Indian Journal of Science, Technology & Environment (IJSTE)

An International Peer Reviewed, Refereed, Indexed & Quarterly Research Journal of Science, Technology & Environment

**ISSN : 3108-2017(Online)**
**3108-1304(Print)**
**IIFS Impact Factor : 5.875**
Vol.-2; Issue-3(July-Sept.) 2026
Page No.- 29-42

https://ijste.gyanvividha.com

**Author's :**

**Manoj Kumar Patel**
Assistant Teacher, Kashidih, Chandrapur, Chhattisgarh, Ph.D. Scholar, ISBM University, Gariyaband, Raipur, Chhattisgarh, India.

Corresponding Author :

**Manoj Kumar Patel**
Assistant Teacher, Kashidih, Chandrapur, Chhattisgarh, Ph.D. Scholar, ISBM University, Gariyaband, Raipur, Chhattisgarh, India.

# Vulnerability Assessment and Risk Management in Protecting Critical Infrastructure : A Comprehensive Analysis

**Abstract :** The protection of critical infrastructure has emerged as a paramount concern for national security, economic stability, and public safety in an era character-ized by cascading threats, digital transformation, and accumulating vulnerabilities. This research paper examines the evolving landscape of vulnerability assessment and risk management methodologies for critical infrastructure protection, analyzing contemporary frameworks, technolo-gical innovations, and practical implementations. Through examination of recent incidents, including cybersecurity breaches in industrial control systems, natural hazard impacts on energy infrastructure, and the emerging threat of NaTech disasters, this paper evaluates the effectiveness of current approaches and identifies pathways toward enhanced resilience. The research synthesizes findings from European Union policy frameworks, United States government initiatives, and academic research to present a holistic understanding of how vulnerability assessment and risk management must evolve to address interconnected threat landscapes. Key findings indicate that traditional siloed approaches to risk management are insufficient, necessitating integrated frameworks that address the convergence of physical and cyber threats, cross-sectoral dependencies, and the compounding effects of multiple hazards. The paper concludes with recommendations for policymakers, infrastructure operators, and risk manage-ment professionals seeking to enhance critical infra-structure resilience in an increasingly complex risk environment.

**Keywords :** critical infrastructure, vulnerability assess-ment, risk management, resilience, cybersecurity, NaTech disasters, cross-sectoral dependencies.

**1. Introduction ;** Modern societies depend fundamentally on the reliable operation of critical infrastructure-the complex systems of assets, networks, and facilities that

provide essential services including energy, water, transportation, healthcare, and digital communications. Without uninterrupted supplies of electricity, safe drinking water, functional healthcare systems, and predictable transportation networks, the fabric of contemporary life would unravel (European Commission, 2026) . The protection of these vital systems against natural and man-made risks has therefore become a central concern for governments, industry operators, and risk management professionals worldwide.

The Global Risks Report 2026 underscores the urgency of this challenge, identifying critical infrastructure vulnerability as one of the most pressing risks facing business leaders and policymakers. Ageing assets are under increasing strain from extreme weather events, targeted physical attacks, and the growing sophistication of cyber threats. Deferred maintenance, short-term investment horizons, and fragmented responsibility for infrastructure risk have left many organizations vulnerable to disruptions that can reverberate across entire economies (Seach, 2026) .

This paper addresses three central research questions: First, what methodologies and frameworks currently exist for assessing vulnerabilities and managing risks to critical infrastructure? Second, how have recent incidents and technological developments shaped the evolution of these approaches? Third, what integrated strategies can enhance resilience against the compounding and interconnected threats of the contemporary risk landscape?

The research methodology combines analysis of policy documents from the European Union and United States, examination of recent technological innovations in cybersecurity and physical protection, and evaluation of practical implementations through case studies. The paper begins by establishing conceptual foundations, then examines contemporary assessment methodologies, analyzes recent incidents and innovations, and concludes with recommendations for future directions in critical infrastructure protection.

## 2. Conceptual Foundations of Vulnerability Assessment and Risk Management

**2.1 Defining Critical Infrastructure and Resilience :** Critical infrastructure encompasses those assets, systems, and facilities whose disruption or destruction would have a debilitating impact on national security, economic stability, public health, or safety. The European Union's Directive on the Resilience of Critical Entities (CER Directive), which entered into force in January 2023, identifies eleven sectors requiring protection: energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, space, and food production and distribution (European Commission, 2026) . Similarly, United States frameworks recognize sixteen critical infrastructure sectors, demonstrating international consensus on the scope of assets requiring protection.

The concept of resilience has emerged as a central organizing principle in critical infrastructure protection. Unlike traditional approaches focused narrowly on preventing specific threats, resilience encompasses the capacity of infrastructure systems to anticipate, absorb, adapt to, and rapidly recover from disruptive events. This broader orientation acknowledges that despite best efforts at prevention, incidents will occur, and systems must be designed to withstand shocks and maintain essential functions throughout disruption and recovery.

**2.2 Vulnerability Assessment: Purposes and Principles :** Vulnerability assessment constitutes a systematic process for identifying, quantifying, and prioritizing weaknesses in infrastructure systems that could be exploited by threats or exacerbated by hazards. According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), vulnerability assessment involves evaluating potential direct and indirect consequences of incidents, known vulnerabilities to various potential threats or hazards, and general or specific threat information (CISA, n.d.) .

