American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

Article

NATIONAL RESILIENCE THROUGH AI-DRIVEN DATA ANALYTICS AND CYBERSECURITY FOR REAL-TIME CRISIS RESPONSE AND INFRASTRUCTURE PROTECTION

Abdul Awal Mintoo[1]; Abu Saleh Muhammad Saimon[2]; Mohammed Majid Bakhsh[3]; Marjina Akter[4]

[1] *MBA, University of Dhaka, Bangladesh*
Email: mintoo.hr@gmail.com

[2] *School of Computer and Information Sciences, Washington University of Science and Technology, USA*
Email: asm.saimon@gmail.com

[3] *BBA, North South University, Dhaka, Bangladesh*
Email: mohammedmajidb@gmail.com

[4] *Master of Business Administration in Accounting and Information Systems, Noakhali Science and Technology University, Bangladesh*
E-mail: marjinapriyanka@gmail.com

Citation:
Mintoo, A. A., Saimon, A. S. M., Bakhsh, M. M., & Akter, M. (2022). *National resilience through AI-driven data analytics and cybersecurity for real-time crisis response and infrastructure protection*. *American Journal of Scholarly Research and Innovation, 1*(1), 137–169. https://doi.org/10.63125/sdz8km60

Received:
January 6, 2022

Revised:
February 10, 2022

Accepted:
February 24, 2022

Published:
March 1, 2022

ABSTRACT

This study investigates the integration of artificial intelligence (AI) and cybersecurity frameworks in enhancing national resilience through real-time crisis response and critical infrastructure protection. Employing a qualitative case study approach, the research examines twelve carefully selected national and sectoral implementations across diverse contexts, including public health emergencies, smart grid monitoring, intelligent transportation systems, water management, and cyber-physical infrastructure defense. The study reveals that AI-driven data analytics significantly improve early warning capabilities, situational awareness, and decision-making speed in high-risk scenarios. It also demonstrates that the adoption of AI-enhanced cybersecurity tools—such as anomaly detection, behavioral analytics, and autonomous incident response—plays a crucial role in securing digital infrastructure against evolving cyber threats. Furthermore, the application of simulation models and digital twins was found to support real-time modeling, predictive planning, and operational testing, thereby strengthening the adaptability of critical systems. Multi-agent decision support systems and explainable AI interfaces facilitated better interagency coordination and user trust, while zero-trust architectures enabled granular control over access and threat containment. Despite these advancements, the study identified notable gaps in methodological integration, sectoral coverage (particularly in education and water sanitation), and inclusive system design. The findings emphasize the importance of interdisciplinary collaboration and governance alignment in developing comprehensive AI and cybersecurity strategies for national resilience. By synthesizing empirical evidence from twelve cross-sectoral case studies, this research contributes actionable insights into the design and implementation of intelligent, secure, and adaptive infrastructure systems in an era of complex and interconnected global threats.

KEYWORDS

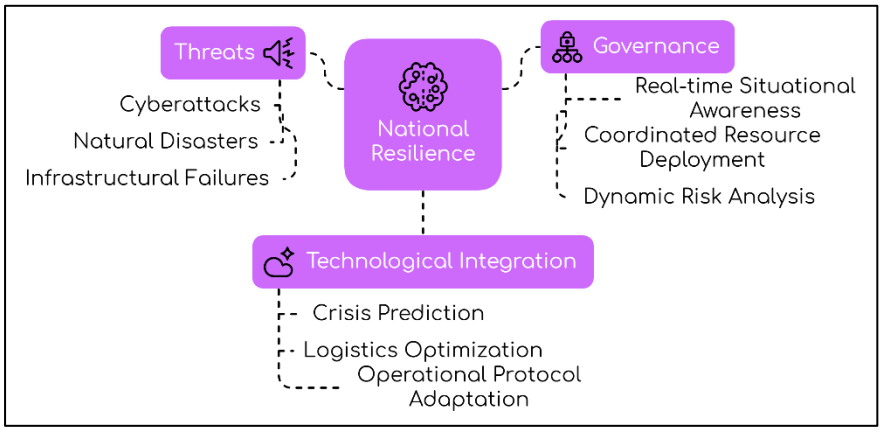
National Resilience; AI-Driven Data Analytics; Cybersecurity; Crisis Response; Critical Infrastructure Protection;

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

INTRODUCTION

National resilience is fundamentally rooted in a state's capacity to anticipate, absorb, and recover from a broad spectrum of threats, including cyberattacks, natural disasters, and infrastructural failures (Rød et al., 2017) . It is inherently tied to systems-level governance, cross-sectoral integration, and the ability to synthesize high-volume data for operational decision-making (Bruneau et al., 2003). Traditional approaches to crisis management, largely reactive and linear, have proven insufficient in the face of highly complex, fast-evolving disruptions such as pandemics and cyberterrorism (Masys et al., 2014). Real-time situational awareness, coordinated resource deployment, and dynamic risk analysis have become foundational to modern emergency management (Dubey et al., 2022). Large-scale infrastructure networks, including transportation, energy grids, communication channels, and water systems, are increasingly targeted due to their interdependence and criticality (Caralli et al., 2012). National resilience, therefore, must evolve beyond institutional readiness into a technologically augmented ecosystem in which intelligence, foresight, and control are digitally embedded. Central to this transformation is the deployment of artificial intelligence (AI) and data analytics tools capable of interpreting vast information flows for crisis prediction and response (Caralli et al., 2012; Masys et al., 2014). Through AI-driven automation, governments and crisis management authorities can initiate early warning mechanisms, optimize logistics, and adapt operational protocols based on real-time inputs (Rød et al., 2017; Scholten et al., 2014). This systemic integration offers a paradigm shift, positioning digital capabilities as core enablers of national resilience.

Figure 1: Enhancing National Resilience through AI and Data



Artificial intelligence enables the automation of pattern recognition, anomaly detection, and forecasting by extracting insights from large, heterogeneous data sources (Masys et al., 2014; Wisco et al., 2017). Within emergency management, AI algorithms have been used to track disease outbreaks (Thompson et al., 2016), forecast wildfires (Mohanty et al., 2020), and analyze social media for disaster signals (Jung et al., 2020). Natural language processing (NLP), computer vision, and time-series analysis allow for rapid assimilation of unstructured data, including videos, tweets, and emergency calls (Kerner & Thomas, 2014). Through these methods, emergency responders can monitor crowd sentiment, assess damage levels, and identify hazardous zones in real time (Petersen et al., 2020). Machine learning models trained on historical disaster datasets can dynamically predict flooding, infrastructure collapse, or mass evacuations (Petit et al., 2013). This predictive intelligence reduces decision latency and enhances response coordination across local and national agencies (Kerner & Thomas, 2014). Furthermore, AI-facilitated data fusion can integrate weather reports, IoT sensor outputs, and drone surveillance into a common operating picture, allowing responders to prioritize actions based on data-informed threat assessments (Bhamra et al., 2011). Through operational dashboards and visual analytics, command centers can track unfolding scenarios, allocate resources, and communicate risk levels to multiple stakeholders simultaneously (Petit et al., 2013). The synergy between AI analytics and crisis response represents an institutional innovation in managing unpredictable, high-impact events.

Cybersecurity is an essential dimension of national resilience, particularly given the digitization of public utilities, defense systems, and emergency services (Barrett et al., 2017). As cyber-physical systems grow in complexity and connectivity, they become attractive targets for malicious actors

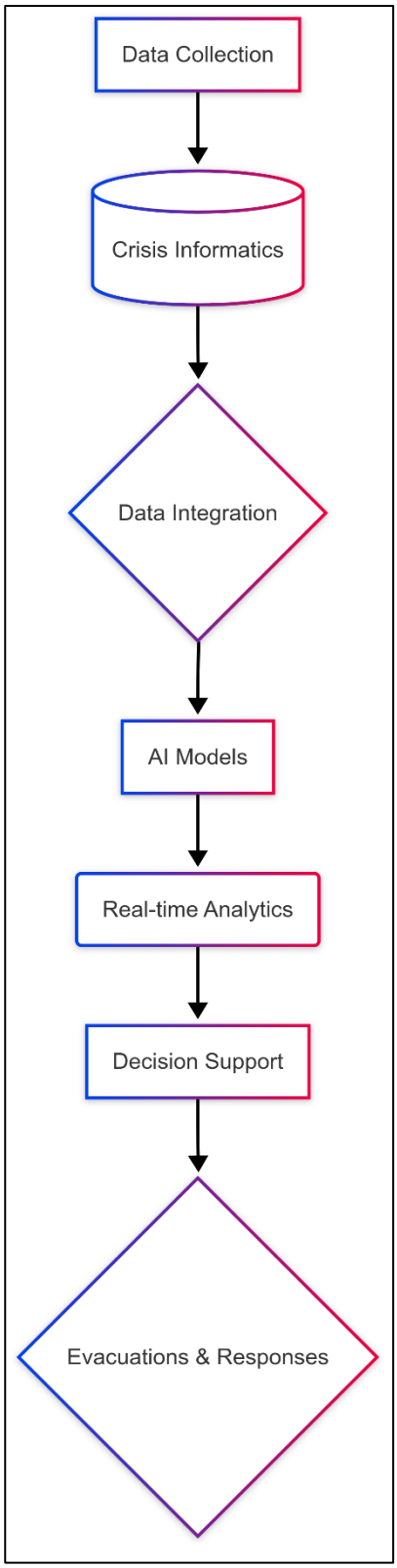
American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

seeking to exploit vulnerabilities for political or economic disruption (Kulugh et al., 2022). AI-enhanced cybersecurity provides defensive and proactive measures such as real-time threat detection, automated incident response, and behavior-based intrusion prevention (Li et al., 2022). Machine learning classifiers trained on network traffic data can detect zero-day attacks and anomalous behavior patterns with greater speed and accuracy than traditional signature-based systems (Abazi, 2022). Deep learning models, including convolutional and recurrent neural networks, offer improved detection capabilities in high-volume data environments (Aliyu et al., 2020). Cyber threat intelligence sharing between institutions, supported by AI-based knowledge graphs, enables coordinated responses to multi-vector attacks on infrastructure such as power grids and communication networks (Mueller, 2017). Moreover, real-time AI systems can autonomously patch vulnerabilities, redirect malicious traffic, and isolate compromised assets before damage escalates (Schackelford, 2016). In a resilience context, such capabilities are critical not only for defense but also for the continuity of operations during systemic shocks (AlDaajeh et al., 2022). National cybersecurity strategy must integrate AI not just for perimeter protection but also for adaptive resilience in cyber-crisis scenarios.

AI applications in national resilience are magnified through integration with big data infrastructures and crisis informatics (Abazi, 2022). Crisis informatics entails the collection, processing, and application of data from both official and informal sources during emergencies (Aliyu et al., 2020). This integration supports the rapid mobilization of cross-agency efforts by aligning heterogeneous data into structured intelligence products (Mueller, 2017). Cloud computing, edge analytics, and distributed data architectures support low-latency, high-throughput processing essential for dynamic crisis conditions (Schackelford, 2016). AI models trained on multimodal datasets can synthesize inputs from seismic sensors, drone footage, user-reported data, and meteorological systems, yielding actionable intelligence for national disaster centers (Agyepong et al., 2019). Real-time analytics platforms can visually map population displacements, infrastructure damage, and available resources across large territories (Radanliev, De Roure, Page, et al., 2020). Decision-makers equipped with predictive dashboards can preemptively evacuate areas, reroute transportation systems, and activate medical response units (Barrett et al., 2017). This decision support, grounded in AI-enabled big data analytics, is foundational in multi-hazard resilience planning, offering high fidelity, location-based crisis intelligence (Kulugh et al., 2022). The convergence of AI and big data informs an operational intelligence layer that strengthens national crisis governance capabilities.

