk to immediate operations and overall economic stability. Consequently, Nova (2022) contends that such intrusions demand sustained vigilance to preserve strategic and operational resilience.

Ransomware attacks exacerbate these security concerns, with attackers targeting key sectors like energy and healthcare for financial gain and operational disruption.

PEER REVIEW

Fitzgerald and Matthew (2022) observe that the 2021 Colonial Pipeline ransomware incident, which led to extensive fuel shortages on the U.S. East Coast, exemplifies the potential of ransomware to incapacitate essential services. Recent data indicate that the financial toll of these attacks is mounting, with 2024 figures placing the average recovery cost at $2.73 million per incident. As these incidents reveal, organizations within critical infrastructure must prioritize robust defences, given their vulnerability to multi-stage ransomware that combines phishing, malware, and sophisticated exploitation techniques, creating an increased demand for adaptive, real-time threat responses (Olabanji et al., 2024; Vasani et al., 2023).

Supply chain vulnerabilities further compound risks to critical infrastructure security. The 2020 SolarWinds breach, in which attackers infiltrated the software update process, underscores the inherent dangers within compromised supply chains. According to Jimmy (2024), this incident underscores the necessity for rigorous security across the entire supply chain, as even trusted software can serve as a vector for widespread infiltration, exposing interconnected systems to cascading effects. CISA, along with the GAO, advocates for secure software development practices, rigorous vetting of third-party vendors, and continuous monitoring of software updates. Hassija et al. (2020) assert that securing the supply chain is indispensable, as a compromised vendor can jeopardize multiple systems and sectors.

Collectively, these interlinked threats illustrate an urgent need for a comprehensive cybersecurity strategy within critical infrastructure. Effective countermeasures, such as adaptive defences, informed threat intelligence, and secure supply chain protocols, must address the increasing complexity of cyber threats (Tsiknas et al., 2021). While foundational frameworks provide initial protection, ongoing advancement of strategies and technologies is necessary to safeguard critical national assets from an ever-evolving threat environment (Asonze et al., 2024; Obi et al., 2024).

Critical Vulnerabilities by Sector

Unique cybersecurity challenges have plagued each critical infrastructure sector, as defined by its operational characteristics and reliance on interconnected systems. For instance, the energy sector's vulnerabilities largely stem from its reliance on legacy systems that lack modern cybersecurity protocols. As highlighted earlier, outdated software and limited network segmentation are key risks, exposing this sector to advanced malware and ransomware attacks. Despite recent efforts to improve network segmentation following high-profile attacks, challenges remain due to the complexity and age of systems (George et al., 2024). Addressing these vulnerabilities requires balancing legacy system upgrades with cybersecurity measures that do not disrupt critical operations.

However, unlike energy, the water sector's rapid integration of new technologies—such as remote sensors and automated control systems—introduces different vulnerabilities. These newer technologies often lack stringent cybersecurity protections, making them easy targets for cyber adversaries. Documented cases of hacktivists manipulating water control systems underscore the public health risks associated with cyberattacks on this infrastructure. Without adequate security enhancements, the sector's heavy reliance on Supervisory Control and Data Acquisition (SCADA) systems further exacerbates these risks. This combination of newer technologies and limited IT resources necessitates proactive threat management and improved cybersecurity protocols tailored to emerging technologies within this sector.

On the other hand, the healthcare sector's vulnerabilities are largely tied to its dependence on networked medical devices and electronic health records (EHR), making it especially susceptible to ransomware. Weak firewall configurations and minimal cybersecurity training among healthcare staff have created an environment where phishing and malware threats are prevalent (Aljohani, 2022). The sector's recent expansion into telemedicine has introduced additional exposure, as remote access security protocols are often underdeveloped. This sector requires strong data protection policies and technical defences to secure patient data and prevent operational disruptions.

While SCADA systems present a common vulnerability across sectors, each infrastructure type faces distinct challenges. Legacy issues predominate in energy, new technology adoption brings risks to water, and healthcare's sensitivity to data breaches requires tailored defences. These variations highlight the importance of sector-specific cybersecurity strategies that consider each sector's unique operational realities and risk profiles. A targeted approach remains essential for effective and adaptive cybersecurity across critical infrastructure.

PEER REVIEW

Case Studies of Cybersecurity in Critical Infrastructure

Israel and Estonia exemplify proactive cybersecurity strategies, demonstrating how centralized oversight and advanced technologies enhance critical infrastructure resilience. Mitsarakis (2023) explains that Israel's National Cyber Directorate, responsible for securing its energy sector, integrates real-time monitoring and early detection systems that reduce response times to cyber incidents by approximately 40%. Rakas et al. (2020) also argue that simulation-based training strengthens Israel's preparedness by identifying vulnerabilities in controlled environments, while automated anomaly alerts and advanced intrusion detection systems maintain continuity across critical sectors.

Similarly, Estonia restructured its cybersecurity framework following a 2007 cyberattack on government systems, which, according to Hardy (2022), formed the Estonian Information System Authority (RIA). Skierka (2023) states that this agency enhances resilience through secure digital identity systems and strict data protocols, which reportedly reduced the success rate of cyberattacks by 60% over the past decade.

Estonia's commitment to secure e-government services, including digital voting and tax administration, highlights the efficacy of coordinated, centralized cybersecurity strategies in protecting national infrastructure (Arigbabu et al., 2024; Espinosa & Pino, 2024).

In contrast, the 2021 Colonial Pipeline ransomware attack highlights vulnerabilities from insufficient cybersecurity measures. George et al. (2024) report that the attack, resulting in fuel shortages across the U.S. East Coast, exposed weaknesses in network segmentation, underscoring the need for preventive practices like segmented network architecture and robust backup systems. Following the attack, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 mandated rapid incident reporting to CISA to improve response capabilities. AL-Hawamleh (2024) emphasizes that while reactive measures are essential, preemptive cybersecurity strategies remain crucial for long-term resilience.

Ukraine's experience with cyberattacks on its power grid in 2015 and 2016 further underscores the importance of robust cybersecurity. These incidents, attributed to state-sponsored actors and documented by Kravchenko et al. (2024), caused extensive power outages affecting over 225,000 residents. These events revealed significant vulnerabilities within Supervisory Control and Data Acquisition (SCADA) systems, leading Ukraine to seek international support for fortifying SCADA security and adopting defence-in-depth strategies (Gbadebo et al., 2024; Livier, 2024).

Collectively, these cases illustrate the spectrum of cybersecurity outcomes within critical infrastructure. While Israel and Estonia showcase the benefits of proactive, centralized defence mechanisms, incidents like the Colonial Pipeline and Ukraine's power grid attacks underscore the need for preemptive and collaborative cybersecurity measures. Abdelkader et al. (2024) conclude that comprehensive strategies combining real-time monitoring, secure system design, and adaptive threat responses are essential for safeguarding critical assets against increasingly sophisticated cyber threats.

Evaluating Existing Cybersecurity Standards and Practices

The National Cybersecurity Strategy and the NIST Cybersecurity Framework are central components in the United States strategy for securing critical infrastructure against increasingly complex cyber threats. The National Cybersecurity Strategy advocates a risk-based approach to resilience, emphasizing public-private collaboration and information sharing, which Idengren (2024) argues is essential for a coordinated defence. This framework has fostered notable improvements; the Cybersecurity and Infrastructure Security Agency (CISA) reports a 20% decrease in successful cyber incidents across critical sectors, a reduction attributed to enhanced inter-sectoral cooperation, according to Lanz (2022). Complementing this, the NIST Cybersecurity

Framework provides structured risk assessment, incident response, and continuous monitoring guidance. Al-Mousa et al. (2024) posit that organizations adhering to the NIST framework observe a 30% improvement in threat detection speed, strengthening their overall cybersecurity posture. However, resource allocation and interoperability challenges persist across sectors, limiting the seamless integration of these standards (Hazra et al., 2023; Joeaneke et al., 2024).