The fundamental purposes of vulnerability assessment include:

1. **Identification:** Discovering specific weaknesses in physical infrastructure, cyber systems, operational procedures, and organizational structures
2. **Quantification:** Measuring the severity and likelihood of potential consequences resulting from vulnerability exploitation
3. **Prioritization:** Establishing which vulnerabilities pose the greatest risks and therefore warrant immediate attention and resource allocation
4. **Communication:** Providing decision-makers with actionable information for risk mitigation investment

Effective vulnerability assessments share common characteristics: they are documented, reproducible, and defensible to ensure transparency and practicality for stakeholders and decision-makers (CISA, n.d.) .

**2.3 The Risk Management Framework :** Risk management for critical infrastructure operates within a structured framework that integrates threat assessment, vulnerability analysis, and consequence evaluation. The fundamental risk equation can be expressed as:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence}$$

Where threat represents the likelihood and nature of potential hazards or attacks, vulnerability reflects the susceptibility of infrastructure to those threats, and consequence captures the magnitude of harm resulting from successful threat exploitation.

This framework supports several essential functions:

- **Risk identification:** Determining which combinations of threats, vulnerabilities, and consequences warrant attention
- **Risk analysis:** Developing qualitative or quantitative understanding of risk magnitudes
- **Risk evaluation:** Comparing analyzed risks against established risk tolerance criteria
- **Risk treatment:** Selecting and implementing measures to modify unacceptable risks

The European Union's approach emphasizes that Member States must adopt national strategies and carry out regular risk assessments to identify entities critical for society and the economy (European Commission, 2026) . Critical entities must then conduct their own risk assessments and implement technical, security, and organizational measures to enhance resilience.

**Figure 1:** The Critical Infrastructure Risk Management Framework

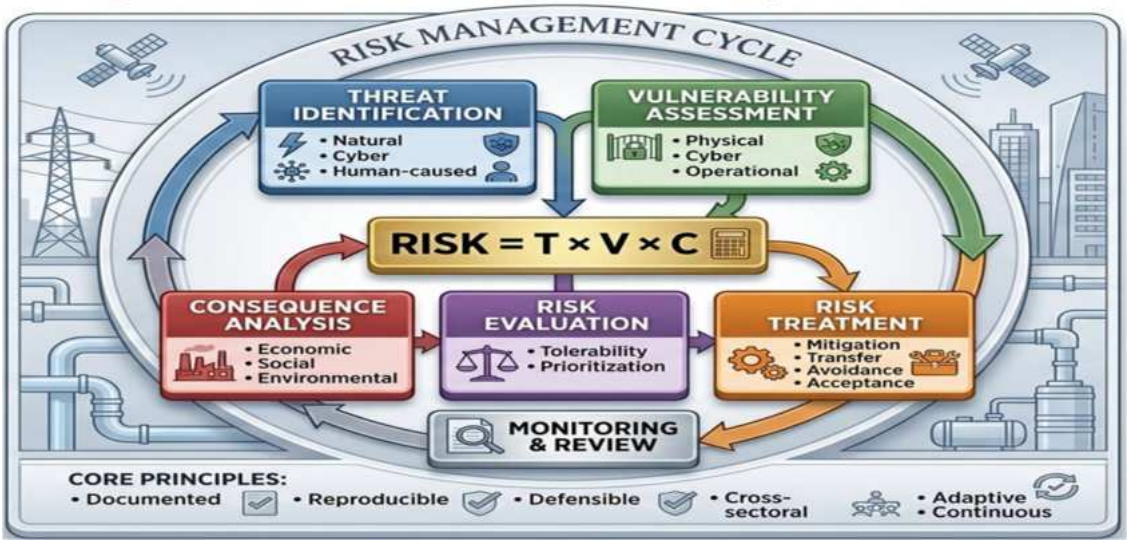



**Fig 1: Critical Infrastructure Risk Management Framework**

## 3. Contemporary Vulnerability Assessment Methodologies

**3.1 Hazard Exposure Analysis :** Hazard exposure analysis identifies critical infrastructure systems and assets located in areas susceptible to natural and man-made hazards. This

methodology typically employs Geographic Information Systems (GIS) for spatial analysis and visualization, enabling quantification of the number, type, and value of critical infrastructure within identified hazard areas (CISA, n.d.) .

Exposure analysis addresses fundamental questions:

- Which infrastructure assets lie within floodplains, earthquake zones, or landslide-prone areas?
- How many critical facilities are exposed to coastal storm surge?
- What infrastructure systems face multiple hazard exposures?

Available tools supporting exposure analysis include USGS seismic hazard maps, NOAA sea level rise viewers, and FEMA flood mapping products (CISA, n.d.) . These resources enable communities and infrastructure operators to understand their hazard landscape and identify assets requiring enhanced protection.

**3.2 Threat and Hazard Scenario Analysis :** Scenario-based methodologies enable infrastructure stakeholders to explore potential impacts across a range of plausible events. FEMA's Threat and Hazard Identification and Risk Assessment (THIRA) process provides guidance for developing risk scenarios based on two factors: the likelihood of a threat or hazard occurring and the consequences of that event if it were to occur (CISA, n.d.) .