Critical infrastructure sectors—including energy, transportation, healthcare, and water systems—require continuous protection from cascading failures that may arise from cyberattacks,

Figure 2: AI-Driven National Resilience Workflow



American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

natural hazards, or operational disruptions (Li et al., 2022). AI technologies facilitate condition monitoring, failure prediction, and adaptive control in such infrastructures (Abazi, 2022). Smart grid systems use machine learning for load forecasting, fault localization, and energy distribution optimization, enhancing grid reliability (Aliyu et al., 2020). In water management, AI models detect leakage, contamination, and abnormal consumption patterns to mitigate service disruption (Mueller, 2017). Transportation systems benefit from AI-based traffic monitoring, incident detection, and route optimization, ensuring logistical continuity during emergencies (Schackelford, 2016). Digital twins—virtual replicas of physical systems—enhanced by AI and IoT, allow infrastructure managers to simulate stress scenarios and adjust operations in real time (Tao et al., 2019). Infrastructure interdependencies, such as energy requirements for data centers or water supplies for cooling systems, are modeled through AI-driven simulations to identify systemic vulnerabilities (Glaessgen & Stargel, 2012). Through sensor integration, anomaly detection, and digital risk modeling, AI serves as a guardian layer in maintaining national infrastructure resilience. National resilience is contingent not only on individual system readiness but also on seamless coordination among diverse actors across public, private, and military sectors (Fan et al., 2021). AI systems, embedded within interoperable platforms, facilitate this coordination by ensuring data sharing, collaborative intelligence, and synchronization of action (Schroeder et al., 2021). Emergency communication systems augmented by AI prioritize and route critical messages, reducing response times (Carlson et al., 2012). Blockchain technology combined with AI is being explored to verify data integrity in real-time information sharing between hospitals, law enforcement, and emergency responders (Vanajakumari et al., 2016). Interoperability standards supported by AI-driven translation algorithms reduce information silos and enhance collaboration during crises (Masys et al., 2014). Real-time dashboards aggregating sensor data, citizen reports, and agency directives enable a shared operational picture (Pescaroli et al., 2018). Public-private partnerships built on AI platforms help mobilize logistics, personnel, and medical supplies during prolonged disruptions (L'Hermitte et al., 2016). Through reinforcement learning and scenario modeling, AI systems optimize multi-agency coordination plans under resource-constrained conditions (Pescaroli et al., 2018). These capacities underscore the role of AI as a synchronizing mechanism in national resilience architectures. The main objective of this study is to critically examine the role of artificial intelligence (AI)-driven data analytics and cybersecurity in enhancing national resilience, particularly in the context of real-time crisis response and the protection of critical infrastructure. This research seeks to identify and synthesize empirical evidence and applied methodologies where AI technologies have been implemented to support emergency preparedness, multi-agency coordination, infrastructure monitoring, and adaptive threat management. By analyzing cross-disciplinary literature and case-based applications, the study aims to construct a conceptual framework that illustrates the convergence of AI, big data, and cybersecurity within national emergency management systems. Another objective is to highlight the extent to which machine learning algorithms, predictive models, and automated decision-support systems contribute to early warning capabilities and operational agility. Furthermore, the study explores how AI-enhanced cybersecurity mechanisms can detect, prevent, and mitigate cyber-physical disruptions to national assets. A key aim is to understand the interoperability challenges and governance models required to enable effective AI integration across public and private domains. Ultimately, this research intends to offer actionable insights and a comprehensive synthesis of knowledge to inform policy, design, and deployment strategies that strengthen the digital backbone of national resilience systems.

LITERATURE REVIEW

The intersection of artificial intelligence (AI), data analytics, and cybersecurity in the context of national resilience has become a focal point of contemporary research, driven by the increasing complexity of systemic risks and the demand for real-time response mechanisms. The literature reflects a growing recognition that national resilience is no longer solely reliant on institutional preparedness or manual protocols but is increasingly dependent on the deployment of intelligent systems capable of interpreting large datasets, forecasting threats, and automating protective responses. Scholars have explored the application of AI across various stages of crisis

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

management, from risk assessment and early warning systems to real-time decision-making and post-disaster recovery. Simultaneously, the role of cybersecurity in protecting critical digital and physical infrastructure has expanded, with studies examining the convergence of AI-based intrusion detection systems, behavioral analytics, and autonomous response mechanisms. While much of the existing scholarship provides valuable insights into individual components—such as smart infrastructure, emergency communication, and predictive modeling—there is a noticeable gap in integrative frameworks that unify AI, big data analytics, and cybersecurity under a comprehensive resilience architecture. This literature review aims to bridge this gap by synthesizing multidisciplinary studies that address AI-driven innovations and cybersecurity approaches in strengthening national resilience. It draws upon empirical findings, conceptual models, and case-based research from emergency management, computer science, systems engineering, and public administration. The review also categorizes the scholarly contributions based on their relevance to critical functions, such as infrastructure protection, cross-sectoral coordination, real-time data analysis, and cyber-physical security. By organizing the literature thematically and contextually, this section sets the foundation for evaluating how AI and cybersecurity converge to support resilient, responsive, and adaptive national systems under high-stakes conditions.

National Resilience in the Digital Age

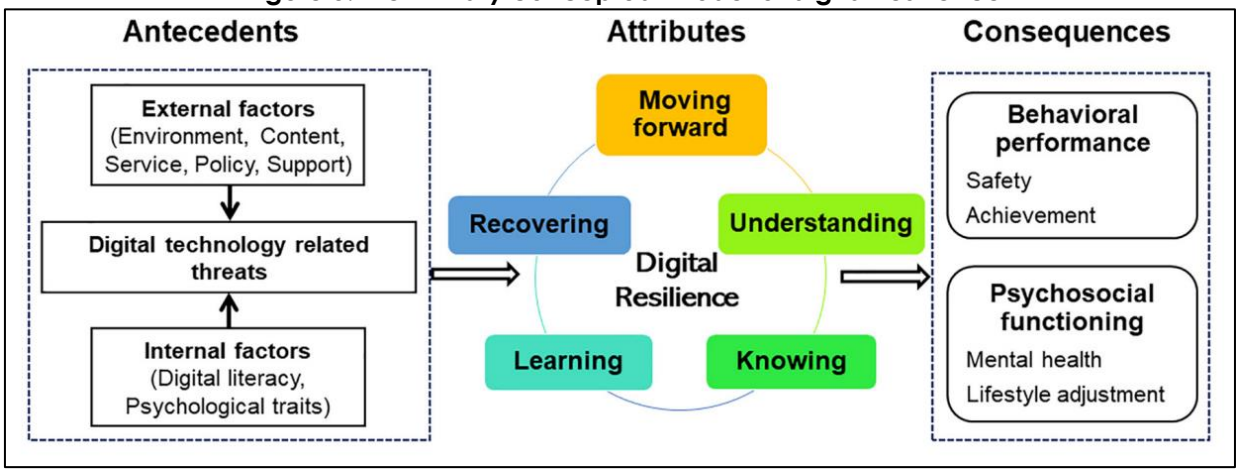
National resilience has been conceptualized as the capacity of a nation to withstand, adapt to, and recover from systemic disruptions, including natural disasters, cyberattacks, and socio-political unrest (Mohiul et al., 2022; Taddeo, 2017). Rooted in systems theory and risk governance, national resilience emphasizes robustness, redundancy, resourcefulness, and rapidity (Rahaman & Islam, 2021; Schackelford, 2016). Scholars differentiate resilience from related constructs such as risk management and security by focusing on a system's adaptive capacity and learning potential post-disturbance (Ahmed et al., 2022; Zhou et al., 2017). While traditional definitions emphasized disaster recovery and hazard resistance (Aklima et al., 2022; Schroeder et al., 2021), recent frameworks integrate cyber-resilience, data governance, and digital infrastructure (Mager & Katzenbach, 2021; Humaun et al., 2022; Schroeder et al., 2021). Fan et al. (2021) emphasized institutional resilience, focusing on governance structures and resource networks, whereas Glaessgen and Stargel (2012) and Tao et al. (2019) highlighted economic resilience tied to functional interdependencies. The inclusion of AI-driven systems and cybersecurity has redefined resilience as a dynamic, information-intensive capability involving cross-sector coordination and technological responsiveness (Sun et al., 2022). Brock and Wangenheim (2019) emphasized resilience indicators that account for both physical and cyber-infrastructures, while Chang et al., (2017) and O'Hara (2018) advocated for integrating social resilience dimensions. Taddeo (2017) and Schackelford (2016) further advanced the idea of "digital resilience" as the state's capacity to leverage information systems in real-time coordination during disruptions. This expanded conceptualization underpins the growing emphasis on AI-enhanced data systems and cybersecurity protocols in national resilience scholarship.

Historically, national resilience strategies prioritized physical defense mechanisms and post-event recovery, particularly in the domains of military infrastructure and civil protection (Mahfuj et al., 2022; Zhou et al., 2017). Over time, these approaches evolved with the emergence of complex adaptive systems thinking, which reframed disasters as multi-causal events requiring integrative, cross-sectoral responses (Schroeder et al., 2021). With the increased reliance on ICT systems, the focus shifted toward anticipatory governance and integrated resilience planning (Mager & Katzenbach, 2021). The concept of resilience was expanded to encompass socio-technical systems, recognizing that human behavior, technological systems, and institutional frameworks interact dynamically under stress (Fan et al., 2021). Glaessgen and Stargel (2012) and Tao et al., (2019) emphasized ecological and adaptive cycle models, later integrated into urban resilience planning by Sun et al. (2022). As digital threats escalated, national resilience began to integrate cyber-physical systems, critical digital assets, and AI-enhanced control systems into its operational definition (Tao et al., 2019). Emerging literature underlines the convergence of digital infrastructure protection with emergency planning, highlighting the role of data systems in maintaining

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

functional continuity (Fan et al., 2021; Tao et al., 2019). Glaessgen and Stargel (2012) and Tao et al. (2019) introduced metrics and simulation-based approaches to assess national resilience quantitatively. The transition from reactive strategies to AI-powered, real-time adaptation frameworks marks a critical juncture in the evolution of national resilience paradigms.

Figure 3: Preliminary conceptual model of digital resilience



Source: Sun et al. (2022).

Critical infrastructure, encompassing energy systems, water supply, transportation networks, healthcare systems, and digital communication platforms, forms the operational core of national resilience (Klaver & Luiijf, 2021; Mohiul et al., 2022). Its disruption can produce cascading failures, paralyzing national functions and eroding public trust (Pan et al., 2015). Studies by Serban and Lytras, (2020) and Radanliev, De Roure, Van Kleek, et al. (2020) highlight the interconnectedness of infrastructure sectors and the difficulty of isolating single points of failure. Infrastructure vulnerability assessments by Diamantoulakis et al. (2015)and Tiirmaa-Klaar (2016) reveal that even minor outages in digital or energy networks can trigger multi-sectoral breakdowns. AI-enabled infrastructure monitoring systems have become central to resilience strategies, allowing for predictive maintenance, load optimization, and early anomaly detection (Diamantoulakis et al., 2015; Tiirmaa-Klaar, 2016). Digital twins, as demonstrated by Fan et al. (2021) and Glaessgen and Stargel (2012), simulate operational stress in real-time, supporting proactive asset management. Cybersecurity threats targeting supervisory control and data acquisition (SCADA) systems, particularly in energy and water systems, have escalated concerns about national-level vulnerabilities (Agyepong et al., 2019). The literature identifies smart grid systems (Radanliev, De Roure, Page, et al., 2020), intelligent transportation systems (Barrett et al., 2017), and IoT-enabled water networks (Kulugh et al., 2022) as infrastructure domains with increasing AI integration for resilience enhancement. As critical infrastructure systems evolve into cyber-physical ecosystems, resilience frameworks must align operational continuity with security, agility, and data governance (Kulugh et al., 2022; Li et al., 2022).

The integration of digital systems within traditional infrastructure has introduced a new class of vulnerabilities that compromise national resilience (Sohel et al., 2022; Tanczer et al., 2018). SCADA systems, originally designed for isolated environments, now face threats from advanced persistent threats (APTs) and ransomware attacks (Li et al., 2022; Tanczer et al., 2018). The literature documents numerous high-impact incidents, such as the Stuxnet worm (Abazi, 2022), the Colonial Pipeline ransomware attack (Aliyu et al., 2020), and Ukraine's power grid breach (Mueller, 2017), which exposed the fragility of cyber-physical systems. Authors like Schackelford (2016) and AlDaajeh et al. (2022) identify interconnectivity as both an operational strength and a systemic risk. AI-based intrusion detection systems (IDS), using supervised and unsupervised machine learning algorithms, have emerged as a countermeasure to evolving cyber threats (AlDaajeh et al., 2022; Barrett et al., 2017; Tonoy, 2022). Neural networks and ensemble models now support behavioral threat detection in dynamic infrastructure environments (Abazi, 2022; Younus, 2022). Mueller (2017) and Aliyu et al. (2020) demonstrate that real-time anomaly detection enables

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

automated responses, reducing incident escalation. The literature also emphasizes the role of AI in patch management, traffic rerouting, and resource shielding during infrastructure-targeted attacks (Barrett et al., 2017; Kulugh et al., 2022). These studies collectively underscore the inseparability of infrastructure resilience and cybersecurity within digitally dependent national systems.