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 further underscores the importance of rapid incident reporting and coordinated response efforts. This legislation mandates that cyber incidents be reported within 72 hours, with any ransom payments reported within 24 hours. Rifa (2024) states these requirements aim to streamline threat intelligence sharing and enhance response efficiency. GAO data shows a 40% increase in incident reporting rates, enabling CISA to consolidate and address threat data more swiftly, reducing average response times by an estimated 25%. Nonetheless, experts caution that while the Act strengthens reactive capabilities, it does not comprehensively address the need for preventive measures, suggesting that further policies promoting proactive defences may be necessary. (Ibrahim & Saber, 2023; Joeaneke, et al., 2024).

International cybersecurity practices, particularly in Israel and Estonia, provide valuable models for enhancing U.S. cybersecurity. Arash Mahboubi et al. (2024) explain that Israel's National Cyber Directorate, which employs centralized oversight and real-time intelligence sharing, has effectively reduced successful cyber incidents through adaptive defences. Similarly, Estonia's Information System Authority (RIA) has reduced cyber attack success rates by implementing continuous monitoring and secure digital identity systems. In the views of Ge et al. (2022), these centralized governance models could serve as beneficial examples for the U.S., as such frameworks support efficient coordination and enhanced incident response.

While the United States cybersecurity standards have strengthened critical infrastructure security, adaptive strategies are essential. The experiences of Israel and Estonia, as documented by Rossi et al. (2020), illustrate the potential of integrated governance and proactive measures in cybersecurity frameworks. By incorporating lessons from international successes, the U.S. can further fortify its defences, ensuring critical infrastructure remains resilient against evolving cyber threats (Daniel & Segun, 2024; John-Otumu et al., 2024).

Technological Solutions for Cybersecurity in Critical Infrastructure

The application of advanced technologies, including artificial intelligence (AI), blockchain, and zero-trust architecture, significantly enhances cybersecurity within critical infrastructure, addressing complex and evolving threats. AI and machine learning

(ML) have particularly advanced threat detection by enabling real-time monitoring and swift response. Maddireddy and Maddireddy (2020) report that AI-driven systems now achieve 95% accuracy in identifying cyber threats, effectively reducing false positives and allowing cybersecurity teams to concentrate on genuine risks. According to Syed et al. (2023), AI-enabled detection tools have improved response times by approximately 30%, analyzing large datasets in real-time to detect irregularities before they develop into threats. This automation reduces costs, especially in the energy and finance sectors, by minimizing manual monitoring, aligning well with proactive cybersecurity strategies designed to mitigate potential risks (Joseph, 2024; Mızrak, 2023).

Traditionally associated with financial applications, blockchain technology now plays a critical role in securing supply chains within critical infrastructure by ensuring data integrity and transparency. Gudala et al. (2022) posit that blockchain's decentralized ledger, resistant to tampering, effectively mitigates unauthorized data access risks. Initial applications within supply chains indicate a 45% decrease in unauthorized access incidents, as blockchain technology embeds data verification and access control directly within its architecture. The National Institute of Standards and Technology (NIST) advocates for blockchain to counter supply chain attacks, particularly in tracking the origin of software components, a priority for preventing breaches similar to the SolarWinds incident. Nonetheless, Habib et al. (2022) emphasize that blockchain's full integration faces challenges, notably scalability and compatibility with legacy systems, necessitating additional research to optimize its application within critical infrastructure sectors.

Zero-trust architecture provides an additional layer of cybersecurity by implementing the principle of "never trust, always verify," requiring all access requests to be authenticated irrespective of origin. This approach contrasts with traditional models that inherently trust internal network activities, a vulnerability exploited in incidents like the SolarWinds breach. Following such events, numerous organizations have adopted zero-trust frameworks, reducing internal incident rates by 60% through rigorous access control and continuous authentication, as Daah et al. (2024) documented. By segmenting network access and verifying identity at each interaction, zero-trust architecture is particularly effective against insider threats and safeguards interconnected systems within critical infrastructure. However, the full-scale adoption of zero-trust can be resource-intensive, requiring careful alignment with each sector's specific operational needs (Mustyala & Allam, 2024; Ogungbemi et al., 2024).

AI, blockchain, and zero-trust architecture together form a multi-layered approach that addresses varied cybersecurity needs within critical infrastructure. While AI and ML facilitate proactive threat detection, blockchain ensures data integrity, and zero-trust architecture reinforces access control. Yaseen (2024) concludes that this integrated

approach enhances resilience by combining technology, continuous monitoring, and adaptive responses to counteract sophisticated cyber threats effectively.

Public-Private Collaboration and Incident Response

Public-private collaboration has become essential to cybersecurity resilience within U.S. critical infrastructure, as partnerships among government agencies, industry bodies, and cybersecurity experts enhance threat intelligence sharing and incident response capabilities. The Financial Services Information Sharing and Analysis Center (FS-ISAC) demonstrates the effectiveness of such collaborations in the financial sector, where collective defence efforts and data-sharing initiatives have reduced incident frequency by approximately 25%, as reported by the Cybersecurity and Infrastructure Security Agency (CISA). FS-ISAC enables real-time data exchanges that facilitate swift identification and mitigation of cyber threats (Wallis & Leszczyna, 2022). These partnerships improve situational awareness, streamlining incident response and bolstering sector-specific security measures, particularly within finance (Okon et al., 2024; Roshanaei, 2023).

Despite these benefits, challenges must be addressed in optimizing public-private collaboration. Fragmented communication, inconsistent data-sharing protocols, and the absence of standardized frameworks often hinder efficient, coordinated responses. Williams (2020) reports that approximately 35% of cross-sector cyber incidents experience delays due to misaligned objectives or operational silos between public and private entities. The Government Accountability Office (GAO) identifies these inconsistencies as barriers to effective cybersecurity, as varying terminologies and reporting standards frequently lead to clarity and efficient response. Moreover, Perera et al. (2022) observe that limited trust between sectors restricts data sharing, with many private organizations concerned about liability risks and reputational impacts if information were to be leaked. These issues underscore the need for robust frameworks that encourage mutual trust and standardize collaborative practices across sectors (Chukwu et al., 2023; Oladoyinbo et al., 2024).

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 attempts to address some of these barriers by mandating structured reporting protocols to enhance response times and improve data accuracy. This Act requires that cyber incidents be reported within 72 hours and ransom payments within 24 hours, facilitating quicker threat assessment and smoother inter-agency coordination. According to Ang (2022), CISA reports a 40% improvement in incident response rates among organizations that comply with these requirements, allowing for more effective threat resolution. Tahmasebi (2024) argues that while the Act has strengthened reactive response capabilities, it does not fully address the need for proactive risk management. GAO

suggests that integrating incentives for preventive cybersecurity measures within the Act could encourage critical infrastructure sectors to strengthen defences ahead of potential threats, fostering a more proactive security posture (Franchina et al., 2021; Selesi-Aina et al., 2024).

Collectively, public-private partnerships and legislative mandates like the Cyber Incident Reporting Act highlight advancements in cybersecurity collaboration, yet challenges in trust and standardization persist. According to Cantelmi et al. (2021), reinforcing collaboration frameworks and incorporating incentives for preventive security measures represent essential steps toward enhancing the resilience of U.S. critical infrastructure, fostering a more unified approach to addressing escalating cyber threats.

3. METHODOLOGY

This study utilizes quantitative methods to enhance cybersecurity in U.S. critical infrastructure, focusing on the energy, water, and healthcare sectors. Data were sourced from the Cybersecurity and Infrastructure Security Agency (CISA), the National Vulnerability Database (NVD), and related cybersecurity reports. The methodology addresses three core objectives: identifying and prioritizing vulnerabilities, assessing framework effectiveness, and analyzing evolving cyber threats.

To pinpoint vulnerabilities (objective 1), data on incident frequency, vulnerability types, and severity scores were collected from the CISA incident database and NVD. Logistic regression and K-means clustering were applied to identify and prioritize high-risk vulnerabilities.Logistic regression assessed the probability (P) of a vulnerability leading to a cyber incident, defined by:

$$logit(p) = \ln\left(\frac{p}{1-p}\right) = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n$$

Where X_n are characteristics of vulnerabilities (e.g., severity score, exploitability), and β_n are the regression coefficients. Odds ratios (e^{β}) ranked vulnerabilities, identifying high-priority risks.