Effective scenario development considers events across three likelihood categories:

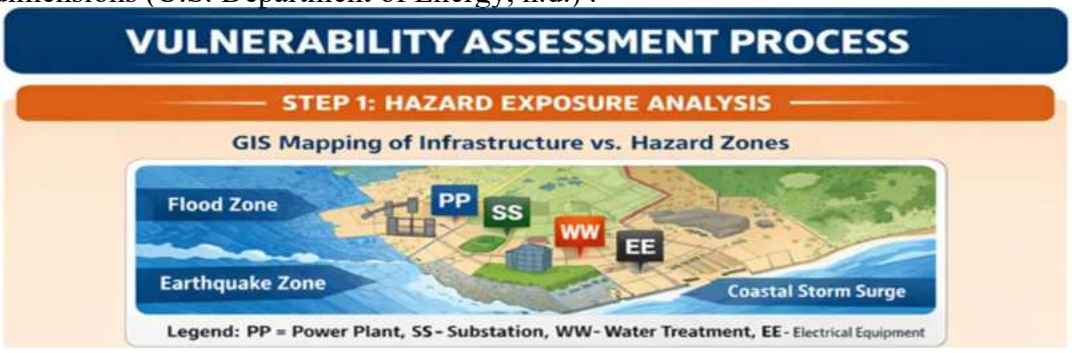
**Table 1: Risk Scenario Likelihood Categories**

| Category | Frequency | Performance Expectation |
|---|---|---|
| Routine | Once every 5 years | Infrastructure remains functional without significant damage |
| Design | Once every 50 years | Minimal damage or disruption as defined by designed performance levels |
| Extreme | Once every 200+ years | Major damage expected but minimal operability maintained |

***Source:*** *Adapted from CISA Risk Assessment Methodologies*

Once developed, scenarios require contextual specification including time, place, and conditions. For example, a hurricane scenario might specify sustained wind speeds, storm surge heights, and precipitation levels, enabling detailed analysis of implications for critical infrastructure systems (CISA, n.d.) .

**3.3 Vulnerability Analysis Techniques :** Vulnerability analysis examines the specific characteristics that make infrastructure susceptible to harm from identified threats and hazards. The U.S. Department of Energy's Vulnerability and Risk Analysis Program (VRAP) has developed and validated methodologies for helping energy-sector organizations identify and understand threats to and vulnerabilities of their infrastructures, addressing both physical and cyber dimensions (U.S. Department of Energy, n.d.) .



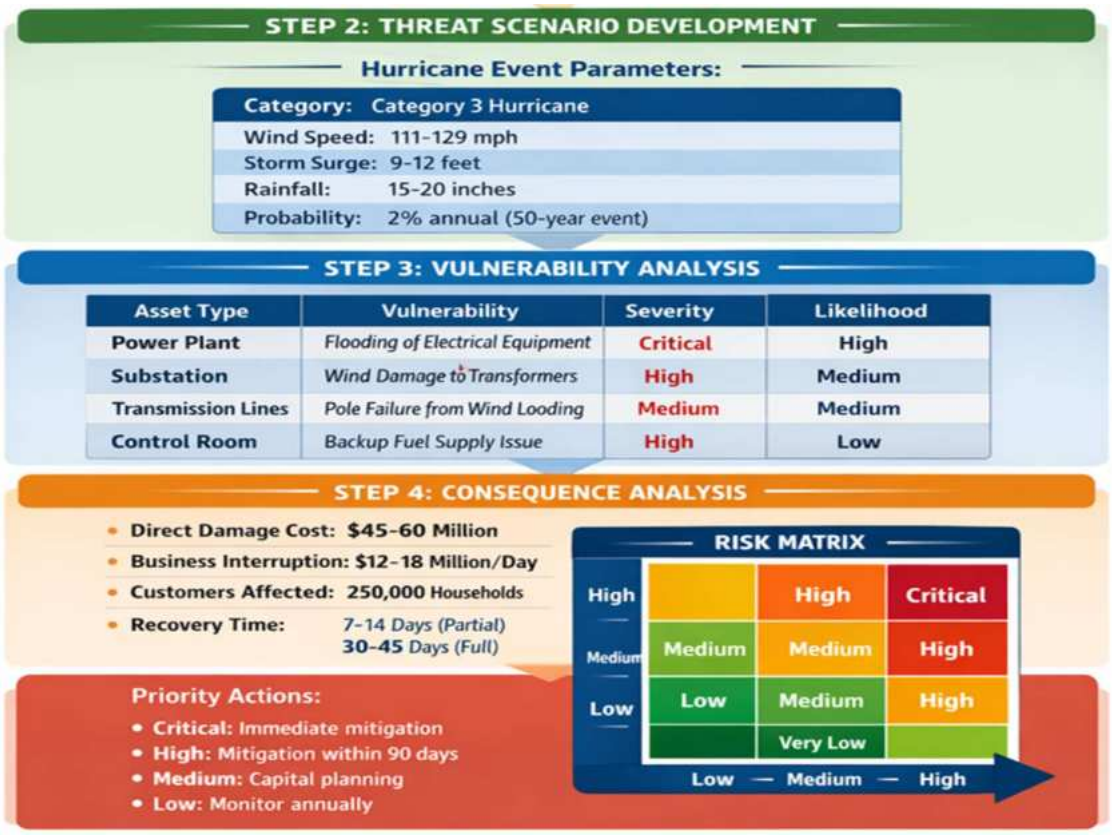



**Fig: Vulnerability assessment process overview**

Key vulnerability analysis approaches include:

**Sector-Specific Assessment Methodologies:** Many critical infrastructure sectors have developed tailored vulnerability assessment frameworks addressing their unique characteristics. These methodologies, documented in Sector-Specific Plans, provide guidance for executing assessments appropriate to each sector's operational context (CISA, n.d.) .