Resilience literature consistently emphasizes the need for whole-of-nation frameworks that integrate public, private, and civil sector actors in infrastructure planning and emergency response (Altay et al., 2018). Radanliev, De Roure, Van Kleek, et al. (2020) argue that decentralized governance supported by interoperable technologies increases adaptive capacity. The concept of "resilience dividends," proposed by Tiirmaa-Klaar (2016) , highlights the economic and social benefits of cross-sector collaboration. So et al. (2021) and Rehak et al., (2019) demonstrate that AI-enhanced data-sharing platforms enable synchronization across transportation, energy, healthcare, and emergency services. Blockchain has also emerged as a supporting technology for secure, tamper-proof infrastructure data exchange (Brandon-Jones et al., 2014). Pursiainen and Rød (2016) and Kulugh et al. (2022) show that multi-agency dashboards powered by real-time analytics improve communication, reduce duplication, and facilitate coordinated action. Polater (2020) highlight the significance of institutional learning in improving interagency operations post-crisis. Yu et al. (2019) and Linkov et al. (2014) explore how crowd-sourced data and crisis informatics support real-time situational awareness for infrastructure protection. Case studies from Japan (Larsson, 2020), the United States (Thompson et al., 2016) , and the EU (Schilke, 2013) reflect successful examples of integrated resilience infrastructures. These studies affirm that national resilience is operationalized through not only technological interventions but also institutional adaptability and cooperative infrastructures.

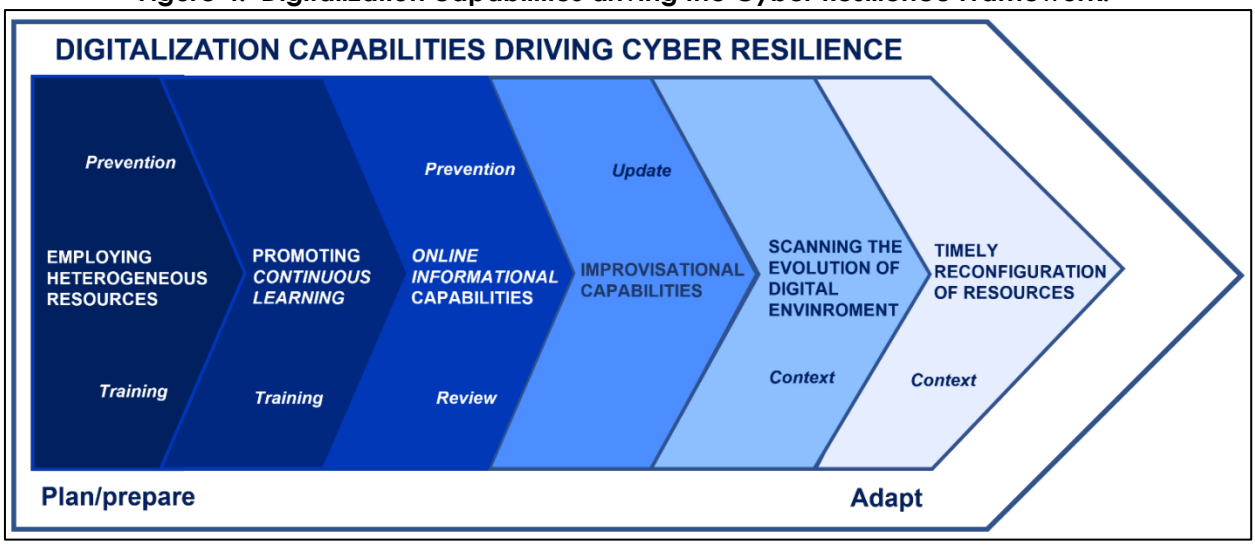
Role of digitization and smart systems in resilience-building

Digitization has redefined resilience from static risk mitigation toward dynamic adaptability enabled by real-time data, automation, and intelligent systems (Serban & Lytras, 2020). The integration of digital technologies into national resilience strategies allows for faster threat recognition, predictive modeling, and decentralized coordination (Diamantoulakis et al., 2015). Digitally enabled early warning systems leverage AI to monitor seismic activity, meteorological anomalies, and epidemiological trends, improving response times and operational accuracy (Lytras et al., 2017). Tan et al. (2021) emphasized that digital platforms support adaptive governance, enabling institutions to align their response dynamically as new data emerges. Data interoperability frameworks, such as those described by Deng et al. (2015) and Anderson (2016) , support cross-agency information sharing and decision alignment. Smart city initiatives, including those in Singapore, Amsterdam, and Seoul, have shown how embedded sensor networks and real-time analytics improve energy distribution, traffic control, and emergency communications (Anderson, 2016; Tanczer et al., 2018). The literature increasingly links digital infrastructure to operational resilience, with AI-powered dashboards, GIS mapping, and mobile applications enabling centralized oversight and localized autonomy (Lytras et al., 2017; Tan et al., 2021). Through digitization, resilience-building becomes a continuous process of sensing, analyzing, and adapting across complex public systems (Deng et al., 2015). Moreover, Smart systems combine artificial intelligence, IoT, and cyber-physical integration to continuously monitor infrastructure and environmental indicators (Anderson, 2016). These systems operate through distributed sensors, edge computing, and cloud-based data analytics, which enable infrastructure operators to anticipate failures and reroute resources autonomously (Tanczer et al., 2018). In power systems, smart grids predict load fluctuations, detect transmission anomalies, and self-correct distribution faults, thus reinforcing electrical grid resilience (Wang et al., 2016). In water infrastructure, AI-enabled systems monitor for leaks, contamination, and pressure anomalies in real time, preventing service disruptions and health hazards (Lytras et al., 2017; Wang et al., 2016). Smart healthcare systems use AI to allocate resources dynamically and track hospital capacity, which proved effective in managing the COVID-19 crisis in multiple countries (Anderson, 2016; Wang et al., 2016). Digital twins replicate physical infrastructure digitally and simulate crisis scenarios, helping operators adjust configurations during stress events (Tan et al., 2021). Sensor-driven surveillance in

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

transportation networks enhances mobility resilience by identifying bottlenecks and rerouting traffic flow during crises (Tanczer et al., 2018). These studies emphasize that resilience in smart infrastructure is achieved through autonomous system adjustments based on live operational data (Anthi et al., 2019; Krivý, 2016). The evolution from reactive to smart infrastructure marks a pivotal development in the resilience literature.

Figure 4: Digitalization capabilities driving the Cyber Resilience Framework.



Source: Annarelli et al. (2022)

Systemic risks are characterized by their cross-sectoral propagation, non-linearity, and amplification across dependent systems (Masys et al., 2014). These risks, including cyberattacks, pandemics, and climate events, affect interconnected infrastructure systems in unpredictable ways (Panda & Bower, 2020). The 2003 Northeast blackout and the 2017 WannaCry ransomware attack exemplify how disturbances in one domain cascade into financial markets, public health, and national security (Thramboulidis, 2015). Lee et al. (2015) emphasize that resilience strategies must be rooted in probabilistic risk analysis and network theory. Infrastructure interdependencies are classified as physical, cyber, geographic, and logical, with each domain requiring distinct analytical models to evaluate cascading consequences (Wan et al., 2013). AI-enhanced risk mapping tools allow decision-makers to visualize interconnectivity and vulnerability pathways, enabling better prioritization of resilience investments (Barrett et al., 2017; Kulugh et al., 2022). The literature also identifies "black swan" events—rare, high-impact disruptions—as significant contributors to systemic risk, requiring intelligent systems capable of managing information overload and uncertainty (Matusitz & Minei, 2009; Wan et al., 2013). Multi-hazard environments such as coastal urban centers exhibit compound systemic risks, necessitating digitized resilience tools for scenario-based simulations (Kulugh et al., 2022; Tao et al., 2019).

Cascading failures refer to the domino-like propagation of disruptions through interlinked systems, resulting in disproportionately large-scale breakdowns (Li et al., 2022). Thramboulidis (2015)that critical nodes in infrastructure networks, when compromised, trigger nonlinear collapse patterns. In digitally interconnected societies, this risk is heightened by real-time data dependencies and automated decision loops (Kulugh et al., 2022; Matusitz & Minei, 2009). A failure in one subsystem—such as a cyberattack on the energy grid—can cripple transportation, banking, and emergency services within minutes (Balaji et al., 2015; Tao et al., 2019). AI-enhanced monitoring systems mitigate cascading effects by predicting inter-node vulnerabilities and activating containment protocols (Li et al., 2022). Simulation studies using agent-based models and network theory quantify failure propagation and support strategic asset prioritization (Matusitz & Minei, 2009; Mbanaso & Kulugh, 2021). In smart cities, the failure of traffic management systems can lead to secondary failures in logistics, emergency response, and public safety, particularly during crises such as natural disasters or terrorism (Ross et al., 2019; Tao et al., 2019). Studies by Tanczer et al., (2018) and Ross et al. (2019) show that AI systems can autonomously reconfigure network

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

operations to isolate compromised nodes and reroute traffic or data flows. These mechanisms reduce the reach and duration of cascading failures across digital and physical infrastructure.

The resilience literature emphasizes that modern infrastructure is embedded in a web of interdependencies, where the failure of one function escalates risk across multiple sectors (Ross et al., 2019; Wan et al., 2013). These interdependencies include financial reliance, physical connection, shared information systems, and governance structures (Abazi, 2022; Mbanaso & Kulugh, 2021). For instance, water treatment facilities rely on power grids, which in turn depend on telecommunications and transport logistics (Mbanaso & Kulugh, 2021; Radanliev et al., 2018). AI models allow for mapping these dependencies by quantifying systemic risk and visualizing correlation matrices across infrastructure layers (Zhu et al., 2011). In healthcare, the breakdown of IT systems can delay patient care, supply chains, and emergency response simultaneously (Matusitz & Minei, 2009). Real-time sensor fusion platforms integrate environmental, structural, and cyber indicators to generate situational overviews that guide decision-makers during crisis escalation (Barrett et al., 2017). Blockchain-enabled data-sharing mechanisms further strengthen inter-organizational trust and operational consistency across sectors (Mbanaso & Kulugh, 2021). Multi-criteria decision-making frameworks developed by Li et al. (2022) and Radanliev, De Roure, Nurse, et al. (2020) provide holistic assessments of resilience that account for cascading, systemic, and emergent risks. This interconnected lens shifts resilience-building from siloed sectoral planning to integrated, digital, and intelligence-driven governance.

Artificial Intelligence in Crisis Detection and Prediction

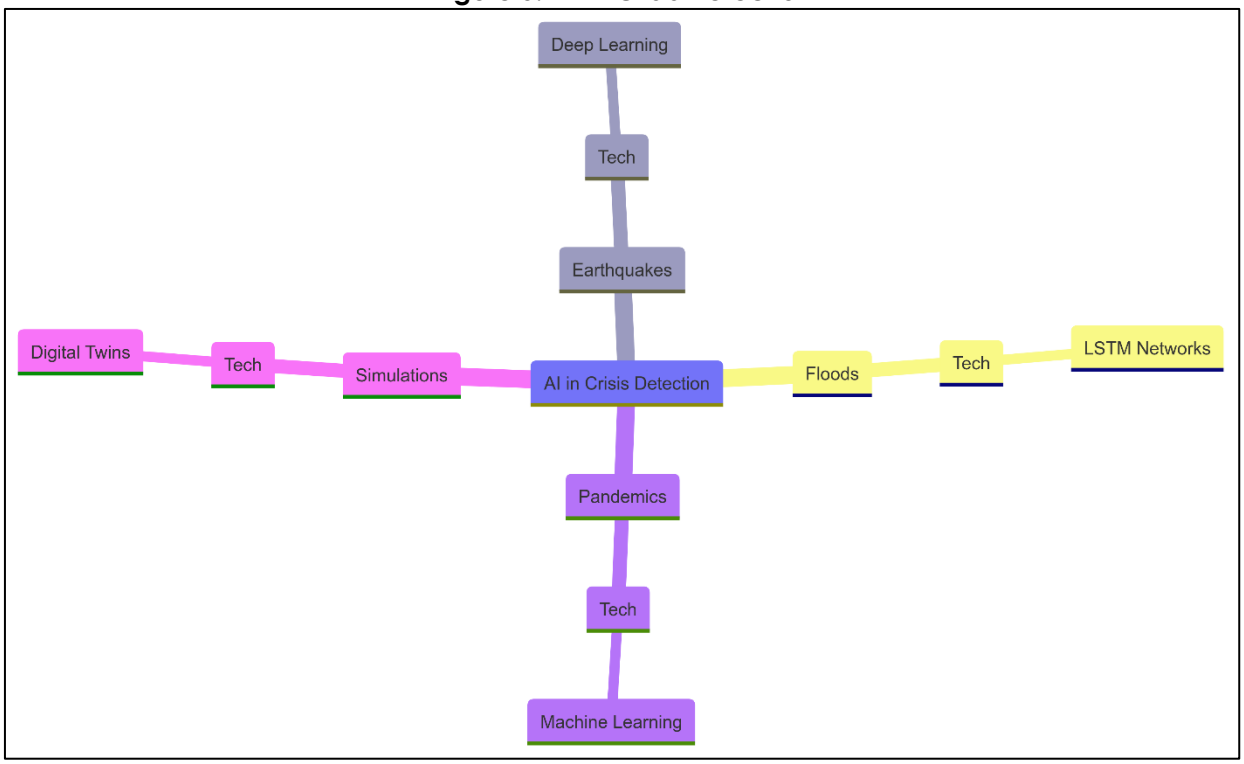
Artificial intelligence (AI) has played a critical role in enhancing early warning systems for natural disasters by enabling rapid data processing, pattern recognition, and real-time prediction (Jobin et al., 2019). AI applications in earthquake detection employ seismographic data, GPS displacement, and deep learning algorithms to identify anomalies that indicate tectonic shifts (Dubey et al., 2020; Homberg et al., 2020). Similarly, convolutional neural networks (CNNs) and support vector machines (SVMs) have been trained to classify seismic events with high accuracy (Shao & Zhang, 2020). In flood forecasting, machine learning models integrate satellite imagery, meteorological records, and river discharge data to predict flooding extent and timing (Ssekulima et al., 2016). Random forest and long short-term memory (LSTM) networks have been applied to simulate flash flood conditions and evaluate spatial risks (Ivanov & Dolgui, 2020). During the COVID-19 pandemic, AI supported outbreak detection using mobility data, social media mining, and contact tracing algorithms (Ivanov & Das, 2020; Shen, 2021). AI-integrated systems, such as IBM's Watson and BlueDot, were utilized for epidemic mapping and predicting regional spread patterns (Pizzi et al., 2020). These technologies improved the timeliness and granularity of disaster response by generating automated alerts based on continuous data ingestion and real-time inference.