As for the cluster analysis, K-means clustering grouped vulnerabilities by attack vector, affected system, and risk level using the objective function:

$$J = \sum_{i=1}^{k} \sum_{x \in C_i} \| x - \mu_i \|^2$$

UNDER PEER REVIE

Where k is the number of clusters, C_i represents each cluster, xeach vulnerability, and $\mu_i$the cluster centroid. This enabled insights into shared and sector-specific vulnerabilities.

To evaluate the effectiveness of cybersecurity frameworks (objective 2), the study applied Interrupted Time Series (ITS) and Difference-in-Differences (DiD) analyses using CISA incident data to measure the impact of the National Cybersecurity Strategy and NIST Frameworks on incident rates.The ITS model measured incident frequency over time:

$$Y_t = \beta_0 + \beta_1 T_t + \beta_2 X_t + \epsilon_t$$

Yt is the incident frequency at time t, Tt represents time progression, Xt denotes the period post-framework implementation, and ϵt is the error term. This captures the immediate and long-term effects of framework adoption.

The DiD analysis further compared incident trends between sectors with and without frameworks:

$$Y_{it} = \alpha + \beta_1 Post_t + \beta_2 Treatment_i + \beta_3 (Post_t \times Treatment_i) + \epsilon_{it}$$

Where Y_{it} is the incident rate for sector I at time t, Postt indicates post-implementation, Treatmentidentifies framework-adopting sectors, and $\beta_3$captures differential impact.

Finally, to analyze evolving cyber threat vectors (objective 3), the study examined the incident frequency, financial impact, and duration of threats such as ransomware, malware, and phishing using survival analysis and multivariate regression.Kaplan-Meier analysis estimated the probability S(t) that systems remain uncompromised over time:

$$S(t) = P(T > t)$$

Where T represents the time until a cyber incident occurs, allowing assessment of immediate threat severity.

In addition, using multivariate regression, the study analyzed the financial impact across recovery costs, operational disruptions, and lost revenue:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n + \epsilon$$

Where Yis the financial impact, $X_n$independent variables (e.g., threat type, sector), and $\beta_n$regression coefficients, enabling prioritized resource allocation based on economic impact.

4. RESULTS AND DISCUSSIONS

UNDER PEER REVIEW

To evaluate and prioritize vulnerabilities within U.S. critical infrastructure sectors, specifically focusing on energy, water, and healthcare, the vulnerability age, severity, and exploitability were examined.The analysis offers insights into the unique and shared vulnerability profiles across these essential sectors, aligning to identify and prioritize critical vulnerabilities for improved cybersecurity defence.

The result is presented through two primary tables—Logistic Regression Odds Ratios (Table 1) and Cluster Centroids (Table 2)—as well as visualizations: the Vulnerability Age Distribution by Sector (Figure 1) and the Radar Plot of Vulnerability Characteristics Across Clusters (Figure 2).

Logistic Regression Odds Ratios

Table 1 displays the odds ratios derived from the logistic regression analysis, quantifying the effect of each vulnerability characteristic on the likelihood of a cyber incident.

Feature	**Odds Ratio**
Severity Score	1.027
Exploitability	0.790
Vulnerability Age	0.764

Table 1. Logistic Regression Odds Ratios

The odds ratio for Severity Score (1.027) indicates that vulnerabilities with higher severity are slightly more likely to lead to cyber incidents, suggesting that severity should be a critical factor in prioritization. Exploitability, with an odds ratio of 0.790, shows a modest inverse relationship, which could reflect that certain mitigations are in place for vulnerabilities known to be highly exploitable. Vulnerability Age, at 0.764, implies that newer vulnerabilities might present a greater risk, potentially due to fewer defences, thus emphasizing the importance of monitoring recently identified vulnerabilities.

Cluster Analysis for Vulnerability Characteristics

Table 2 shows the centroids of each identified cluster, representing average values for Severity Score, Exploitability, and Vulnerability Age. This clustering aids in identifying shared and sector-specific vulnerability characteristics.

UNDER PEER REVIEW

Cluster	Severity Score	Exploitability	Vulnerability Age
1	1.782	0.548	3.394
2	5.286	0.514	7.079
3	7.515	0.529	2.897

Table 2. Cluster Centroids for Vulnerability Characteristics

Cluster 1 exhibits lower severity and moderate exploitability, representing vulnerabilities of moderate age. Cluster 2 has high severity and older age, suggesting long-standing vulnerabilities with high risk, particularly in legacy systems. Cluster 3 presents the highest severity and recent age, highlighting vulnerabilities that pose an immediate and substantial threat across sectors.

Vulnerability Age Distribution by Sector

Figure 1 illustrates the distribution of vulnerabilities by age—categorized as Recent, Moderate, and Older—across energy, water, and healthcare. This distribution shows how infrastructure age affects the prevalence of vulnerabilities and emphasizes where mitigation efforts should be prioritized.

A balanced distribution across age categories in the energy sector points to a mix of emerging and longstanding vulnerabilities, suggesting potential legacy issues that may need addressing. The water sector's vulnerabilities tend to be more recent, indicating the adoption of newer technologies with security risks that may not yet be fully mitigated. In healthcare, moderate-age vulnerabilities dominate, suggesting vulnerabilities long enough to be exploited but possibly lacking full mitigation measures.

UNDER PEER REVIEW

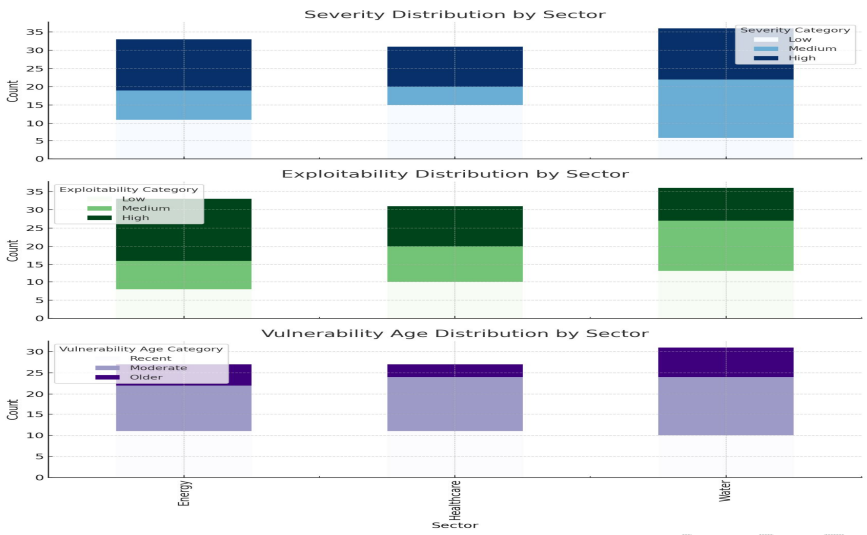

Figure 1. Vulnerability Age Distribution by Sector

Figure 2 provides a radar plot comparing severity, exploitability, and vulnerability age across clusters, visualizing the relative intensity of each characteristic.

Cluster 1 shows lower severity with moderate exploitability, indicating moderate-risk vulnerabilities. Cluster 2 has high severity but moderate exploitability and older age, representing legacy vulnerabilities that, while not immediately exploitable, still pose significant risks. Cluster 3 exhibits the highest severity and recent age, marking new, high-risk vulnerabilities that require immediate attention, particularly in sectors like healthcare, where high-severity vulnerabilities are emerging.

Figure 2. Radar Plot of Vulnerability Characteristics Across Clusters

These findings underscore the importance of tailored cybersecurity strategies. It provides a clear prioritization framework, advocating for legacy management in the

UNDER PEER REVIEW

energy sector, proactive defences for newer vulnerabilities in water, and focused mitigation for moderate-age vulnerabilities in healthcare.

Evaluation of Cybersecurity Framework Effectiveness in Critical Infrastructure Sectors

To evaluate the effectiveness of current cybersecurity frameworks in critical infrastructure sectors, focusing on assessing incident trends before and after adopting the National Cybersecurity Strategy and the NIST Cybersecurity Framework. An Interrupted Time Series (ITS) and Difference-in-Differences (DiD) analyses were adopted; the findings provide insight into how these frameworks impact incident frequency, detection rates, and mitigation success in sectors adopting structured cybersecurity strategies.