**Infrastructure Survey Tool (IST):** CISA's voluntary, web-based vulnerability survey enables identification and documentation of overall facility security and resilience. The tool produces weighted scores on various factors, displayed graphically in an IST Dashboard that compares data against similar facilities to inform protective measures and resource allocation (CISA, n.d.) .

**Integrated Rapid Visual Screening (IRVS):** Developed by the DHS Science and Technology Directorate, this methodology provides facility-level risk assessment against multiple threats and hazards, incorporating analysis of site characteristics, architecture, building envelope, structural components, mechanical systems, and security features (CISA, n.d.) .

**3.4 Consequence Analysis and Performance Evaluation :** Consequence analysis estimates the potential impacts of infrastructure disruption, including direct physical damage, economic losses, and social consequences. The FEMA HAZUS-MH methodology provides nationally applicable standardized models for estimating potential losses from earthquakes, floods, and hurricanes, using GIS technology to estimate physical, economic, and social impacts (CISA, n.d.) .

The National Institute of Standards and Technology (NIST) Community Resilience Planning Guide (CRPG) offers an approach for evaluating operational capabilities of critical infrastructure systems against established performance goals under various threat scenarios. This methodology emphasizes understanding how long communities can continue operating when services and infrastructure systems are compromised, establishing expected timelines for

operational recovery (CISA, n.d.) .
Performance targets are typically defined at three levels:

- 30% operational capacity: Functions needed to initiate response and recovery activities
- 60% operational capacity: Capacity needed for daily operations to resume at reduced scale
- 90% operational capacity: Normal operating capacity

## 4. Recent Innovations and Technological Developments

**4.1 The Physical Vulnerability Database :** Researchers at Vrije Universiteit Amsterdam, the University of Oxford, and Deltares have developed a comprehensive Physical Vulnerability Database for Critical Infrastructure Hazard Risk Assessments. This database contains fragility and vulnerability curves for evaluating expected or potential damages to infrastructure assets from flooding, earthquakes, windstorms, and landslides (Nirandjan et al., 2024) .
The database consists of three components:

- Summary table: Information on hazard, exposure, and vulnerability characteristics
- Curve collection: Fragility and vulnerability curves for multiple hazard types
- Cost data: Values for estimating asset damages in combination with vulnerability curves

Version 1.1.0, released in October 2024, incorporates improvements and additions including curves from recent research by McKenna et al. (2021), Tsubaki et al. (2016), and Argyroudis et al. (2018) (Nirandjan et al., 2024) . This resource enables more accurate quantification of physical vulnerabilities across multiple hazard types, supporting evidence-based risk management decisions.

**4.2 RADIANT: AI-Powered Cyber Defense for Critical Infrastructure :** Researchers at Texas A&M University's Clean and Resilient Energy Systems (CARES) Laboratory have developed RADIANT (Reactive Autoencoder Defense for Industrial Adversarial Network Threats), a cybersecurity system designed to detect and defend against stealth cyberattacks targeting critical infrastructure such as power grids and water systems (Texas A&M University, 2025) .

Stealth cyberattacks represent a sophisticated class of adversarial threats that disguise malicious activity as legitimate network traffic, making them difficult for both automated detectors and human operators to identify. RADIANT functions as a reactive defense layer that complements existing cybersecurity systems, improving detection capabilities while avoiding the costly retraining typically required by traditional intrusion detection systems (Texas A&M University, 2025) .

According to lead developer Dr. Irfan Khan, RADIANT maintains reliable detection and operator confidence even when attackers attempt to induce machine-learning systems to misclassify malicious activity as normal. The system works by reconstructing incoming data and identifying inconsistencies, filtering out manipulations to enhance accuracy and reduce false alarms (Texas A&M University, 2025) .

Ph.D. student Syed Wali Abbas Rizvi, lead author of the research, describes RADIANT as "deployment oriented," emphasizing its ability to integrate with existing intrusion detection systems in substations, microgrids, and process plants with minimal overhead (Texas A&M University, 2025) .

**4.3 ARIA AZT PROTECT: Industrial Control System Security :** ARIA Cybersecurity's AZT PROTECT solution demonstrates the practical application of advanced cybersecurity for industrial control systems. Deployed at a large U.S. steel producer, the system protects critical production applications from attacks and dangerous unintentional Industrial Control System (ICS) updates (ARIA Cybersecurity, 2025) .

The steel producer's concerns were twofold: attacks penetrating IT defenses into

production OT networks could disrupt steel production, damage equipment, and pose serious risks to worker safety. The mill deployed AZT PROTECT to its critical production infrastructure, implementing an "ICS Lockdown" approach that prevents unauthorized changes to critical systems (ARIA Cybersecurity, 2025) .

The system's value was demonstrated when IT experienced firewall issues that allowed a flood of vendor updates into the OT network before proper firewall rules could be reactivated. AZT PROTECT intercepted these updates and, operating under full ICS lockdown policy, prevented them from executing—keeping protected devices fully operational. The Plant Manager noted that without this protection, the updates could have caused hours of processing time, multiple device reboots, and potential long-term outages if untested updates created issues (ARIA Cybersecurity, 2025) .