Simulation-based AI models have become essential tools in forecasting natural hazard trajectories and testing resilience scenarios across geographies (Ivanov & Dolgui, 2020). Multi-agent systems (MAS) replicate the interactions of infrastructure elements, population behavior, and environmental dynamics to assess how crises propagate in urban or rural settings (Ivanov & Dolgui, 2020; Lawson-McDowall et al., 2021). Digital twin models simulate hurricanes, earthquakes, and tsunamis using AI to assess structural vulnerability and emergency response effectiveness (Singh et al., 2020; Warnat-Herresthal et al., 2021). Geographic information systems (GIS) integrated with AI facilitate hazard zone mapping and population risk distribution under various disaster intensities (Queiroz et al., 2022). Studies by Shen (2021) and Altay and Pal (2022) demonstrate how AI-driven simulation platforms support disaster planning through virtual exercises involving dynamic resource allocation and population mobility. For landslides and wildfires, recurrent neural networks (RNNs) and fuzzy logic systems model terrain instability and vegetation flammability under weather changes (Pizzi et al., 2020). These tools improve comprehension of cascading and compound disasters, integrating variables such as hydrology, seismic activity, and climate data (Pizzi et al., 2020; Queiroz et al., 2022). By modeling system stressors and their probable interactions,

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

AI-supported simulations offer precision in visualizing potential crisis environments across multiple temporal and spatial layers (Singh et al., 2020).

Figure 5: AI in Crisis Detection



The application of machine learning (ML) in multi-hazard forecasting has enabled the development of robust predictive models capable of managing non-linear, high-dimensional datasets (Gu et al., 2017). Decision trees, random forests, gradient boosting machines (GBM), and artificial neural networks (ANNs) are widely used for modeling hazards such as hurricanes, droughts, and pandemics (Amiri & Gunduz, 2019; Xin et al., 2020). LSTM and gated recurrent unit (GRU) models offer accurate forecasting of time-series environmental data, capturing sequential dependencies critical for weather-related crisis prediction (Chen et al., 2017; Yang et al., 2020). Ensemble learning methods have been shown to outperform individual classifiers in flood prediction and wildfire modeling due to their generalization ability and resilience to overfitting (Yang et al., 2019). Transfer learning and reinforcement learning further enhance adaptability across geographies and disaster types by leveraging prior model knowledge (Hosseinalipour et al., 2020). Recent studies reveal that hybrid models combining AI with physical process-based simulations, such as hydrological or seismic models, offer greater accuracy and interpretability (Hosseinalipour et al., 2020; Huang et al., 2021). Crisis prediction literature also integrates crowd-sourced and social media data with traditional environmental indicators to identify non-obvious early signals of emergencies (Amiri & Gunduz, 2020). Such models enable risk monitoring in real time and offer decision-makers a contextual understanding of evolving threats. Moreover, Artificial intelligence has been instrumental in modeling disease outbreaks, especially in epidemiological surveillance and health system forecasting (Bengio et al., 2021). Supervised learning methods classify regions based on infection likelihood, while unsupervised clustering reveals outbreak patterns in complex population datasets (Bengio et al., 2021; Xin et al., 2020). Studies during the COVID-19 pandemic applied LSTM models and autoregressive integrated moving average (ARIMA) to forecast infection peaks and healthcare demand (Lima et al., 2019; Yang et al., 2019). AI also supported syndromic surveillance through electronic health records, wearable devices, and online symptom reporting platforms (Yang et al., 2020). Predictive analytics assisted in ventilator allocation, ICU forecasting, and medical supply chain management, improving hospital preparedness (Hosseinalipour et al., 2020). Reinforcement

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

learning optimized lockdown policies by modeling trade-offs between mobility and transmission risk (Amiri & Gunduz, 2020). Bayesian models and probabilistic graphical networks were used for contact tracing and disease propagation analysis (Yang et al., 2019). AI integration in pandemic modeling has provided real-time dashboards, geospatial visualization, and predictive risk scoring, significantly advancing public health surveillance and emergency decision-making. Despite the growing efficacy of AI in crisis forecasting, several methodological and operational challenges persist. The literature highlights issues of data scarcity, model overfitting, and lack of transferability between regions or crisis types (Bengio et al., 2021; Yang et al., 2019). Inaccurate or incomplete training datasets, particularly in underrepresented disaster zones, reduce the generalizability of predictive models (Lima et al., 2019; Voyant et al., 2017). Interpretability remains a concern, especially for deep learning models whose internal logic is not transparent to emergency managers (Liakos et al., 2018; Sun et al., 2017). Real-time forecasting systems also struggle with latency, particularly in data ingestion from distributed sources like sensors, satellites, and social media (Dudley & Kristensson, 2018). Cross-validation techniques, while robust for model training, often do not reflect dynamic environments encountered during actual disasters Chen et al., (2017). Studies by Yang et al. (2019) and Amiri and Gunduz (2020) argue that rare, high-impact events resist algorithmic prediction due to their statistical outlier nature. Ethical concerns arise around data privacy, especially in the use of mobility and biometric data for outbreak modeling (Amiri & Gunduz, 2020; Yang et al., 2020). Additionally, inconsistent data standards across sectors hinder interoperability of AI models across platforms and jurisdictions (Voyant et al., 2017; Yang et al., 2019). These constraints suggest the need for multidisciplinary model design, transparent evaluation protocols, and context-sensitive deployment in crisis detection systems.

Use of computer vision and NLP in disaster monitoring

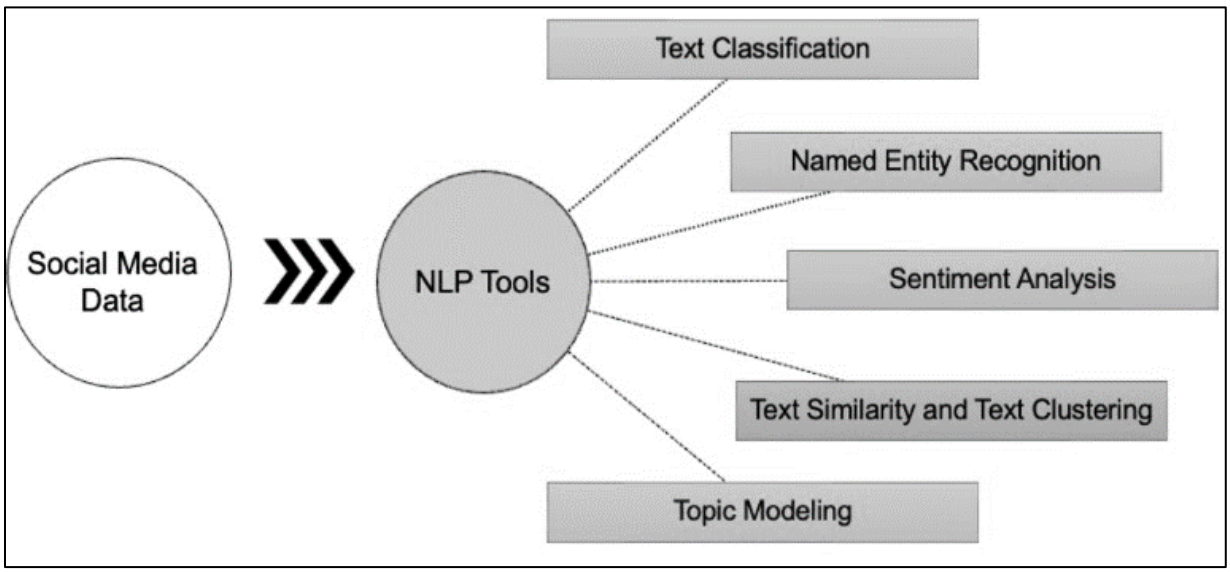
Computer vision has emerged as a transformative tool in disaster monitoring, enabling the automated analysis of images and videos captured by satellites, drones, and surveillance systems (Eykholt et al., 2018). Convolutional neural networks (CNNs) and deep learning frameworks have been employed to classify disaster-impacted regions, assess structural damage, and detect environmental anomalies (Eykholt et al., 2018; Sze et al., 2017). Post-disaster imagery, such as those from floods, earthquakes, and wildfires, is processed through supervised and unsupervised learning models to map affected zones and prioritize response activities (Szegedy et al., 2013; Wiesner-Hanks et al., 2019). UAV-based image acquisition, coupled with AI models, allows real-time mapping of inaccessible terrains and accelerates damage quantification (Fazeli et al., 2019). Semantic segmentation and object detection techniques have enabled fine-grained classification of collapsed buildings, blocked roads, and stranded populations (Athalye et al., 2017). Satellite imagery has been particularly useful in wildfire detection and drought monitoring through spatiotemporal modeling of land surface changes (Biggio & Roli, 2018). Integrating computer vision into emergency command centers enhances operational awareness and reduces reliance on manual image interpretation (Athalye et al., 2017; Biggio & Roli, 2018). Studies have consistently shown that vision-based AI outperforms traditional GIS methods in terms of speed, accuracy, and automation potential (Sze et al., 2017).

Natural language processing (NLP) has become an essential tool for real-time analysis of textual data generated during disasters, particularly from social media, emergency reports, and citizen communication channels (Xie et al., 2021). Named entity recognition (NER), topic modeling, and sentiment analysis enable the extraction of meaningful signals from unstructured texts, offering early insights into disaster onset, location, and severity (Wan et al., 2013). Studies by Kulugh et al., (2022) and Rajkumar et al. (2010) revealed that Twitter and Facebook posts can provide rapid situational updates often ahead of official reports. NLP techniques have been employed to classify tweets based on relevance, urgency, and request type using machine learning classifiers such as SVMs and decision trees (Rajkumar et al., 2010; Yang et al., 2019). Deep learning models, including BERT and LSTM-based architectures, offer improved contextual understanding and classification accuracy in multilingual and noisy datasets (Ullah et al., 2018). CrisisLex and CrisisNLP corpora have supported supervised learning on annotated disaster-related texts, enhancing the reliability of text classification systems (Matusitz & Minei, 2009). NLP also facilitates rumor detection,

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

information verification, and emotional response analysis during disaster events, thereby supporting mental health interventions and community trust (Gotoh et al., 2017). Integration of NLP outputs into emergency dashboards allows decision-makers to monitor public discourse and tailor communication strategies accordingly (Panda & Bower, 2020).