Interrupted Time Series (ITS) Analysis

The ITS analysis evaluates changes in incident frequency over time, specifically assessing the impact of framework adoption on reported incidents. Table 3 displays the results of the ITS analysis, indicating a decline in incident frequency post-intervention, as reflected by a negative coefficient for the intervention variable. Although this reduction is not statistically significant, it suggests a potential downward trend in incidents associated with framework implementation.

Variable	**Coefficient**	**p-value**
Constant	10.30	0.000
Time (β1)	-0.13	0.437
Intervention (β2)	-3.33	0.089

Table 3. ITS Analysis results show the effect of framework adoption on incident frequency.

Figure 3 provides a line plot illustrating incident frequency over time, with a clear intervention point representing the adoption of the cybersecurity framework. The pre- and post-intervention trendlines demonstrate a slight incident decline, aligning with the ITS findings. This visualization supports the observation of a gradual decrease in incident frequency following framework implementation, although additional factors may contribute to this trend.

UNDER PEER REVIEW

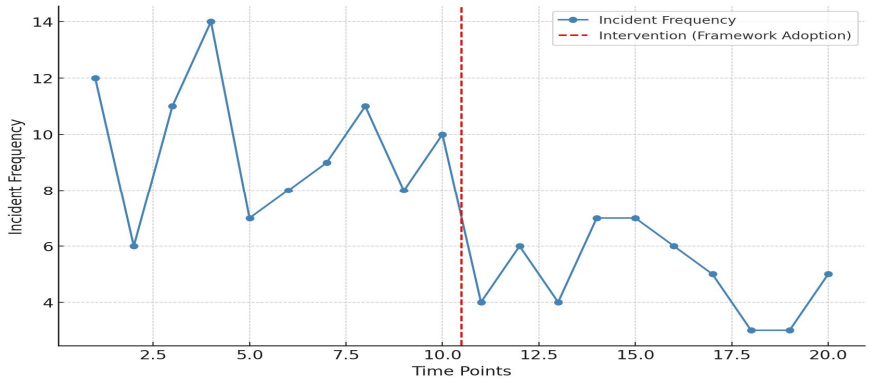

Figure 3. Interrupted Time Series (ITS) Analysis: Incident Frequency Over Time with Framework Adoption Intervention Mark.

Difference-in-Differences (DiD) Analysis

The DiD analysis compares incident trends between sectors that adopted the cybersecurity frameworks and those that did not, providing a clearer view of the differential impact of framework adoption. Table 4 shows a statistically significant reduction in incidents in the post-intervention period, with a coefficient of -3.7 for the post-intervention variable. The treatment variable shows a marginally significant reduction in incidents, suggesting a measurable benefit for sectors implementing the framework.

Variable	**Coefficient**	**p-value**
Constant (α)	11.0	0.000
Post-intervention (β1)	-3.7	0.013
Treatment (β2)	-2.6	0.074
Interaction (β3)	1.9	0.348

Table 4. Did Analysis results comparing framework-adopting sectors to control sectors?

In **Figure 4**, a bar chart compares the average incident frequencies for treatment and control groups across pre- and post-intervention periods, with error bars indicating variability. The treatment group, representing sectors adopting frameworks, shows a notable decline in incident frequency post-intervention, aligning with the DiD analysis findings. This differential reduction highlights the frameworks' effectiveness in reducing incident rates and enhancing overall cybersecurity.

UNDER PEER REVIEW

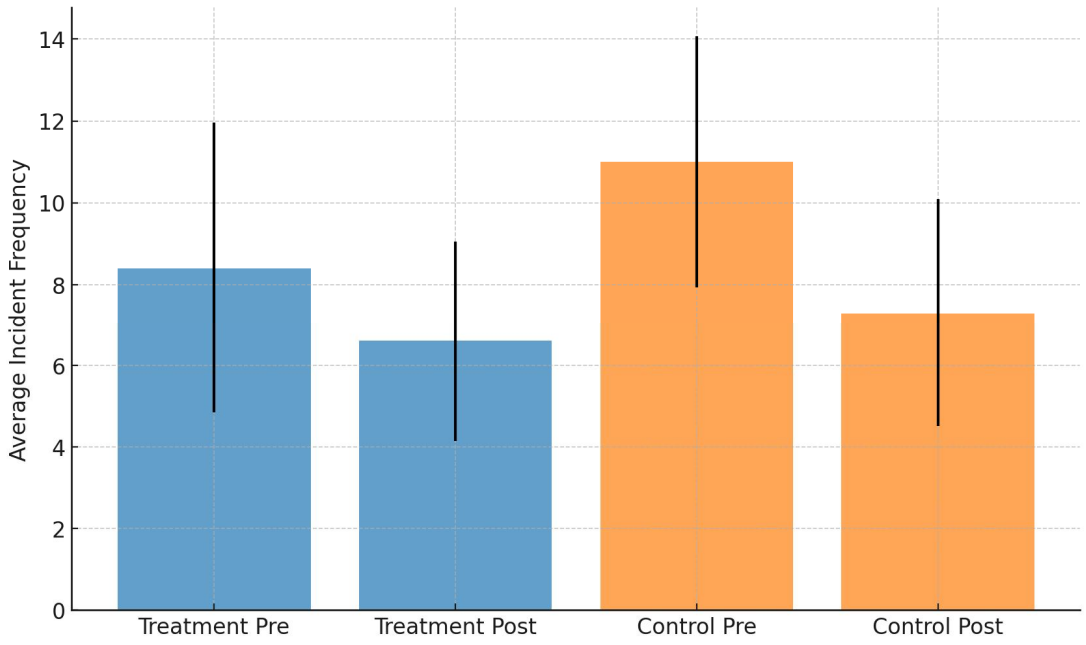

Figure 4. Difference-in-Differences (DiD) Analysis: Incident Frequency for Treatment and Control Groups Across Pre and Post-Intervention Periods.

This evaluation provides evidence supporting these frameworks' continued and enhanced adoption to bolster national cybersecurity resilience.

Analysis of Evolving Cyber Threat Vectors in Critical Infrastructure Sectors

Survival probabilities and economic impacts for each threat were examined to analyze the evolving cyber threat vectors affecting critical infrastructure—specifically Advanced Persistent Threats (APTs), ransomware, and phishing. This analysis assesses resilience duration and financial impact, offering insights for resource prioritization and defence strategies.

Findings are presented in two tables: Survival Analysis (Kaplan-Meier) Results (Table 5) and Economic Impact of Threat Vectors (Table 6). They are accompanied by three visualizations: the Survival Probability Line Plot (Figure 5), the Economic Impact Breakdown by Threat Vector (Figure 6), and the Incident Count vs. Total Economic Impact Scatter Plot (Figure 7).

Survival Analysis of Threat Vectors

Table 5 provides survival probabilities over 10, 30, and 60 days for ransomware, malware, and phishing. Ransomware presents the most immediate risk, with a survival probability of 0.85 at 10 days, dropping to 0.45 at 60 days, indicating that ransomware breaches critical infrastructure systems more quickly. In contrast, malware exhibits

higher resilience with a survival probability of 0.92 at 10 days, declining more gradually to 0.68 at 60 days. Phishing presents a moderate resilience profile, with a survival probability starting at 0.88 at 10 days and decreasing to 0.55 by 60 days.

Threat Vector	Survival Probability (10 days)	Survival Probability (30 days)	Survival Probability (60 days)
Ransomware	0.85	0.65	0.45
Malware	0.92	0.80	0.68
Phishing	0.88	0.72	0.55

Table 5. Survival probabilities For critical infrastructure resilience against various cyber threats.

Figure 5 illustrates survival probabilities across the three threat vectors, visually comparing resilience duration. Ransomware shows the most rapid decline, emphasizing the need for rapid detection and response to mitigate its potential impact. Malware's higher survival probability underscores its longer breach timeline, suggesting a need for persistent monitoring.