**4.4 Liberty Eclipse: Cyber-Physical Exercise Platform :** The U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) sponsors Liberty Eclipse, a full-scale cyber-physical exercise enabling cyber professionals to practice mitigating and responding to cyber attacks using real-world systems (U.S. Department of Energy, 2025) .

The November 2025 exercise hosted over 250 participants from more than 20 organizations, providing a "no-fault environment" where participants experienced real indicators and consequences of cyber attacks without risk to real-world operations. Over six exercise scenarios, participants learned attack methodologies, appropriate response strategies, and self-assessed their cybersecurity measures (U.S. Department of Energy, 2025) .

Liberty Eclipse emphasizes collaboration over competition, bringing together professionals from operational technology (OT), information technology (IT), operations, cybersecurity, and engineering. According to exercise director Brian Marko, "This joint training helps us align internal response strategies and ensure cross-functional teamwork when timeliness is paramount. Such collaboration is critical to building the energy resilience necessary to not only recover from cyber incidents, but to prevent them in the first place" (U.S. Department of Energy, 2025) .

**4.5 HARMONI: Addressing NaTech Disasters :** The HARMONI project, a Horizon Europe initiative running from January 2026 to January 2030, addresses the growing complexity of NaTech (Natural Hazard Triggering Technological) disasters by developing a comprehensive platform to enhance prevention, monitoring, and response for critical infrastructures (Yayan & Yayan, 2026) .

NaTech disasters occur when natural hazards such as earthquakes, floods, or storms trigger technological accidents involving hazardous materials or infrastructure failures. These events pose particular challenges because they combine the unpredictability of natural disasters with the potentially catastrophic consequences of industrial accidents.

The HARMONI platform integrates three functional components:

- **Prevention:** Digital Twins for critical infrastructures enable modeling of cascading effects and worst-case scenarios to inform prevention and mitigation strategies
- **Monitoring:** Advanced remote sensing algorithms, UAV-SAR imaging, and on-site data collection deliver real-time monitoring and early warnings of vulnerabilities
- **Action/Response:** A Hybrid NaTech Decision Assessment (HNDA) integrates federated learning, human expertise, and social science insights to recommend actionable Standard Operating Procedures (SOPs) tailored to evolving disaster scenarios

The project includes six use cases demonstrating technologies in diverse NaTech scenarios, including a cross-border collaboration use case validating interoperability and scalability with existing systems (Yayan & Yayan, 2026) .

## 5. European Union Framework for Critical Infrastructure Resilience

**5.1 The Critical Entities Resilience (CER) Directive :** The European Union has established a comprehensive legislative framework for critical infrastructure protection through the Directive on the Resilience of Critical Entities (CER Directive), which entered into force on 16 January 2023. Member States were required to transpose the Directive into national legislation by 17 October 2024, with full application from 18 October 2024 (European Commission, 2026) .

The CER Directive aims to strengthen critical entity resilience against a range of threats including natural hazards, terrorist attacks, insider threats, sabotage, and public health emergencies. Key requirements include:

1. **National strategies:** Member States must adopt national strategies and carry out regular risk assessments to identify entities critical for society and the economy
2. **Entity-level assessments:** Critical entities must conduct their own risk assessments and implement technical, security, and organizational measures to enhance resilience
3. **Incident notification:** Entities must notify competent authorities of incidents disrupting essential services
4. **Cross-border support:** Entities operating in six or more Member States receive additional advice on meeting obligations
5. **Commission support:** The European Commission provides Union-level overview of cross-border and cross-sectoral risks, best practices, guidance material, and methodologies (European Commission, 2026)

The Directive covers eleven sectors: energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, space, and food production and distribution. A Commission Delegated Regulation establishes a non-exhaustive list of essential services in each sector for use by competent authorities in conducting risk assessments and identifying critical entities (European Commission, 2026) .

The Critical Entities Resilience Group (CERG), established by the Directive, facilitates cooperation among Member States and with the Commission, enabling exchange of information and good practices on resilience issues (European Commission, 2026) .

**5.2 Council Recommendation on Critical Infrastructure Resilience :** In response to acts of sabotage against critical infrastructure in the EU, the Council adopted a Recommendation on a Union-wide coordinated approach to strengthen critical infrastructure resilience on 8 December 2022. Building on the five-point plan for resilient critical infrastructure presented by President von der Leyen in October 2022, the Recommendation addresses three priority areas: preparedness, response, and international cooperation (European Commission, 2026) .

To enhance preparedness, the Recommendation invites Member States to:

- Update risk assessments to reflect current threats
- Conduct stress tests based on common principles and joint scenarios at EU level, beginning with the energy sector

The energy sector stress test was completed by the end of 2023, with outcomes feeding resilience-enhancing cooperation at EU level. The Commission's Protective Security Advisory Missions provide additional support to Member States upon request (European Commission, 2026) .

**5.3 International Cooperation :** The EU-NATO Task Force on resilience of critical infrastructure, launched in 2023, issued an assessment report with recommendations for addressing risks and incidents with significant cross-border relevance. International cooperation priorities include the EU neighborhood in the Western Balkans and Eastern Europe, with particular focus on supporting Ukraine, as well as frequent cooperation with authorities from the

United States and Canada (European Commission, 2026) .