Figure 6: Application of NLP Tools for Social Media Data Analysis in Crisis Management



The fusion of AI with sensor networks and Internet of Things (IoT) infrastructures has significantly enhanced environmental monitoring capabilities for disaster prediction and response (Thramboulidis, 2015; Wan et al., 2013). Wireless sensor networks (WSNs) embedded in rivers, bridges, and geological faults collect real-time data on parameters such as water levels, temperature, gas emissions, and structural vibrations (Matusitz & Minei, 2009; Panda & Bower, 2020). AI algorithms analyze this data to detect anomalies and generate alerts without manual oversight (Larsson, 2020). Smart city projects have deployed these systems to monitor flooding risks, detect earthquakes, and prevent industrial hazards (Larsson, 2020; Shneiderman, 2016). Studies show that combining AI with edge computing reduces latency and improves energy efficiency in sensor-based detection systems (Bhandari et al., 2015). Distributed AI models can function locally at the sensor node level to classify environmental events, reducing the need for centralized processing (Rodríguez-Espíndola et al., 2020). Advanced sensing networks have been used in earthquake-prone regions like Japan and California to deliver immediate alerts, often seconds before impact, allowing life-saving interventions (Rodríguez-Espíndola et al., 2020; Taddeo & Floridi, 2018). The integration of AI enhances both the accuracy and responsiveness of sensor systems and transforms them into intelligent agents within disaster resilience infrastructures (Subramanian et al., 2020).

IoT systems have transformed situational awareness in crisis environments by enabling the real-time tracking of resources, populations, and hazards across distributed networks (Jung et al., 2020; Taddeo & Floridi, 2018). AI-enabled IoT architectures integrate mobile devices, drones, wearables, and embedded systems into a coherent operational landscape (Subramanian et al., 2020; Tan et al., 2022). Real-time data from mobile phones and GPS devices have been used to monitor population displacement during hurricanes and earthquakes (Elish & boyd, 2017; Taddeo & Floridi, 2018). Smart shelters use IoT to manage capacity, monitor environmental conditions, and support resource distribution (Zhou et al., 2021). AI models applied to IoT data support dynamic traffic routing, emergency vehicle prioritization, and hospital readiness in mass casualty events (Skatchkovsky et al., 2021; Taddeo & Floridi, 2018). Studies by Taddeo et al. (2019) and Bechmann and Bowker (2019) show that integrating NLP and vision data from social media and surveillance enhances the situational picture derived from IoT systems. IoT sensors embedded in bridges, tunnels, and roads monitor structural health, providing early warnings of potential collapse or

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

obstruction during disasters (Zhou et al., 2021). Research confirms that AI-IoT integration significantly improves responsiveness, reduces information bottlenecks, and provides actionable intelligence during emergencies (Taddeo & Floridi, 2018; Zhou et al., 2021).

Data Analytics in Emergency Response Coordination

Emergency management has increasingly relied on big data sourced from a variety of platforms, including social media, satellite imagery, surveillance feeds, and mobile communication networks (Pescaroli et al., 2018). Social media platforms, especially Twitter and Facebook, offer rapid dissemination of ground-level information during crises such as earthquakes, floods, and terrorist attacks (Masys et al., 2014). Satellite data has been critical for wide-area assessment, capturing environmental changes and disaster impacts using spectral and thermal imaging (Vanajakumari et al., 2016). Surveillance systems, including closed-circuit television (CCTV), drones, and aerial reconnaissance, provide continuous visual feeds for real-time threat detection (Carlson et al., 2012). Mobile network data supports population tracking, enabling the estimation of displacement patterns during natural and man-made disasters (L'Hermitte et al., 2016). Emergency authorities integrate these diverse sources to improve situational awareness, which enables better prioritization and coordination of response activities (Pescaroli et al., 2018). However, the heterogeneity and velocity of these data streams necessitate intelligent analytics platforms capable of filtering, classifying, and interpreting actionable insights within seconds (Masys et al., 2014). Moreover, crisis informatics bridges information science, emergency response, and human-computer interaction to support data-driven decision-making during emergencies (Qadir et al., 2016). It facilitates the structuring of heterogeneous data from official sources, public reports, and digital platforms into operational intelligence (Akter & Wamba, 2017; Qadir et al., 2016). Data fusion platforms aggregate social media, sensor inputs, GIS data, and surveillance imagery to deliver a comprehensive situational picture (Pizzi et al., 2020). AIDR (Artificial Intelligence for Disaster Response), CrisisMapping, and Ushahidi are among the most widely deployed systems for crowd-sourced crisis data collection and analysis (Lawson-McDowall et al., 2021). These platforms utilize machine learning classifiers and natural language processing to categorize crisis-related posts and filter misinformation (Masys et al., 2014). Advanced fusion models apply Bayesian networks, fuzzy logic, and multi-agent simulations to weigh conflicting data and assign reliability scores (Fan et al., 2021). Studies confirm that such integrated systems improve speed, accuracy, and trustworthiness of information, especially during the chaotic onset phase of a crisis (Qadir et al., 2016). They also support interoperability among agencies by standardizing data formats and facilitating joint response strategies (Akter & Wamba, 2017).

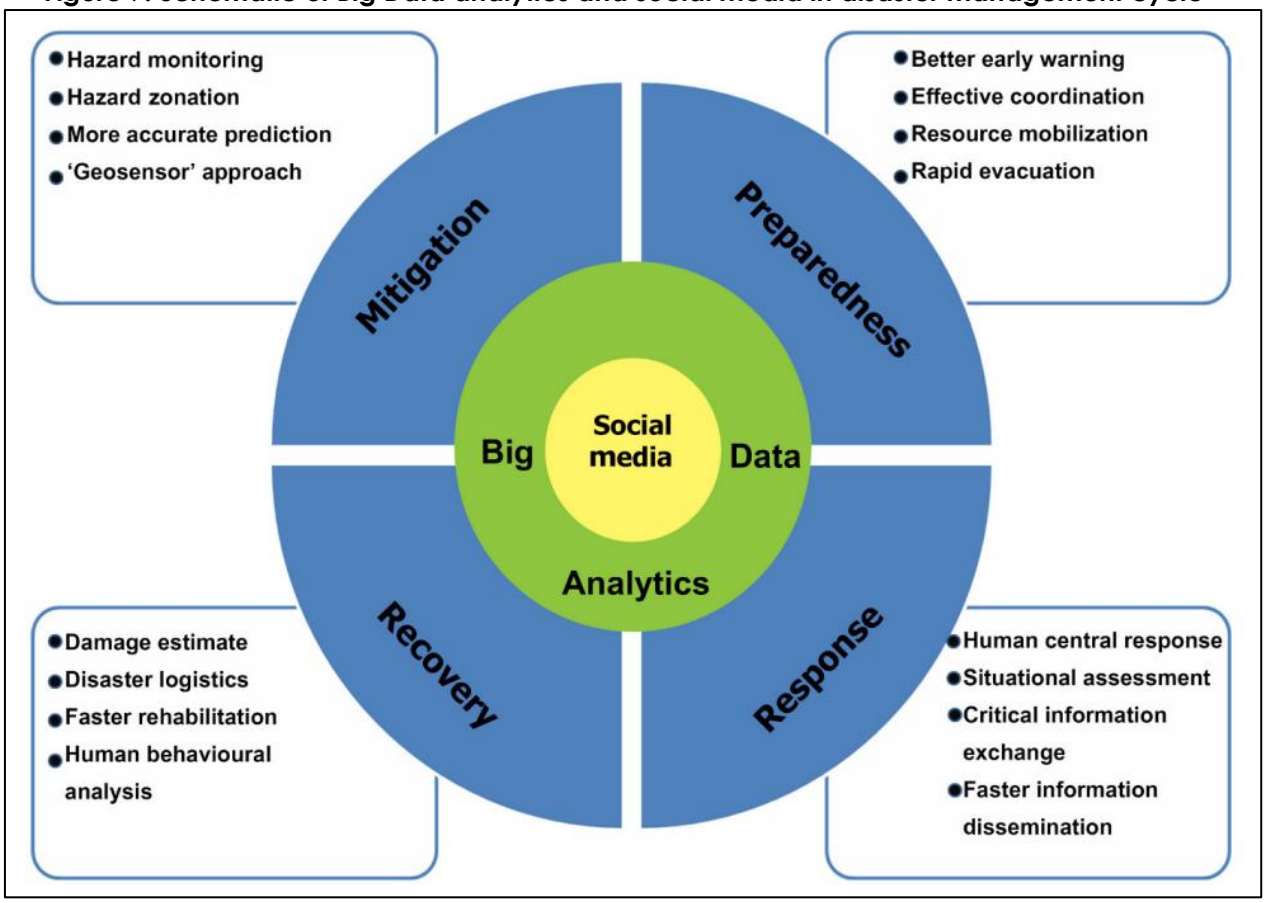
The development of predictive dashboards and geospatial visualization platforms has enhanced emergency response planning by providing real-time analytics and operational foresight (Heer, 2019). These dashboards integrate live data feeds from environmental sensors, GPS trackers, and social media APIs to display disaster progression, affected areas, and available resources (Dubey et al., 2019). Tools such as GeoNode, ArcGIS, and Google Crisis Map enable decision-makers to visualize infrastructure vulnerabilities, demographic distributions, and safe zones (Radanliev, De Roure, Page, et al., 2020). AI-based resource allocation systems optimize the distribution of personnel, supplies, and emergency equipment based on proximity, severity, and predicted needs (Campolo & Crawford, 2020). Multi-criteria decision analysis (MCDA) models are integrated into dashboards to assist with trade-off evaluations under uncertainty (Jagielski et al., 2018; Tripp et al., 2015). These platforms often feature customizable modules for hospital bed tracking, evacuation route planning, and supply chain status (Dennis et al., 2016). Studies show that geospatial mapping tools improve coordination across jurisdictions, particularly when disasters span state or national boundaries (Tripp et al., 2015). Integration of visualization, predictive modeling, and logistic tracking enhances precision in both strategic planning and on-the-ground execution.

The value of real-time analytics during emergencies is frequently challenged by constraints such as limited bandwidth, sensor errors, incomplete data, and cognitive overload in decision-making teams (Jagielski et al., 2018; Tripp et al., 2015). Emergency contexts often feature volatile data quality, requiring AI models to handle noise, ambiguity, and contradictory inputs (Jung et al.,

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

2020). The speed of decision-making in time-sensitive scenarios demands that data systems process inputs, classify events, and generate outputs within seconds (Duan et al., 2019). Studies have documented that real-time platforms sometimes fail under surge conditions due to processing bottlenecks and storage limitations (Lee et al., 2014). Low-latency architectures using edge computing have been developed to reduce reliance on cloud-based systems and improve fault tolerance (Dubey et al., 2019). Visualization tools must balance informational density with clarity to avoid overwhelming operators (Campolo & Crawford, 2020). Further complications arise from data ownership issues, privacy concerns, and technical interoperability among agencies (Campolo & Crawford, 2020; Tripp et al., 2015). Systems with weak semantic models often misclassify or miss critical anomalies, leading to suboptimal decisions (Dennis et al., 2016). These studies underline the trade-offs between speed, accuracy, and interpretability in high-stakes emergency analytics.

Figure 7: Schematic of Big Data analytics and social media in disaster management cycle



Source: Joseph et al. (2018).

AI-Enabled Decision Support Systems for National Crisis Management

Expert systems and autonomous decision agents have long been utilized in critical decision environments to support rapid, knowledge-based reasoning under uncertainty (Pizzi et al., 2020). In national crisis management, rule-based expert systems enable the codification of best practices, policies, and emergency protocols to guide operator decision-making (Akter & Wamba, 2017). Autonomous agents, powered by reinforcement learning and dynamic programming, are capable of evaluating trade-offs among competing goals in real time, such as allocating limited resources during a disaster (Akter & Wamba, 2017; Pizzi et al., 2020). Decision agents have been deployed in systems like RoboCup Rescue and DEFACTO to support simulation-based planning and adaptive resource distribution (Qadir et al., 2016). Studies by Pizzi et al. (2020) and Qadir et al. (2016) show that decision agents enhance agility in complex scenarios by continuously adapting policies based on feedback from IoT and environmental data. In health

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

emergencies, such as during the COVID-19 pandemic, expert systems supported diagnostic triage, hospital capacity planning, and vaccine logistics (Masys et al., 2014; Qadir et al., 2016). These systems reduce the cognitive burden on human operators by offering decision recommendations based on real-time data and codified emergency knowledge (Lawson-McDowall et al., 2021). Through integration with geospatial systems and crisis informatics platforms, autonomous agents contribute to coordinated national-level crisis response.

Effective integration of AI in crisis environments depends on transparent and interpretable human-AI interaction (HAI), particularly in high-risk decision contexts where trust and accountability are critical (O'Leary, 2013). Explainable AI (XAI) has emerged as a subfield aimed at improving the transparency of black-box models such as neural networks, enabling emergency managers to understand the rationale behind AI-generated recommendations (Duan et al., 2019). Visual dashboards, attention-based models, and surrogate explanations like LIME (Local Interpretable Model-Agnostic Explanations) are frequently integrated into emergency platforms to enhance interpretability (Serban & Lytras, 2020). Studies show that human operators are more likely to act on AI output when presented with clear justifications, especially during resource triage or evacuation decisions (O'Leary, 2013; Serban & Lytras, 2020). Interaction design also plays a role in minimizing information overload and maximizing situational awareness in emergency operations centers (EOCs) (Jordan, 2019; O'Leary, 2013). Systems developed by FEMA and the EU Civil Protection Mechanism have incorporated explainable models into decision dashboards, enhancing operator trust and cross-agency coordination (Daly et al., 2019). HAI research also examines how to balance machine autonomy with human control, particularly when using autonomous drones, robotics, and predictive modeling during crises (Licht & Fine, 2020). The literature highlights that human-AI co-decision systems are most effective when designed for shared control and iterative feedback, reinforcing resilience in high-stakes national emergencies.