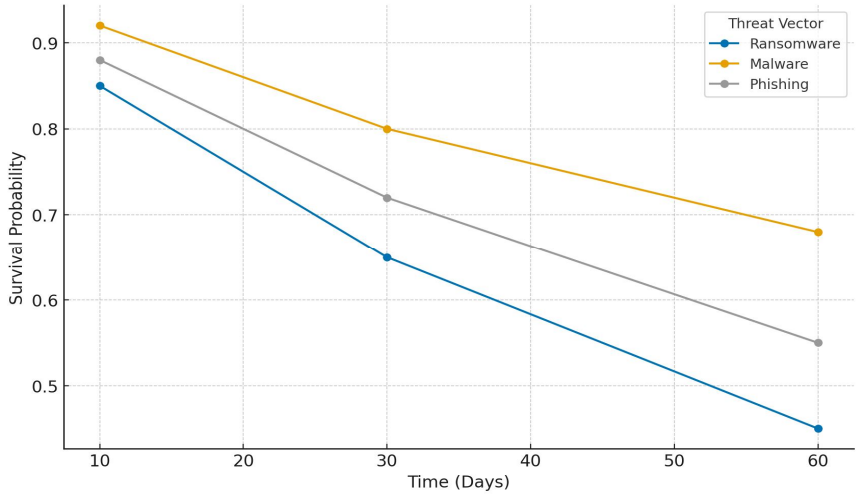

Figure 5. Survival Probability Over Time by Threat Vector.

Economic Impact of Threat Vectors

Table 6 summarises the estimated economic impact of each threat vector, including the number of incidents, recovery costs, lost revenue, and operational disruption costs. Ransomware incurs the highest costs across all categories, with an average recovery

UNDER REVIEW

cost of $540,000 per incident, combined with notable losses in revenue ($220,000) and operational disruptions ($160,000). Phishing presents similar economic impacts, while malware incurs lower costs in each category.

Threat Vector	Incident Count	Recovery Cost ($K)	Lost Revenue ($K)	Operational Disruption Cost ($K)
Ransomware	15	540	220	160
Malware	10	480	190	140
Phishing	12	515	210	155

Table 6. Estimated the economic impact of different threat vectors, highlighting incident frequency and financial implications across recovery, revenue loss, and operational disruption.

Figure 6 presents a breakdown of economic impact by cost type for each threat vector, showing that ransomware's recovery costs dominate its economic footprint. Phishing also incurs high recovery costs, while malware's economic impact is comparatively lower, suggesting a less intensive immediate resource allocation requirement.

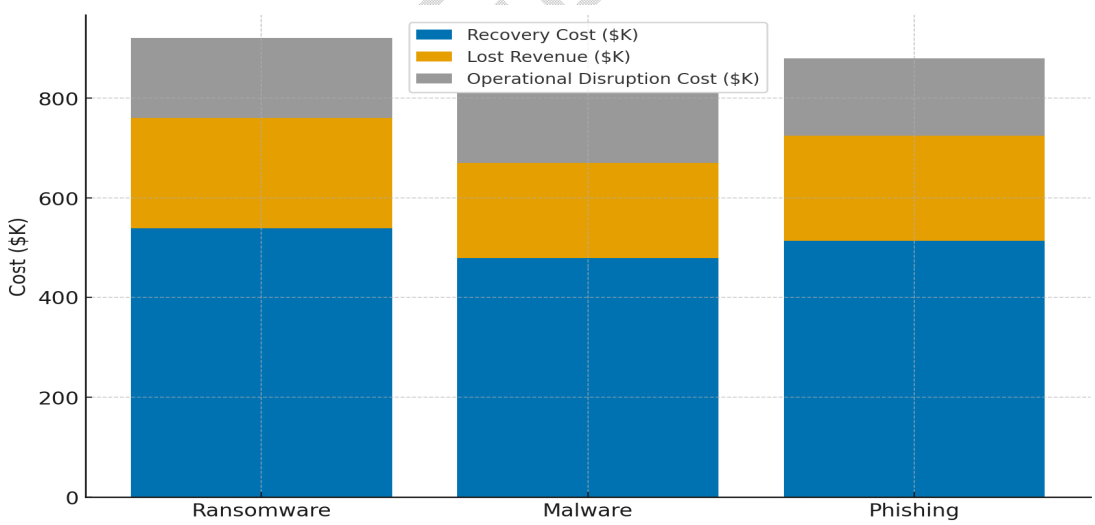

Figure 6. Economic Impact Breakdown by Threat Vector.

Figure 7 visualizes the relationship between incident count and total economic impact for each threat vector. Ransomware's high incident count and substantial economic impact underscore its critical threat status, warranting prioritized defences and resources. With moderate incident count and economic impact, phishing also requires

attention, while malware's lower overall impact may be addressed with ongoing monitoring.

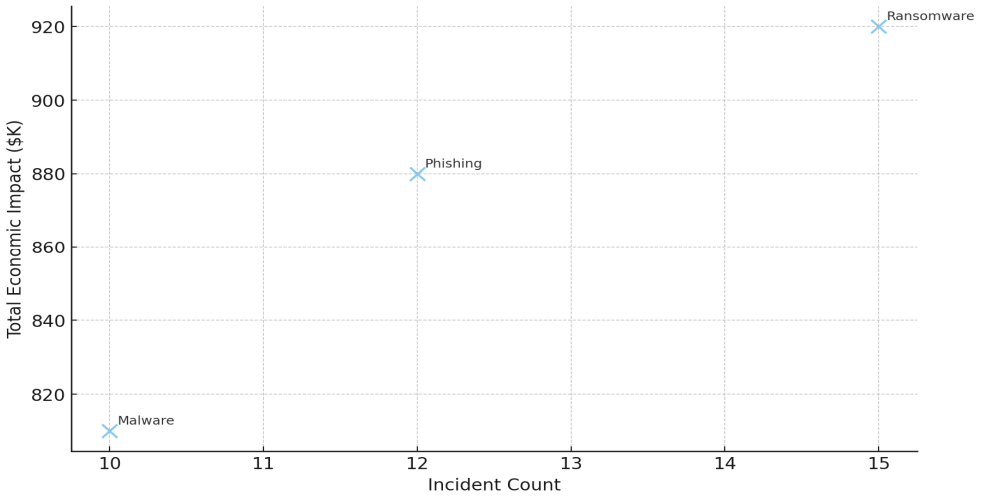

Figure 7. Incident Count vs. Total Economic Impact by Threat Vector.

The findings indicate that ransomware poses the most immediate and financially impactful threat to critical infrastructure sectors, with significant recovery costs and a rapid time to breach. Phishing also represents a considerable threat in terms of economic impact, while malware exhibits a lower impact profile. The combined insights from survival analysis and economic impact data suggest that resources should be allocated in alignment with these threat vectors' specific risk profiles, emphasizing rapid response capabilities for ransomware and moderate defences for phishing and malware. This approach supports a prioritized cybersecurity strategy, enhancing resilience and reducing the economic burden on critical infrastructure.

DISCUSSION

The findings from this study underscore the need for a multidimensional approach to bolstering cybersecurity across U.S. critical infrastructure, as distinct sectors reveal unique vulnerability profiles that affect their exposure to cyber threats. The results on vulnerability prioritization reveal that severity remains a significant determinant of cybersecurity risk, as shown in Table 1, with the odds ratio of 1.027 for severity score indicating a heightened likelihood of incidents in the presence of severe vulnerabilities. Such findings align with existing literature underscoring the criticality of addressing severe vulnerabilities to prevent exploitations (Mallick & Nath, 2024). Interestingly, exploitability exhibits a moderate inverse relationship to incident likelihood, suggesting that sectors have introduced measures to mitigate highly exploitable vulnerabilities. This trend resonates with the containment strategies seen in sectors with legacy systems (George et al., 2024). Further, the age of vulnerabilities proves influential; newer

UNDER PEER REVIEW

vulnerabilities tend to have fewer mitigations in place, exposing sectors to immediate risks. This aligns with current understandings in cybersecurity literature, where more recent vulnerabilities often lack robust countermeasures, leaving systems particularly susceptible to exploitation (Odo, 2024).