The Council Recommendation on a Blueprint to coordinate response to disruptions of critical infrastructure with significant cross-border relevance establishes actions for improved EU-level coordination, including information sharing, coordination with EU crisis mechanisms, exchanges on public communication approaches, incident reporting, and technical support from other countries or EU institutions to affected Member States (European Commission, 2026) .

**5.4 Implementation Timeline and Guidance**

**Table 2: CER Directive Implementation Milestones**

| Date | Requirement |
|---|---|
| 16 January 2023 | CER Directive enters into force |
| 17 October 2024 | Member States transpose Directive into national legislation |
| 18 October 2024 | Directive applies, replacing European Critical Infrastructure Directive |
| 17 January 2026 | Member States adopt national strategies and complete risk assessments |
| 17 July 2026 | Member States identify critical entities based on risk assessment outcomes |

***Source:*** *European Commission, 2026*

On 11 September 2025, the Commission adopted Guidelines on the identification of critical entities, providing non-binding guidance to EU countries for identifying critical entities in the eleven key sectors. The Guidelines also offer a voluntary template for reporting outcomes of national risk assessments (European Commission, 2026) .

**6. Integration Challenges: The Compounding Risk Landscape**

**6.1 The Interconnected Nature of Contemporary Threats :** The Global Risks Report 2026 signals that the most pressing risks are no longer acting independently but compounding with each other in ways demanding holistic, cross-disciplinary approaches. Three intersecting domains receive particular attention: critical infrastructure vulnerability, the ripple effects of digital transformation, and the destabilizing influence of societal factors such as misinformation and polarization (Seach, 2026) .

Each domain in isolation represents a significant challenge; together, they create a risk environment where losses can quickly escalate, threatening not just individual projects but entire business models. For risk professionals, this means immediate need to reassess exposure to infrastructure failure not only in terms of physical damage but also business interruption and reputation loss (Seach, 2026) .

**6.2 The Convergence of Physical and Cyber Risk :** Digital transformation has revolutionized every aspect of infrastructure operations, unlocking new efficiencies but introducing fresh vulnerabilities. The interconnected nature of modern operations means that a cyber incident can trigger supply chain breakdowns, equipment failures, and cascading financial losses, with impacts reaching far beyond data security (Seach, 2026) .

Increasing reliance on cloud computing, remote operations, and digital communications amplifies the potential consequences of disruption. Cyber risk is now inseparable from physical risk, with operational downtime, asset damage, and regulatory repercussions all possible outcomes from a single event. Boardrooms must expand their horizon scanning to include multi-risk scenarios—for instance, how a ransomware attack might compound the effects of an extreme weather event, paralyzing response systems when they are most needed (Seach, 2026) .

**6.3 Cross-Sectoral Dependencies and Cascading Failures :** Modern infrastructure systems exhibit complex interdependencies that can propagate failures across sectors. The European

Commission emphasizes the importance of developing a Union-level overview of cross-border and cross-sectoral risks, recognizing that disruptions rarely remain contained within a single sector or jurisdiction (European Commission, 2026) .

For example, a cyberattack on an energy utility may disrupt power supply to water treatment facilities, which in turn cannot provide clean water to hospitals, which lose capacity to provide healthcare services. Understanding and modeling these cascading effects requires sophisticated analytical approaches that transcend traditional sector-specific risk assessments.

The HARMONI project's Digital Twin approach addresses this challenge by enabling modeling of cascading effects and worst-case scenarios across interconnected infrastructure systems, supporting more comprehensive risk management strategies (Yayan & Yayan, 2026) .

**6.4 Societal Factors as Risk Amplifiers :** Perhaps the most insidious threat identified in contemporary risk assessments is the impact of societal risks, particularly the rapid spread of misinformation and growing polarization. These trends complicate crisis management and decision-making, disrupt supply chains, and can undermine both public trust and internal morale (Seach, 2026) .

For infrastructure operators, the challenge is anticipating how social unrest, reputational attacks, or breakdowns in communication might amplify the consequences of physical and digital incidents. Proactive communication, clear internal policies, and crisis simulations accounting for misinformation scenarios can strengthen readiness and reduce vulnerability to external shocks (Seach, 2026) .

## 7. Case Studies: Recent Incidents and Lessons Learned

**7.1 Steel Mill Cybersecurity Incident Prevention :** The ARIA Cybersecurity deployment at a large U.S. steel producer provides valuable insights into the practical challenges of protecting industrial control systems. The facility's concerns reflected broader industry anxieties about attacks penetrating IT defenses into production OT networks, potentially disrupting operations, damaging equipment, and endangering workers (ARIA Cybersecurity, 2025) .

The incident that tested the AZT PROTECT system involved firewall lockups in the IT-to-OT network DMZ-a not uncommon problem when complex protection rules cause issues during rule additions. When operators reset firewalls to default mode to achieve recovery, a flood of vendor updates entered the OT network before proper firewall rules could be reactivated (ARIA Cybersecurity, 2025) .

This scenario illustrates several key vulnerabilities:

- **Configuration complexity:** Complex protection rules themselves can create failure modes
- **Recovery procedures:** Emergency recovery actions may create new vulnerabilities
- **Update management:** Unsolicited vendor updates pose significant risks to operational continuity
- **Defense in depth:** Multiple protective layers are essential when primary defenses fail

The AZT PROTECT system's successful intervention—intercepting updates and preventing execution according to ICS lockdown policy—demonstrates the value of host-based protection that remains operational regardless of network perimeter status. The Plant Manager's observation that prevented updates could have caused "a very expensive lost production day" underscores the business case for such investments (ARIA Cybersecurity, 2025) .