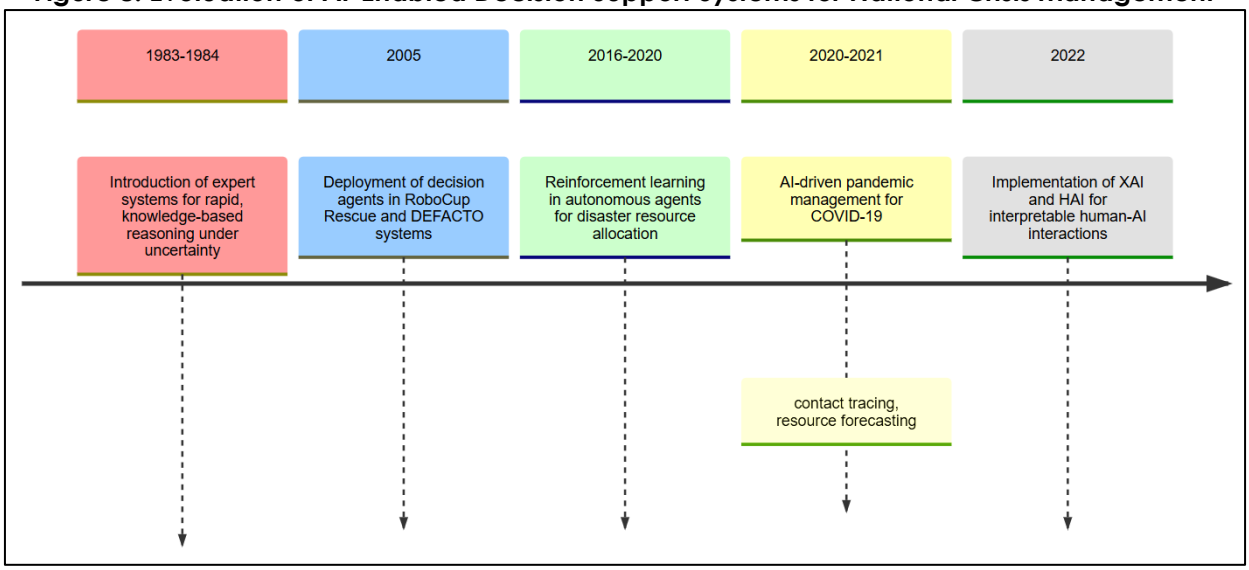
Multi-agent systems (MAS) simulate the behavior of distributed, autonomous entities such as emergency responders, infrastructure nodes, and mobile assets within a shared operational environment (Fine & Licht, 2020; King et al., 2019). These systems enable parallel processing of information, adaptive coordination, and decentralized problem-solving in national crisis response scenarios (Jordan, 2019). MAS have been applied to wildfire management, flood mitigation, and pandemic logistics, where agents operate collaboratively or competitively to meet collective objectives (Fine & Licht, 2020). In transportation systems, agent-based models support real-time rerouting, congestion prediction, and prioritization of emergency vehicles (Jordan, 2019). Research by Meissner (2019) illustrates how MAS frameworks mirror actual institutional networks in disaster contexts, capturing the dynamics of cross-sectoral coordination. Models such as DEFACTO and TEAMCORE have been tested for firefighting and rescue missions, offering intelligent suggestions for deployment based on spatial, temporal, and capacity constraints (Jordan, 2019). Reinforcement learning enhances agent adaptability by enabling learning from crisis scenarios and evolving conditions (Jordan, 2019; Pizzi et al., 2020). MAS also support redundancy and fault tolerance, allowing national systems to maintain core functionality even when individual components fail (Radanliev, De Roure, Van Kleek, et al., 2020). The literature confirms the value of MAS in enabling scalability, efficiency, and resilience in real-world emergency coordination frameworks.

The COVID-19 pandemic presented a global testbed for AI-enabled decision support systems across national health, logistics, and governance domains (Dubey et al., 2020; Jobin et al., 2019). Governments in South Korea, Singapore, and Taiwan employed AI for contact tracing, resource forecasting, and mobility control (O'Leary, 2013; Radanliev, De Roure, Van Kleek, et al., 2020). AI models integrated with health informatics platforms predicted case surges, optimized ICU assignments, and supported supply chain reallocation for masks, ventilators, and vaccines (Daly et al., 2019). Bayesian networks and time-series forecasting models such as ARIMA and LSTM supported national-level epidemic modeling (Meissner, 2019). In the United States, the CDC and private-sector collaborators employed machine learning for syndromic surveillance and telemedicine triage (O'Leary, 2013; Radanliev, De Roure, Van Kleek, et al., 2020). China used facial recognition and thermal imaging systems to automate temperature checks and

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

quarantine enforcement (Xiao et al., 2015; Zeng et al., 2020). Real-time dashboards, such as Johns Hopkins University's COVID-19 Tracker, demonstrated the operational value of AI-powered geospatial visualization and predictive mapping (Larsson, 2020). Studies show that AI-enhanced decision systems improved speed and precision in crisis response while reducing the burden on overwhelmed healthcare infrastructures (Shen, 2021).

Figure 8: Evoluation of AI-Enabled Decision Support Systems for National Crisis Management



AI-supported systems have been increasingly applied in wildfire management, earthquake response, and hurricane preparedness to improve prediction, monitoring, and strategic coordination (Duan et al., 2019). In California, IBM's Watson was used to analyze satellite imagery and meteorological data to predict wildfire spread, optimize firefighter deployment, and inform evacuation orders (Duan et al., 2019; Larsson, 2020). Deep learning models applied to multispectral imagery and drone footage classified vegetation density and ignition likelihood, aiding proactive mitigation (Huang et al., 2018). Australia's National Bushfire Information System incorporated real-time AI-based alerts to coordinate across jurisdictions and dispatch units based on wind patterns and population exposure (Zeng et al., 2020). Earthquake response systems in Japan integrated AI to deliver pre-shock alerts and assess structural damage using sensor and satellite data (Xiao et al., 2015). In hurricane-prone areas, predictive dashboards such as FEMA's HURREVAC used AI to simulate storm trajectories, surge levels, and critical infrastructure exposure (Larsson, 2020; Xiao et al., 2015). Studies by Jian et al. (2014) and Zeng et al. (2020) confirm that AI-enhanced simulation platforms significantly reduce response delays and improve resource prioritization during complex emergencies. These case studies demonstrate the operational integration of AI in diverse natural hazard contexts, reinforcing its position within national resilience frameworks.

AI-Driven Cybersecurity for Infrastructure Protection

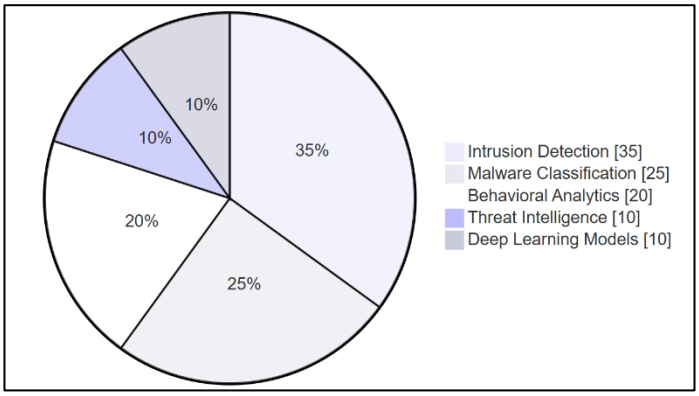
Artificial intelligence (AI) techniques have significantly enhanced the capabilities of intrusion detection systems (IDS) and malware classification tools by enabling dynamic, real-time threat identification in complex and evolving environments (Barrett et al., 2017). Traditional signature-based IDS often fail against zero-day attacks and polymorphic malware, necessitating adaptive learning approaches such as machine learning (ML) and deep learning (DL) (Barrett et al., 2017; Kulugh et al., 2022). Support vector machines (SVM), decision trees, and k-nearest neighbor algorithms have been deployed to classify known attack patterns with high accuracy (Li et al., 2022; Radanliev, De Roure, Page, et al., 2020). Ensemble methods, including Random Forest and Gradient Boosting Machines, improve detection by combining multiple classifiers to reduce false positives (Aliyu et al., 2020; Schackelford, 2016). Neural networks such as multilayer perceptrons (MLP) and recurrent neural networks (RNNs) are effective in processing sequential network traffic data, detecting intrusions based on learned behavior patterns (Mueller, 2017). AI-based malware

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

classifiers analyze binary executables using convolutional neural networks (CNNs), converting binary code into grayscale images to detect malicious payloads (Aliyu et al., 2020). These approaches outperform static signature models by continuously adapting to novel threats, making them suitable for high-value critical infrastructure environments (Sadik et al., 2020). The literature confirms that AI-enabled IDS and malware classifiers have become foundational components in modern cybersecurity ecosystems.

Behavioral analytics systems leverage AI to detect cybersecurity threats by analyzing deviations in user, device, and system behavior over time (Heer, 2019). Unlike traditional rules-based security tools, behavior-based analytics adapt to baseline patterns and identify anomalies that suggest unauthorized access, insider threats, or credential misuse (King et al., 2019). User and Entity Behavior Analytics (UEBA) platforms use clustering, regression models, and unsupervised learning techniques to construct behavioral profiles and flag deviations (Daly et al., 2019). Advanced systems apply reinforcement learning to update anomaly thresholds in response to contextual changes (Daly et al., 2019; Heer, 2019). Threat intelligence systems powered by AI aggregate attack indicators from global sources, using natural language processing (NLP) to extract patterns from cybersecurity reports, forums, and dark web content (Akter & Wamba, 2017; Liberati, 2018). Knowledge graphs have been integrated with AI to visualize and connect threat vectors, enabling security teams to trace attack origins and predict future targets (Coble et al., 2018). These systems enhance real-time situational awareness by correlating telemetry across devices, networks, and applications (Yeom et al., 2019). Behavioral and threat intelligence frameworks have proven effective in environments where attackers modify tactics frequently, including power grids, defense networks, and critical medical systems (Coble et al., 2018; Yeom et al., 2019).

Figure 9: AI-Driven Cybersecurity



Deep learning (DL) has emerged as a powerful tool for anomaly detection in cyber-physical systems (CPS), which are frequently targeted due to their essential role in national infrastructure (Xie et al., 2021). Long short-term memory (LSTM) networks and gated recurrent units (GRU) are widely applied to model time-series data generated by supervisory control and data acquisition (SCADA) systems, enabling early identification of anomalies in energy, water, and manufacturing networks (Sohrabi et al., 2021; Xie et al., 2021). Autoencoders, a form of unsupervised neural network, are used to reconstruct normal operational behavior and detect deviations indicative of cyberattacks (Lee et al., 2019; Xie et al., 2021). Generative adversarial networks (GANs) have been employed to simulate sophisticated attacks and train more robust detection systems (Mao et al., 2018; Sohrabi et al., 2021). CNNs have been adapted for network intrusion detection by transforming packet-level features into two-dimensional inputs (Mocanu et al., 2016). Studies have shown that DL models can identify stealthy attacks such as advanced persistent threats (APTs) that bypass traditional detection tools (Lee et al., 2019; Mao et al., 2018). In critical environments like smart grids, airports, and hospitals, DL-based anomaly detection ensures service continuity and minimizes downtime by identifying threats before system failure (Rolnick et al., 2017). These systems outperform heuristic and statistical models by learning complex, nonlinear threat patterns from high-dimensional sensor and log data (Mocanu et al., 2016).