The clustering analysis of vulnerability characteristics provides valuable insights, distinguishing between sector-specific and cross-sectoral vulnerabilities (see Table 2). Cluster 1, characterized by moderate age and lower severity, aligns with vulnerabilities that present relatively lower risks across sectors, as observed in foundational infrastructure elements with controlled access points. In contrast, Cluster 2's high-severity, older vulnerabilities highlight a pressing concern for legacy systems, which represent substantial risks despite moderate exploitability. This echoes the findings of previous analyses where older vulnerabilities in core systems persist as high-risk points, requiring strategic intervention to address legacy software weaknesses and longstanding exposure (Makrakis et al., 2021). Cluster 3, displaying the highest severity and most recent age, signals immediate concerns, particularly for sectors like healthcare, where the emergence of high-severity vulnerabilities calls for urgent mitigative strategies, a finding supported by Aljohani's (2022) observations on healthcare sector exposure.

In evaluating the efficacy of current cybersecurity frameworks, the Interrupted Time Series (ITS) and Difference-in-Differences (DiD) analyses show a stronger effect of framework adoption on incident rates. Although the ITS analysis does not indicate a statistically significant decline in incident rates post-intervention, the trend of gradual reduction aligns with frameworks' long-term effects, which aim to build resilience through continual improvement (Table 3). The DiD analysis, however, provides clearer evidence of a framework-related reduction in incidents, with a notable coefficient of -3.7 for the post-intervention period (see Table 4). This differential impact highlights the potential for structured frameworks, like the National Cybersecurity Strategy, to enhance defenses over time, underscoring findings by Zabierek et al. (2021) that emphasize incremental yet sustained impacts on cybersecurity efficacy. Figures 3 and 4 illustrate this impact, showing both the temporal progression of incident reduction and the comparative benefits in sectors adopting these frameworks. This suggests the utility of expanding such frameworks across sectors with less comprehensive protocols (Safitra et al., 2023).

When examining evolving cyber threat vectors, survival analysis reveals the varying resilience durations across ransomware, malware, and phishing attacks, offering a perspective on the immediacy and persistence of these threats (Table 5). Ransomware presents the highest immediate risk, with survival probabilities showing a steep decline within the first 60 days, underscoring the critical need for rapid response capabilities as

UNDER PEER REVIEW

documented by Fitzgerald and Matthew (2022) regarding the swift disruption potential of ransomware attacks. In contrast, malware demonstrates comparatively longer resilience, suggesting that the industry may have developed containment strategies that mitigate rapid breaches, though the persistence of malware remains a concern. Phishing, with moderate resilience, underscores the continued threat of social engineering, as indicated by Riel (2024), who notes the effectiveness of employee training in reducing this vulnerability. The economic analysis further emphasizes ransomware's substantial financial toll, with higher recovery costs and lost revenue across incidents (Table 6). This reflects the urgency observed in recent studies to contain ransomware and reduce financial impact (Vasani et al., 2023). Figures 5, 6, and 7 provide a comprehensive visualization of these findings, highlighting the differential impact of each threat vector on resilience duration and economic costs, with ransomware clearly positioned as the most economically and operationally impactful.

These findings underscore the necessity for targeted cybersecurity strategies tailored to sector-specific vulnerabilities and evolving threat vectors. The evidence reinforces the need for ongoing framework adoption, legacy vulnerability management, and an emphasis on rapid detection and response capabilities, particularly against ransomware. This study's integrated analysis of vulnerability characteristics, framework efficacy, and threat vector impact provides a foundational basis for prioritizing cybersecurity resources, advancing the discourse on infrastructure resilience, and aligning with international best practices, as documented by Strat (2023) and others in this field.

5. CONCLUSION AND RECOMMENDATION

This study highlights cybersecurity vulnerabilities across U.S. critical infrastructure sectors, particularly energy, water, and healthcare. The research reveals that certain vulnerabilities, especially high-severity and recently identified ones, present an immediate risk to system resilience and demand prompt mitigation. Though incremental, the effectiveness of current cybersecurity frameworks shows measurable impact in reducing incidents over time, underscoring the value of structured frameworks and continuous improvement efforts. Additionally, the study emphasizes that ransomware poses the most immediate and financially significant threat, necessitating prioritized responses and resource allocation.

Based on these findings, the recommendations are as follows:

1. The U.S. should strengthen targeted frameworks that focus on mitigating high-severity, recent vulnerabilities, with a particular emphasis on sectors most at risk, such as healthcare.

UNDER PEER REVIEW

2. Cybersecurity frameworks should expand to include proactive resilience measures, such as simulation-based training and advanced threat detection, to address legacy vulnerabilities.

3. Adopting a zero-trust architecture across critical infrastructure sectors can mitigate internal risks, particularly against ransomware.

4. Robust public-private partnerships, with standardized protocols for real-time threat intelligence sharing, should be fostered to enhance incident response capabilities and bolster collective resilience against cyber threats across the critical infrastructure landscape.

UNDER PEER REVIEW

Disclaimer (Artificial intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

REFERENCES

Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D.-E. A., Bajaj, M., Blazek, V., & Prokop, L. (2024). Securing Modern Power Systems: Implementing Comprehensive Strategies to Enhance Resilience and Reliability Against Cyber-Attacks. *Results in Engineering*, *23*, 102647–102647. https://doi.org/10.1016/j.rineng.2024.102647

Adigwe, C. S., Olaniyi, O. O., Olabanji, S. O., Okunleye, O. J., Mayeke, N. R., & Ajayi, S. A. (2024). Forecasting the Future: The Interplay of Artificial Intelligence, Innovation, and Competitiveness and its Effect on the Global Economy. *Asian Journal of Economics, Business and Accounting*, *24*(4), 126–146. https://doi.org/10.9734/ajeba/2024/v24i41269

Akinola, O. I., Olaniyi, O. O., Ogungbemi, O. S., Oladoyinbo, O. B., & Olisa, A. O. (2024). Resilience and Recovery Mechanisms for Software-Defined Networking (SDN) and Cloud Networks. *Journal of Engineering Research and Reports*, *26*(8), 112–134. https://doi.org/10.9734/jerr/2024/v26i81234

AL-Hawamleh, A. (2024). Cyber Resilience Framework: Strengthening Defenses and Enhancing Continuity in Business Security. *International Journal of Computing and Digital Systems*, *15*(1), 1315–1331. https://doi.org/10.12785/ijcds/150193

Al-Mousa, A., Alzaibaq, O., & Hashyeh, Y. (2024). Deep Learning-Based Real-Time Weapon Detection System. *International Journal of Computing and Digital Systems*, *20*, 2210–2142. https://doi.org/10.12785/ijcds/XXXXXX

Aljohani, T. M. (2022). Cyberattacks on Energy Infrastructures: Modern War Weapons. *ArXiv:2208.14225 [Cs]*. https://arxiv.org/abs/2208.14225

Ang, K. W. G. (2022, September 1). *A Case Study for Cyber Incident Report in Industrial Control Systems*. Dspace.mit.edu. https://hdl.handle.net/1721.1/147296

UNDER PEER REVIEW

Arash Mahboubi, Luong, K., Hamed Aboutorab, Hang Thanh Bui, Jarrad, G., Bahutair, M., Seyit Camtepe, Ganna Pogrebna, Ahmed, E., Barry, B., & Gately, H. (2024). Evolving techniques in cyber threat hunting: A systematic review. *Journal of Network and Computer Applications*, 104004–104004. https://doi.org/10.1016/j.jnca.2024.104004

Arigbabu, A. S., Olaniyi, O. O., & Adeola, A. (2024). Exploring Primary School Pupils' Career Aspirations in Ibadan, Nigeria: A Qualitative Approach. *Journal of Education, Society and Behavioural Science*, *37*(3), 1–16. https://doi.org/10.9734/jesbs/2024/v37i31308

Arigbabu, A. T., Olaniyi, O. O., Adigwe, C. S., Adebiyi, O. O., & Ajayi, S. A. (2024). Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale. *Asian Journal of Research in Computer Science*, *17*(5), 85–107. https://doi.org/10.9734/ajrcos/2024/v17i5441