**7.2 Liberty Eclipse Exercise Outcomes :** The Liberty Eclipse cyber-physical exercise provides insights into effective approaches for building organizational cyber capabilities. By emphasizing collaboration over competition and bringing together diverse professional communities (OT, IT, operations, cybersecurity, engineering), the exercise addresses the cross-functional coordination essential for effective incident response (U.S. Department of Energy, 2025) .

Key lessons from Liberty Eclipse include:

**The value of realistic training environments:** Using real-world systems in controlled settings enables participants to experience genuine attack consequences without risking actual operations. This "no-fault environment" supports learning and capability building that tabletop exercises cannot provide (U.S. Department of Energy, 2025) .

**Cross-functional integration:** Effective response requires coordinated action across organizational silos. Liberty Eclipse's approach of establishing operations centers with remote staff for prioritized tasks models the real-world coordination needed during actual incidents (U.S. Department of Energy, 2025) .

**Peer learning and mentorship:** The exercise structure provides opportunities for industry participants to mentor others while jointly defending against simulated attacks, building community capabilities alongside individual skills (U.S. Department of Energy, 2025) .

According to Brian Marko, "The lessons learned will shape how utilities across the country and globally prepare for evolving threats" (U.S. Department of Energy, 2025) .

## 8. Recommendations for Enhanced Vulnerability Assessment and Risk Management

**8.1 For Infrastructure Operators :** Prioritize resilience of core assets: Undertake regular, cross-disciplinary assessments of infrastructure exposures, ensuring that maintenance and upgrade programs are central to business planning. Deferred maintenance and short-term investment horizons create accumulating vulnerabilities that manifest during stress events (Seach, 2026) .

**Strengthen scenario planning:** Move beyond single-risk frameworks by developing horizon scanning that considers multiple risk interactions. Use workshops and simulations to stress-test contingency plans against compound scenarios combining cyber, physical, and societal threats (Seach, 2026) .

**Foster cross-functional collaboration:** Break down internal silos between IT, OT, operations, engineering, and risk management. Engage suppliers, insurers, and public authorities to share information and coordinate on risk management strategies (Seach, 2026) .

**Invest in layered defense:** The steel mill case study demonstrates that network perimeter protection alone is insufficient. Implement host-based protection systems like RADIANT or AZT PROTECT that remain operational when network defenses fail (Texas A&M University, 2025; ARIA Cybersecurity, 2025) .

**8.2 For Policymakers and Regulators :** Support vulnerability data infrastructure: The Physical Vulnerability Database developed by Nirandjan et al. (2024) demonstrates the value of systematic vulnerability data collection and sharing. Policymakers should support continued development and maintenance of such resources .

**Promote cross-border coordination:** The EU's Critical Entities Resilience Group and EU-NATO Task Force provide models for international cooperation that should be expanded and deepened (European Commission, 2026) .

**Fund research and development:** Continued investment in innovative approaches like HARMONI's NaTech platform, RADIANT's AI-powered detection, and Liberty Eclipse's exercise capabilities is essential for staying ahead of evolving threats (Yayan & Yayan, 2026; Texas A&M University, 2025; U.S. Department of Energy, 2025) .

**Establish performance expectations:** Clear performance goals across routine, design, and extreme event categories, as outlined in CISA guidance, enable consistent assessment and improvement of infrastructure resilience (CISA, n.d.) .

**8.3 For Risk Management Professionals :** Expand risk assessment scope: Move beyond traditional hazard lists to consider compound scenarios where multiple risks interact. Evaluate

potential insurance coverage gaps related to risk interdependencies (Seach, 2026) .

**Integrate reputational risk:** Monitor public sentiment and stakeholder engagement, integrating reputational risk into broader resilience planning. Proactive communication and crisis simulations accounting for misinformation scenarios can reduce vulnerability to external shocks (Seach, 2026) .

**Leverage quantitative tools:** Utilize resources like the Physical Vulnerability Database to move from qualitative to quantitative vulnerability assessments, supporting evidence-based resource allocation decisions (Nirandjan et al., 2024) .

**Promote boardroom engagement:** Boards should devote agenda time to long-term risk trends, focusing on systemic exposures and risk accumulation potential, supported by up-to-date analytics and regular reporting from risk teams (Seach, 2026) .

**9. Conclusion :** Vulnerability assessment and risk management for critical infrastructure stand at a critical juncture. The threat landscape has evolved dramatically from the relatively bounded concerns of previous decades to encompass compounding hazards, converging physical and cyber threats, and cascading failures across interconnected systems. Ageing infrastructure assets face increasing strain from extreme weather events, sophisticated cyberattacks, and emerging NaTech disasters, while deferred maintenance and fragmented responsibility compound these vulnerabilities.

The response to this challenge must be equally transformative. Traditional siloed approaches to risk management are no longer sufficient. Instead, integrated frameworks must address the full spectrum of threats while accounting for interdependencies across sectors and the amplifying effects of societal factors like misinformation and polarization.

Encouragingly, significant progress is evident across multiple fronts. Policy frameworks such as the EU's CER Directive establish comprehensive requirements for national strategies, entity-level assessments, and cross-border cooperation. Technological innovations including RADIANT's AI-powered detection, AZT PROTECT's ICS lockdown capabilities, and HARMONI's NaTech platform demonstrate the potential of advanced tools to enhance protection. Methodological advances like the Physical Vulnerability Database provide quantitative foundations for evidence-based risk management.