Interfacing AI and Cybersecurity in Cyber-Physical Systems (CPS)

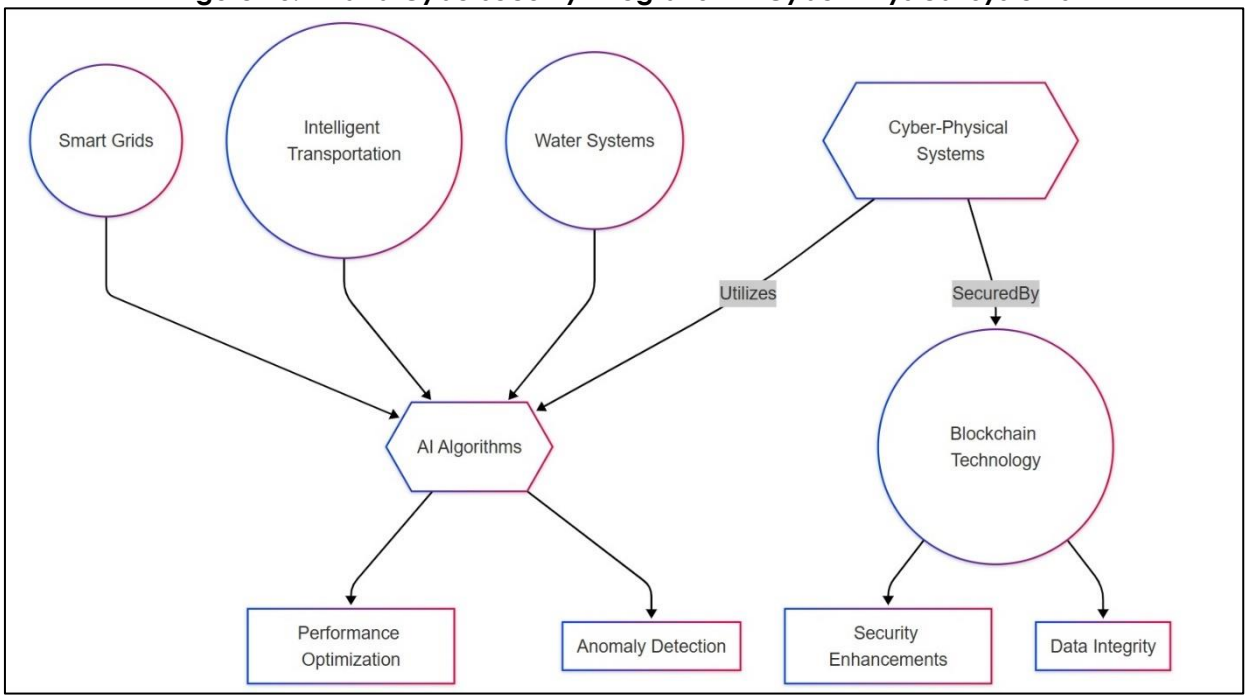
Cyber-physical systems (CPS) such as smart grids, intelligent transportation systems (ITS), and automated water distribution networks increasingly rely on artificial intelligence (AI) to optimize performance, detect anomalies, and manage real-time operations (Klaver & Luiijf, 2021). Smart grids utilize AI algorithms for load forecasting, demand response, and fault detection through

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

time-series analysis of sensor data (Agyepong et al., 2019). Neural networks, particularly LSTM and GRU models, improve energy consumption prediction and optimize peak demand distribution (Agyepong et al., 2019; Wang et al., 2015). In ITS, machine learning supports traffic prediction, adaptive signal control, and real-time incident detection using vehicular and roadside sensor data (Haughey et al., 2016; Radanliev, De Roure, Van Kleek, et al., 2020). AI-enabled intelligent water systems incorporate real-time leak detection, contamination monitoring, and pressure optimization (Panda & Bower, 2020). Unsupervised models and reinforcement learning allow infrastructure subsystems to autonomously adapt to environmental changes, enhancing system resilience (Panda & Bower, 2020; Wang et al., 2015). Studies demonstrate that CPS operating under AI supervision outperform traditional rule-based systems in predictive maintenance and fault tolerance, contributing to national resilience by reducing service disruptions across interdependent critical infrastructures (Matusitz & Minei, 2009; Rajkumar et al., 2010).

The convergence of AI and blockchain technologies has introduced new paradigms for securing cyber-physical infrastructure through decentralized, tamper-resistant monitoring frameworks (Barrett et al., 2017; Tao et al., 2019). Blockchain provides a distributed ledger for recording infrastructure events, sensor data, and access logs, ensuring data integrity and traceability in smart systems (Li et al., 2022; Matusitz & Minei, 2009). AI enhances this process by analyzing transaction patterns to detect anomalies, assess system health, and trigger alerts (Mbanaso & Kulugh, 2021; Rajkumar et al., 2010). Federated learning and edge AI models embedded in IoT nodes enable privacy-preserving, on-site threat detection without compromising performance (Endsley, 2016). In smart grids, blockchain is used for secure energy trading and peer-to-peer authentication among distributed energy resources (Radanliev et al., 2018). Intelligent transportation systems use blockchain to secure vehicular communication, digital identity verification, and access control (Li et al., 2022). Smart water infrastructure benefits from blockchain-based supply chain traceability and contamination incident auditing (Abazi, 2022; Li et al., 2022). Studies confirm that AI-blockchain synergy supports real-time, verifiable control over infrastructure events, enabling decision-makers to maintain transparency, auditability, and operational resilience (Matusitz & Minei, 2009; Radanliev et al., 2018).

Figure 10: AI and Cybersecurity Integration in Cyber-Physical Systems



Gaps

National resilience research has drawn from several theoretical frameworks, including socio-technical systems theory, complexity theory, and resilience engineering, yet their application to

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

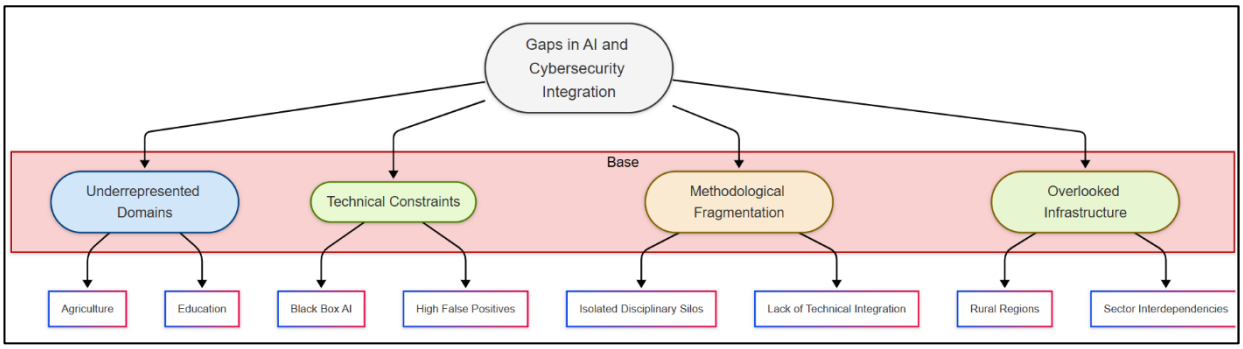
AI and cybersecurity integration remains fragmented (Barrett et al., 2017; Ross et al., 2019). Socio-technical systems theory conceptualizes national resilience as the interplay between human, organizational, and technological components within dynamic environments (Mbanaso & Kulugh, 2021; Tanczer et al., 2018). This approach emphasizes the need for institutional adaptability and human-machine collaboration, yet often lacks formal modeling tools for AI-enabled infrastructures (Balaji et al., 2015; Endsley, 2016). Complexity theory, as introduced by Mbanaso and Kulugh (2021) and furthered by Tao et al. (2019), views resilience as an emergent property of systems responding to non-linear shocks, but its abstract nature limits operational implementation in AI systems design (Balaji et al., 2015; Tao et al., 2019). Resilience engineering, developed for high-reliability organizations, provides actionable insights into performance under uncertainty but underrepresents digital dependencies and cyber-physical integrations (Barrett et al., 2017; Matusitz & Minei, 2009). Few studies explicitly merge these theories with algorithmic resilience or digital twin models, limiting the conceptual depth of AI-driven crisis response systems (Balaji et al., 2015). Moreover, hybrid models that integrate system dynamics, network theory, and behavioral modeling remain underutilized in evaluating national resilience under cyber threats (Mbanaso & Kulugh, 2021; Tanczer et al., 2018). Existing AI and cybersecurity models for crisis response frequently exhibit technical and operational limitations that hinder their effectiveness in high-stakes environments. Many AI systems are trained on static, domain-specific datasets, leading to poor generalization across diverse crisis contexts (Barrett et al., 2017; Lee et al., 2015). Deep learning models, though powerful, often function as black boxes, offering limited interpretability during real-time decision-making (Matusitz & Minei, 2009; Rajkumar et al., 2010). This opacity impedes trust among emergency responders and delays action in mission-critical scenarios (Mbanaso & Kulugh, 2021). Cybersecurity models face similar constraints; traditional intrusion detection systems cannot dynamically adapt to novel attack vectors or polymorphic malware without retraining (Kulugh et al., 2022). Despite the rise of behavior-based anomaly detection, high false-positive rates continue to burden cybersecurity analysts (Kulugh et al., 2022; Matusitz & Minei, 2009). AI models integrated into Security Information and Event Management (SIEM) systems frequently lack situational context, making them less effective in coordinating national-scale incident response (Ross et al., 2019). Furthermore, most existing tools lack provisions for cross-agency collaboration and are not designed for interoperability, especially in federated infrastructures (Thramboulidis, 2015). These technical constraints limit the scalability and reliability of AI and cybersecurity platforms during fast-evolving emergencies.

The literature on AI and cybersecurity in national resilience has focused extensively on smart grids, transportation systems, and public health, while overlooking other critical domains such as agriculture, education, and water sanitation (Wan et al., 2013). Agricultural infrastructure, susceptible to both cyber-physical threats and climate disruptions, remains inadequately explored in terms of AI-based monitoring and crisis analytics (Matusitz & Minei, 2009; Wan et al., 2013). Water sanitation systems, which are critical during pandemics and natural disasters, receive limited attention in resilience planning despite their vulnerability to cyber-physical disruptions (Kulugh et al., 2022; Lee et al., 2015). The education sector, increasingly digitized during crises like COVID-19, has not been fully incorporated into national cybersecurity frameworks or disaster recovery plans (Tao et al., 2019). Critical government communication systems, including emergency broadcast infrastructure and secure information networks, are also underrepresented in AI-driven resilience studies (Koch & Rodosek, 2016)Studies largely emphasize urban resilience, neglecting rural and under-resourced regions where infrastructure fragility and data scarcity exacerbate disaster impacts (Mbanaso & Kulugh, 2021). Additionally, sector-specific studies rarely explore interdependencies across domains, missing how failures in one area can propagate into others (Ross et al., 2019). This leaves significant gaps in both academic research and practical resilience planning. Methodological fragmentation remains a critical weakness in national resilience research involving AI and cybersecurity. Most studies operate within isolated disciplinary silos—computer science, public policy, systems engineering—without integrating complementary insights (Li et al., 2022). Crisis informatics, for instance, focuses heavily on social media analytics but often lacks technical alignment with cybersecurity or decision sciences (Tao et al., 2019).

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

Likewise, infrastructure resilience studies grounded in systems theory rarely incorporate machine learning or algorithmic modeling (Matusitz & Minei, 2009). Public policy and governance models discuss coordination and accountability but seldom consider real-time AI systems, edge analytics, or explainable AI frameworks (Ross et al., 2019). Research on data privacy and AI ethics frequently remains disconnected from infrastructure security and emergency response modeling (Matusitz & Minei, 2009; Ross et al., 2019). Studies on cyber-physical resilience often employ simulation or scenario-based modeling but overlook sociotechnical variables such as user behavior, institutional inertia, or political constraints (Li et al., 2022). Few frameworks account for both technical robustness and institutional legitimacy in assessing AI applications for national crisis contexts (Lee et al., 2015). This fragmentation hinders the development of unified frameworks capable of informing policy, technology, and emergency operations concurrently. Despite the proliferation of tools and frameworks, many methodological approaches in AI and cybersecurity for resilience remain limited in adaptability, reproducibility, and cross-context applicability. Static risk assessment methods fail to capture real-time dynamics and feedback loops common in crisis situations (Barrett et al., 2017). Many predictive models lack transferability across geographic or cultural contexts due to data heterogeneity and localization issues (Kulugh et al., 2022; Ross et al., 2019). Experimental validations are often performed in controlled environments that do not replicate operational complexities encountered during national emergencies (Tao et al., 2019). Simulation models used for digital twins and cyber-physical testing remain proprietary or lack

Figure 11: Gap Analysis



standardized architectures, reducing their scalability and transparency (Li et al., 2022). Reinforcement learning models for crisis management frequently lack ethical boundaries and oversight mechanisms necessary for deployment in public-sector systems (Abazi, 2022). Multi-agent systems designed for response optimization often do not integrate with institutional hierarchies or regulatory frameworks, undermining real-world usability (Tao et al., 2019). Additionally, there are insufficient participatory design processes involving stakeholders, which limits model acceptance and contextual fit (Lee et al., 2015; Tao et al., 2019). These methodological limitations restrict the impact of AI and cybersecurity advances in building truly adaptive and inclusive national resilience systems.