Asonze, C. U., Ogungbemi, O. S., Ezeugwa, F. A., Olisa, A. O., Akinola, O. I., & Olaniyi, O. O. (2024). Evaluating the Trade-offs between Wireless Security and Performance in IoT Networks: A Case Study of Web Applications in AI-Driven Home Appliances. *Journal of Engineering Research and Reports*, *26*(8), 411–432. https://doi.org/10.9734/jerr/2024/v26i81255

Cantelmi, R., Di Gravio, G., & Patriarca, R. (2021). Reviewing qualitative research approaches in the context of critical infrastructure resilience. *Environment Systems and Decisions*, *41*(3), 341–376. https://link.springer.com/article/10.1007/s10669-020-09795-8

Chukwu, E., Adu-Baah, A., Niaz, M., Nwagwu, U., & Chukwu, M. U. (2023). Navigating Ethical Supply Chains: The Intersection of Diplomatic Management and Theological Ethics. *International Journal of Multidisciplinary Sciences and Arts*, *2*(1), 127–139. https://jurnal.itscience.org/index.php/ijmdsa/article/view/2874

Collier, Z. A., & Sarkis, J. (2021). The zero trust supply chain: Managing supply chain risk in the absence of trust. *International Journal of Production Research*, *59*(11), 1–16. https://doi.org/10.1080/00207543.2021.1884311

Daah, C., Qureshi, A., Awan, I., & Konur, S. (2024). Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework. *Electronics*, *13*(5), 865. https://doi.org/10.3390/electronics13050865

Daniel, & Segun, S. (2024). EMERGING TRENDS IN CYBERSECURITY FOR CRITICAL INFRASTRUCTURE PROTECTION: A COMPREHENSIVE REVIEW.

UNDER PEER REVIEW

Computer Science & IT Research Journal, *5*(3), 576–593. https://doi.org/10.51594/csitrj.v5i3.872

Espinosa, V. I., & Pino, A. (2024). E-Government as a Development Strategy: The Case of Estonia. *International Journal of Public Administration*, 1–14. https://doi.org/10.1080/01900692.2024.2316128

Fitzgerald, & Matthew. (2022). *Tactics, Techniques, and Procedures (TTPs) of Ransomware Groups and the Threats Posed to United States National Security - ProQuest*. Www.proquest.com. https://search.proquest.com/openview/a1c2c2ab19921b6dbd43cf2ba343ecba/1?pq-origsite=gscholar&cbl=18750&diss=y

Franchina, L., Inzerilli, G., Scatto, E., Calabrese, A., Lucariello, A., Brutti, G., & Roscioli, P. (2021). Passive and active training approaches for critical infrastructure protection. *International Journal of Disaster Risk Reduction*, *63*, 102461. https://doi.org/10.1016/j.ijdrr.2021.102461

Gbadebo, M. O., Salako, A. O., Selesi-Aina, O., Ogungbemi, O. S., Olateju, O. O., & Olaniyi, O. O. (2024). Augmenting Data Privacy Protocols and Enacting Regulatory Frameworks for Cryptocurrencies via Advanced Blockchain Methodologies and Artificial Intelligence. *Journal of Engineering Research and Reports*, *26*(11), 7–27. https://doi.org/10.9734/jerr/2024/v26i111311

Ge, P., Teng, F., Konstantinou, C., & Hu, S. (2022). A resilience-oriented centralised-to-decentralised framework for networked microgrids management. *Applied Energy*, *308*, 118234. https://doi.org/10.1016/j.apenergy.2021.118234

George, D. A. S., Baskar, D. T., & Srikaanth, D. P. B. (2024). Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors. *Partners Universal International Innovation Journal*, *2*(1), 51–75. https://doi.org/10.5281/zenodo.10639463

Gudala, L., Reddy, A. K., Ashok, & Venkataramanan, S. (2022). Leveraging Biometric Authentication and Blockchain Technology for Enhanced Security in Identity and Access Management Systems. *Journal of Artificial Intelligence Research*, *2*(2), 21–50. https://www.thesciencebrigade.com/JAIR/article/view/250

Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet*, *14*(11). MDPI. https://doi.org/10.3390/fi14110341

UNDER PEER REVIEW

Hardy, A. (2022, July 6). *Securing e-Estonia: Challenges, Insecurities, Opportunities*. Social Science Research Network. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4155377

Hassija, V., Chamola, V., Gupta, V., Jain, S., & Guizani, N. (2020). A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Internet of Things Journal*, *8*(8), 1–1. https://doi.org/10.1109/jiot.2020.3025775

Hazra, A., Adhikari, M., Amgoth, T., & Srirama, S. N. (2023). A Comprehensive Survey on Interoperability for IIoT: Taxonomy, Standards, and Future Directions. *ACM Computing Surveys*, *55*(1), 1–35. https://doi.org/10.1145/3485130

Ibrahim, M. S., & Saber, S. (2023). Machine Learning and Predictive Analytics: Advancing Disease Prevention in Healthcare. *Journal of Contemporary Healthcare Analytics*, *7*(1), 53–71. https://publications.dlpress.org/index.php/jcha/article/view/16

Idengren, P. (2024). *Cybersecurity and The Resilience Measures in Critical Infrastructure in Sweden : A Comparative Desk Study Between Sweden and The United States*. DIVA. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1867013

Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *2*(1), 129–171. https://doi.org/10.60087/jaigs.v2i1.102

Joeaneke, P. C., Kolade, T. M., Val, O. O., Olisa, A. O., Joseph, S. A., & Olaniyi, O. O. (2024). Enhancing Security and Traceability in Aerospace Supply Chains through Block Chain Technology. *Journal of Engineering Research and Reports*, *26*(10), 114–135. https://doi.org/10.9734/jerr/2024/v26i101294

Joeaneke, P. C., Val, O. O., Olaniyi, O. O., Ogungbemi, O. S., Olisa, A. O., & Akinola, O. I. (2024). Protecting Autonomous UAVs from GPS Spoofing and Jamming: A Comparative Analysis of Detection and Mitigation Techniques. *Journal of Engineering Research and Reports*, *26*(10), 71–92. https://doi.org/10.9734/jerr/2024/v26i101291

John-Otumu, A. M., Ikerionwu, C., Olaniyi, O. O., Dokun, O., Eze, U. F., & Nwokonkwo, O. C. (2024). Advancing COVID-19 Prediction with Deep Learning Models: A Review. *2024 International Conference on Science, Engineering and Business*

UNDER PEER REVIEW

for Driving Sustainable Development Goals (SEB4SDG), Omu-Aran, Nigeria, 2024, 1–5. https://doi.org/10.1109/seb4sdg60871.2024.10630186

Joseph, S. A. (2024). Balancing Data Privacy and Compliance in Blockchain-Based Financial Systems. *Journal of Engineering Research and Reports*, *26*(9), 169–189. https://doi.org/10.9734/jerr/2024/v26i91271

Kravchenko, O., Veklych, V., Krykhivskyi, M., & Madryha, T. (2024). Cybersecurity in the face of information warfare and cyberattacks. *Multidisciplinary Science Journal*, *6*, 2024ss0219–2024ss0219. https://doi.org/10.31893/multiscience.2024ss0219

Lanz, Z. (2022). Cybersecurity Risk in U.S. Critical Infrastructure: An Analysis of Publicly Available U.S. Government Alerts and Advisories. *International Journal of Cybersecurity Intelligence & Cybercrime*, *5*(1), 43–70. https://vc.bridgew.edu/ijcic/vol5/iss1/4/

Livier, J. (2024). *The Cyber Policies Behind Critical Infrastructure: A Look at the Preparedness of the Top Nuclear Energy-Producing Nations*. Scholarship @ Claremont. https://scholarship.claremont.edu/cmc_theses/3642/

Maddireddy, B. R., & Maddireddy, B. R. (2020). Proactive Cyber Defense: Utilizing AI for Early Threat Detection and Risk Assessment. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 64–83. https://ijaeti.com/index.php/Journal/article/view/321

Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C., & Benjamin, J. (2021). Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents. *IEEE Access*, *9*, 165295–165325. https://doi.org/10.1109/ACCESS.2021.3133348