The path forward requires sustained commitment from all stakeholders. Infrastructure operators must prioritize resilience through regular assessments, cross-functional collaboration, and layered defenses. Policymakers must support vulnerability data infrastructure, promote international cooperation, and fund continued research and development. Risk management professionals must expand assessment scope, integrate reputational considerations, leverage quantitative tools, and promote boardroom engagement with long-term risk trends.

The stakes could not be higher. Without reliable energy supplies, safe drinking water, functional healthcare, and predictable transportation, modern societies cannot function. Ensuring the resilience of critical infrastructure against contemporary and emerging threats is not merely a technical challenge but a fundamental requirement for societal well-being and economic prosperity. The frameworks, tools, and approaches examined in this paper provide foundations for meeting that challenge-but their effective implementation requires sustained commitment, collaboration, and investment from all those responsible for the infrastructure upon which we all depend.

**References :**

1. ARIA Cybersecurity. (2025, August 12). *ARIA Cybersecurity Protects Large US Steel Mills from Cyberattacks*. Nasdaq.

2. CISA (Cybersecurity and Infrastructure Security Agency). (n.d.). *Risk Assessment Methodologies: An Infrastructure Resilience Planning Framework (IRPF) Resource*. U.S. Department of Homeland Security.
3. European Commission. (2026, January 13). *Critical infrastructure resilience at EU-level*. Migration and Home Affairs.
4. Nirandjan, S., Koks, E. E., Ye, M., Pant, R., van Ginkel, K. C. H., Aerts, J. C. J. H., & Ward, P. J. (2024). *Physical Vulnerability Database for Critical Infrastructure Hazard Risk Assessments* (Version V1.1.0) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.13889558
5. Seach, P. (2026, February 6). *Global Risks Report 2026: An urgent call for boardroom action on property, infrastructure and operational resilience*. Airmic / Zurich Insurance Group.
6. Texas A&M University. (2025, October 23). *Texas A&M Researchers Develop Cyber Defense System for Critical Infrastructure*. Security Info Watch.
7. U.S. Department of Energy. (2025, November 26). *Powering Resilience: How CESER's Liberty Eclipse Safeguards the Nation's Energy Infrastructure*. Office of Cybersecurity, Energy Security, and Emergency Response.
8. U.S. Department of Energy. (n.d.). *Vulnerability Assessment Methodology Report*. Office of Critical Infrastructure Protection.
9. Yayan, U., & Yayan, K. (2026). *HARMONI – Hazard Assessment and Risk Management of NaTech Emergencies with Cross-Collaboration Opportunities*. UFUK AVRUPA Projesi, Horizon Europe
10. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley.
11. Bodeau, D., Graubart, R., & Fabius-Greene, J. (2019). *Cyber Resiliency Engineering Framework*. MITRE Corporation.
12. Boyes, H., Isbell, R., & Watson, T. (2015). Critical infrastructure cybersecurity: Problems and solutions. *International Journal of Critical Infrastructure Protection*, 8, 34–40.
13. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, 56, 1–27.
14. ENISA. (2023). *Threat Landscape for Critical Infrastructure*. European Union Agency for Cybersecurity.
15. Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 19(1), 33–56.
16. ISO. (2022). *ISO/IEC 27005: Information Security Risk Management*. International Organization for Standardization.
17. Kott, A., & Linkov, I. (2019). *Cyber Resilience of Systems and Networks*. Springer.
18. Krutz, R. L. (2017). *Computer Security: Principles and Practice*. Pearson.
19. Landoll, D. (2016). *The Security Risk Assessment Handbook*. CRC Press.
20. Linkov, I., & Trump, B. D. (2019). *The Science and Practice of Resilience*. Springer.
21. National Institute of Standards and Technology (NIST). (2023). *Framework for Improving Critical Infrastructure Cybersecurity*. NIST.
22. NIST. (2020). *Guide for Conducting Risk Assessments (SP 800-30)*. National Institute of Standards and Technology.
23. NIST. (2022). *Security and Privacy Controls for Information Systems (SP 800-53)*.
24. North Atlantic Treaty Organization (NATO). (2021). *Cyber Defence and Resilience Strategy*. NATO Cooperative Cyber Defence Centre of Excellence.

25. Perrow, C. (2011). *Normal Accidents: Living with High-Risk Technologies*. Princeton University Press.
26. Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), 11–25.
27. Ross, R., McEvilley, M., & Oren, J. (2014). *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. NIST.
28. Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton.
29. Stallings, W. (2018). *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Addison-Wesley.
30. Ten, C. W., Liu, C. C., & Govindarasu, M. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, 23(4), 1836–1846.
31. The World Bank. (2022). *Cybersecurity and Critical Infrastructure Protection*. World Bank Publications.
32. United Nations Office for Disaster Risk Reduction (UNDRR). (2021). *Global Assessment Report on Disaster Risk Reduction*.
33. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102.
34. World Economic Forum. (2024). *Global Cybersecurity Outlook*. World Economic Forum.
35. Zio, E. (2016). *Challenges in the Vulnerability and Risk Analysis of Critical Infrastructure Systems*. Reliability Engineering & System Safety, 152, 137–150.

•