Mallick, A., & Nath, R. (2024). *Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments*. https://worldscientificnews.com/wp-content/uploads/2024/01/WSN-1901-2024-1-69-1.pdf

Mitsarakis, K. (2023). Contemporary Cyber Threats to Critical Infrastructures: Management and Countermeasures. *Ihu.edu.gr*. https://repository.ihu.edu.gr//xmlui/handle/11544/30295

Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Journal of Business,*

UNDER PEER REVIEW

Economics and Finance, *10*(3). https://doi.org/10.17261/pressacademia.2023.1807

Modesti, P., Golightly, L., Holmes, L., Opara, C., & Moscini, M. (2024). Bridging the Gap: A Survey and Classification of Research-Informed Ethical Hacking Tools. *Journal of Cybersecurity and Privacy*, *4*(3), 410–448. https://doi.org/10.3390/jcp4030021

Mustyala, A., & Allam, K. (2024). Architecting Resilient Fintech Systems for Fraud Risk Management Using Microservices. *Architecting Resilient Fintech Systems for Fraud Risk Management Using Microservices*. https://doi.org/10.56472/25839233/IJAST-V2I2P108

Nova, K. (2022). Security and Resilience in Sustainable Smart Cities through Cyber Threat Intelligence. *International Journal of Information and Cybersecurity*, *6*(1), 21–42. https://publications.dlpress.org/index.php/ijic/article/view/28

Obi, C., Akagha, V., Onimisi, S., Chigozie, A., None Shedrack Onwusinkwue, & Ibrahim, A. (2024). COMPREHENSIVE REVIEW ON CYBERSECURITY: MODERN THREATS AND ADVANCED DEFENSE STRATEGIES. *Computer Science & IT Research Journal*, *5*(2), 293–310. https://doi.org/10.51594/csitrj.v5i2.758

Odo, C. (2024). Strengthening Cybersecurity Resilience: the Importance of Education, Training, and Risk Management. *Social Science Research Network*. https://doi.org/10.2139/ssrn.4779289

Ogungbemi, O. S., Ezeugwa, F. A., Olaniyi, O. O., Akinola, O. I., & Oladoyinbo, O. B. (2024). Overcoming Remote Workforce Cyber Threats: A Comprehensive Ransomware and Bot Net Defense Strategy Utilizing VPN Networks. *Journal of Engineering Research and Reports*, *26*(8), 161–184. https://doi.org/10.9734/jerr/2024/v26i81237

Okon, S. U., Olateju, O. O., Ogungbemi, O. S., Joseph, S. A., Olisa, A. O., & Olaniyi, O. O. (2024). Incorporating Privacy by Design Principles in the Modification of AI Systems in Preventing Breaches across Multiple Environments, Including Public Cloud, Private Cloud, and On-prem. *Journal of Engineering Research and Reports*, *26*(9), 136–158. https://doi.org/10.9734/jerr/2024/v26i91269

Olabanji, S. O., Marquis, Y. A., Adigwe, C. S., Abidemi, A. S., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection. *Asian Journal of Research in Computer Science*, *17*(3), 57–74. https://doi.org/10.9734/ajrcos/2024/v17i3424

UNDER PEER REVIEW

Oladoyinbo, T. O., Olabanji, S. O., Olaniyi, O. O., Adebiyi, O. O., Okunleye, O. J., & Alao, A. I. (2024). Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics. *Asian Journal of Advanced Research and Reports*, *18*(2), 1–23. https://doi.org/10.9734/ajarr/2024/v18i2601

Perera, S., Jin, X., Maurushat, A., & Opoku, D.-G. J. (2022). Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. *Informatics*, *9*(1), 28. mdpi. https://doi.org/10.3390/informatics9010028

Rakas, S. V. B., Stojanovic, M. D., & Markovic-Petrovic, J. D. (2020). A Review of Research Work on Network-Based SCADA Intrusion Detection Systems. *IEEE Access*, *8*, 93083–93108. https://doi.org/10.1109/access.2020.2994961

Riel, J. F. (2024). *Examining the Implications of a Significant Cyberattack on U.S. Infrastructure*. Encompass. https://encompass.eku.edu/honors_theses/1044/

Rifa, M. (2024). *Challenges to small and medium businesses for cyber threat intelligence sharing*. DIVA. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1866623

Roshanaei, M. (2021). Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. *Journal of Computer and Communications*, *09*(08), 80–102. https://doi.org/10.4236/jcc.2021.98006

Roshanaei, M. (2023). Cybersecurity Preparedness of Critical Infrastructure-A National Review. *Journal of Critical Infrastructure Policy* •, *4*, 2023. https://doi.org/10.18278/jcip.4.1.4

Rossi, M., Minicozzi, G., Pascarella, G., & Capasso, A. (2020). ESG, Competitive advantage and financial performances: a preliminary research. *Handle.net*, 969–986. https://doi.org/manual

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*, *15*(18), 13369. https://doi.org/10.3390/su151813369

Selesi-Aina, O., Obot, N. E., Olisa, A. O., Gbadebo, M. O., Olateju, O. O., & Olaniyi, O. O. (2024). The Future of Work: A Human-centric Approach to AI, Robotics, and Cloud Computing. *Journal of Engineering Research and Reports*, *26*(11), 62–87. https://doi.org/10.9734/jerr/2024/v26i111315

UNDER PEER REVIEW

Skierka, I. (2023). When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis. *Government Information Quarterly*, *40*(1), 101781. https://doi.org/10.1016/j.giq.2022.101781

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions. *Electronics*, *9*(11), 1864. mdpi. https://www.mdpi.com/2079-9292/9/11/1864

Strat, F. E. (2023). Insecurity Unveiled? China and Israel's Use of AI and Mass Surveillance for National Security and Identity. *Dspace.cuni.cz*. https://dspace.cuni.cz/handle/20.500.11956/187326

Syed, F. M., Faiza Kousar E S, & Johnson, E. (2023). AI-Driven Threat Intelligence in Healthcare Cybersecurity. *Revista de Inteligencia Artificial En Medicina*, *14*(1), 431–459. http://redcrevistas.com/index.php/Revista/article/view/145

Tahmasebi, M. (2024). Beyond Defense: Proactive Approaches to Disaster Recovery and Threat Intelligence in Modern Enterprises. *Journal of Information Security*, *15*(2), 106–133. https://doi.org/10.4236/jis.2024.152008

Tsiknas, K., Taketzis, D., Demertzis, K., & Skianis, C. (2021). Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures. *IoT*, *2*(1), 163–186. https://doi.org/10.3390/iot2010009

Vasani, V., Bairwa, A. K., Joshi, S., Pljonkin, A., Kaur, M., & Amoon, M. (2023). Comprehensive Analysis of Advanced Techniques and Vital Tools for Detecting Malware Intrusion. *Electronics*, *12*(20), 4299. https://doi.org/10.3390/electronics12204299

Wallis, T., & Leszczyna, R. (2022). EE-ISAC—Practical Cybersecurity Solution for the Energy Sector. *Energies*, *15*(6), 2170. https://doi.org/10.3390/en15062170

Williams, R. (2020). Surmounting Boundaries: Closing The Governance Gap Governance Arrangements In Public Sector Ict Shared Services. *Open Access Victoria University of Wellington | Te Herenga Waka (Figshare)*. https://doi.org/10.26686/wgtn.17151725.v1

Yaseen, A. (2024). Enhancing Cybersecurity through Automated Infrastructure Management: A Comprehensive Study on Optimizing Security Measures. *Quarterly Journal of Emerging Technologies and Innovations*, *9*(1), 38–60. https://vectoral.org/index.php/QJETI/article/view/68

UNDER PEER REVIEW

Zabierek, L., Bueno, F., Kennis, G., Sady-Kennedy, A., Kanyeka, N., & Kolbe, P. (2021). *P A P E R Toward a Collaborative Cyber Defense and Enhanced Threat Intelligence Structure FOREWORD AND SELECT DISCUSSION BY*. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/8.10.21%20Toward%20a%20Collaborative%20Cyber%20Defense%20and%20Enhanced%20Threat%20Intelligence%20Structure.pdf

UNDER PEER REVIEW