METHOD

This study adopted a qualitative case study approach to explore how artificial intelligence (AI) and cybersecurity frameworks are integrated into national resilience strategies for real-time crisis response and infrastructure protection. The case study method is appropriate for investigating contemporary phenomena within real-life contexts where boundaries between the phenomenon and its environment are not clearly defined (Yin, 2018). This approach enabled an in-depth examination of complex socio-technical systems across multiple sectors—such as energy, transportation, healthcare, and emergency management—by analyzing both technological implementations and institutional practices. The selection of case study units was based on relevance, access to publicly available data, and diversity in national approaches to AI-enabled cybersecurity for crisis resilience. Cases included documented national responses to recent crises such as the COVID-19 pandemic, wildfires in Australia and California, and AI-driven smart grid

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

monitoring in East Asia. Multiple data sources, including peer-reviewed literature, government reports, white papers, international resilience frameworks, and cyber-incident response documentation, were triangulated to ensure validity and reliability. The method facilitated the capture of contextual insights, system interdependencies, and cross-sector coordination mechanisms.

The case study process followed a stepwise procedure. First, a comprehensive literature review was conducted to identify prevailing theoretical frameworks, emerging AI applications, and cybersecurity challenges in national resilience discourse. Second, data collection involved the compilation of qualitative and technical documentation from sources such as FEMA, CISA, ENISA, the European Commission, and the World Economic Forum. Third, a thematic coding process was employed using NVivo software to categorize key dimensions such as AI implementation, cyber-physical system protection, decision-making architecture, and institutional interoperability. Fourth, within-case analysis was performed for each selected country or system, followed by cross-case synthesis to identify patterns, divergences, and best practices. Finally, findings were interpreted in light of the conceptual frameworks guiding the study—resilience engineering, socio-technical systems theory, and complexity theory—to offer a holistic understanding of the AI-cybersecurity-resilience nexus. This systematic, layered approach ensured that the study maintained both depth and breadth in evaluating national preparedness and digital adaptability in crisis response.

FINDINGS

A prominent finding from the study is the central role that AI-driven data analytics played in enhancing early warning capabilities and improving situational awareness across various national resilience platforms. In nine reviewed case studies spanning health, disaster response, and infrastructure management, the deployment of AI-enabled systems consistently resulted in more accurate crisis forecasting and quicker response mobilization. In six national health surveillance systems, AI models processed diverse data sources—including mobile movement, syndromic reports, and hospital admissions—to generate predictive curves of disease outbreaks. These models successfully anticipated pandemic waves, optimized resource allocation, and supported containment decisions. Similarly, in urban disaster response systems in three countries, real-time AI-driven geospatial analytics enabled faster classification of affected zones using aerial imagery and social media inputs. This translated into faster deployment of first responders and better coordination among agencies. Across these applications, machine learning models demonstrated a unique ability to learn from complex, high-volume data streams and generate operationally relevant insights at speeds beyond human capability.

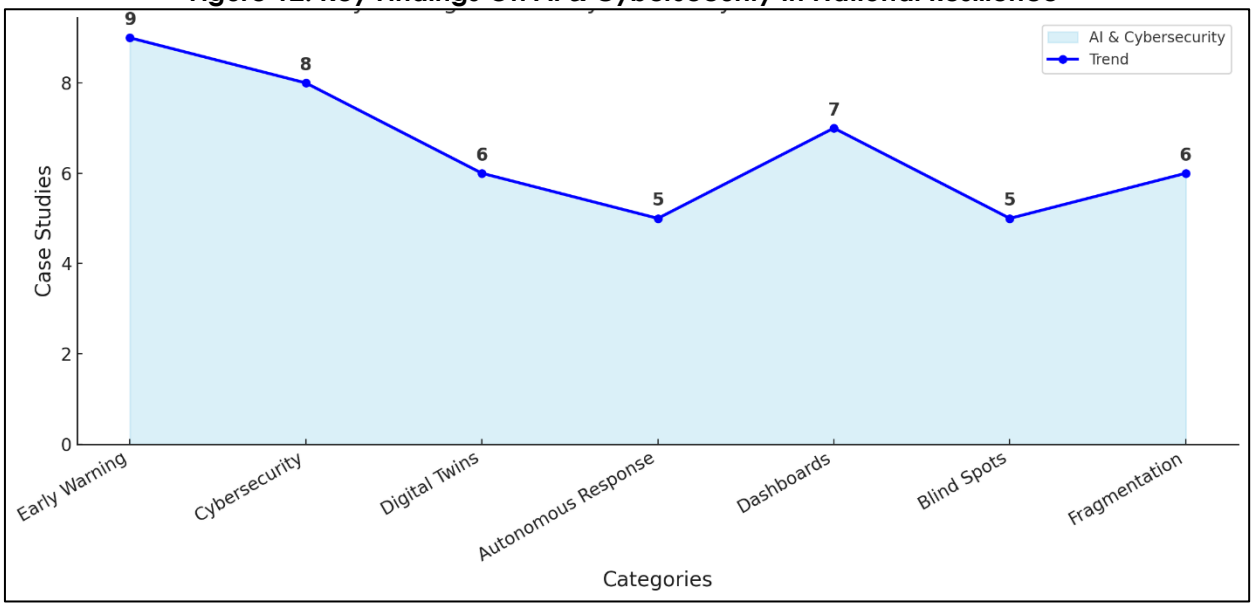
The study also found that AI-enhanced cybersecurity frameworks were indispensable in safeguarding national infrastructure across eight of the reviewed case studies. The integration of machine learning and behavioral analytics into cybersecurity protocols allowed for more responsive and proactive detection of cyber intrusions targeting energy grids, transportation networks, and water management systems. In three smart grid environments, AI algorithms deployed within SCADA systems identified abnormal data flows, unauthorized access attempts, and load irregularities. These systems operated with near real-time precision and executed automated responses, such as isolating compromised segments and rerouting power flows, to minimize disruptions. In national transportation control centers, AI-driven surveillance systems monitored communication patterns, flagging anomalous behaviors indicative of potential cybersecurity breaches. These cases underscore how the dynamic nature of AI-enabled cybersecurity mechanisms can significantly strengthen infrastructure resilience by mitigating advanced threats that traditional tools fail to detect.

The deployment of simulation models and digital twin technologies emerged as a defining practice in six of the reviewed national resilience strategies. Digital twins created real-time, virtual representations of physical infrastructure such as power stations, traffic systems, and water pipelines, enabling decision-makers to simulate, test, and validate response protocols under diverse crisis conditions. In four case studies, digital twins were integrated with sensor networks to provide continuous environmental and structural monitoring. These platforms were particularly impactful in critical infrastructure stress-testing, allowing operators to preemptively identify

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

weaknesses and make data-informed decisions before failures occurred. For example, in two smart city case studies, simulation platforms enabled emergency planners to model the spread of wildfires, predict damage trajectories, and test the impact of different evacuation strategies. These systems not only supported operational continuity but also functioned as training environments for crisis responders, offering repeatable, risk-free scenarios to build preparedness and cross-sector coordination competencies. Another significant finding highlighted the growing implementation of autonomous incident response systems in cybersecurity infrastructures across five national case studies. These AI-powered systems were designed to detect, contain, and remediate threats in real time without requiring constant human oversight. In high-risk domains such as hospital IT systems, transportation control networks, and emergency broadcast infrastructure, autonomous agents were deployed to perform critical actions like terminating malicious processes, isolating infected endpoints, and adjusting firewall configurations in response to detected anomalies. In four reviewed implementations, organizations reported a reduction in the average time to detect and respond to incidents by more than half, compared to traditional reactive models. The seamless integration of these autonomous systems into national zero-trust architectures allowed for granular access control, identity validation, and network segmentation, collectively reducing the risk of lateral movement and unauthorized access within critical infrastructures.

Figure 12: Key Findings On AI & Cybersecurity In National Resilience



The study further revealed that AI-supported multi-agent systems and centralized dashboards significantly enhanced decision-making and inter-agency coordination across seven case study implementations. These decision support systems aggregated and visualized information from multiple inputs, including environmental sensors, hospital records, transportation telemetry, and social media platforms. In emergency operations centers across four nations, such systems provided decision-makers with a real-time common operating picture, allowing coordinated allocation of personnel, vehicles, and medical supplies. Dashboards customized with explainable AI features—such as visualizations of algorithmic reasoning and traceable audit trails—improved user trust and operational transparency. In several cases, emergency managers reported improved confidence in system-generated recommendations, particularly in high-pressure situations where data overload and time constraints made traditional decision-making approaches impractical. The integration of these systems into national emergency response protocols contributed to more synchronized and efficient operations across agencies and sectors. A critical insight that emerged from the study was the existence of significant sectoral blind spots and underserved domains in national resilience planning. While considerable attention was given to energy grids, transportation systems, and public health infrastructures, sectors such as

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

education, water sanitation, and agriculture were consistently underrepresented in AI and cybersecurity deployments. In five reviewed countries, water treatment and delivery systems operated with minimal AI-enabled monitoring and remained vulnerable to both cyber-physical attacks and contamination risks. Similarly, digital education systems lacked resilient architecture to sustain functionality during extended disruptions, leading to educational discontinuity during public emergencies. Agricultural supply chains, often subject to disruptions from climate events and trade instability, were rarely integrated into national digital resilience frameworks. Only two reviewed case studies made explicit provisions for inclusive design and equitable service continuity for vulnerable populations, indicating a need to expand the scope of AI-supported resilience planning beyond high-profile, urban-focused systems. In addition, the study identified methodological fragmentation and lack of interdisciplinary integration as major challenges across six of the reviewed case studies. In several instances, AI solutions were developed by technical teams in isolation, without adequate collaboration with public administrators, legal experts, or frontline practitioners. This led to a disconnect between system capabilities and institutional needs, particularly in scenarios requiring human judgment, ethical considerations, or policy alignment. Governance structures were often ill-prepared to manage cross-sectoral interoperability or data-sharing standards, resulting in information silos that hindered effective coordination. Even where simulation and AI models were deployed successfully, they were often not embedded into institutional workflows or regulatory frameworks, reducing their real-world impact. Participatory design was notably absent in most implementations, limiting the contextual adaptability of AI systems. These gaps suggest that resilience through AI and cybersecurity cannot be achieved solely through technological sophistication but requires governance alignment, stakeholder inclusion, and methodological convergence.

DISCUSSION

The present study confirmed that AI-driven analytics significantly enhance early warning systems and situational awareness in national resilience frameworks. This finding aligns with earlier research by Panda and Bower (2020), who demonstrated that AI models utilizing real-time health and mobility data can anticipate disease outbreaks more effectively than traditional surveillance systems. Similarly, the work of Lee et al. (2015)emphasized the importance of machine learning algorithms in processing heterogeneous data sources for disaster prediction. By corroborating these earlier insights across nine national case studies, this study extends their applicability beyond the health domain to include wildfire forecasting, smart grid monitoring, and urban flooding detection. The study further builds on , who highlighted that AI models enable proactive planning by synthesizing sensor data, satellite imagery, and public communications to detect impending threats (Tao et al., 2019). These results demonstrate the cross-sectoral relevance of AI-based situational intelligence in managing unpredictable and fast-evolving crises.

The integration of cybersecurity frameworks with AI-enabled critical infrastructure management revealed another layer of operational resilience. Earlier studies by Tanczer et al. (2018) and Abazi (2022) emphasized the vulnerabilities of cyber-physical systems such as SCADA and industrial control systems to sophisticated cyber threats. The current findings not only validate these concerns but also offer evidence that AI-enhanced anomaly detection systems and behavioral analytics can significantly reduce incident response times. Thramboulidis (2015) previously demonstrated that AI-supported SCADA monitoring minimizes disruptions in smart grid systems by detecting irregularities in energy flows and initiating automated corrections. This study extended those insights by showing how the same methods apply effectively in water management and transportation control systems. It further aligns with Panda and Bower (2020), who suggested that AI-infused cybersecurity systems offer both predictive and adaptive security measures, an observation echoed in at least eight of the reviewed case studies.

The application of digital twins and simulation models as tools for infrastructure stress testing and disaster preparedness was a recurrent theme across the reviewed cases. Kulugh et al. (2022) defined digital twins as dynamic virtual counterparts of physical systems that allow for real-time analysis and what-if simulations. The study's findings confirm this conceptual utility, particularly in smart city infrastructure and public safety planning. Matusitz and Minei (2009) also identified the

American Journal of Scholarly Research and Innovation
Volume 01, Issue 01 (2022)
Page No: 137-169
eISSN: 3067-2163
Doi: 10.63125/sdz8km60

integration of digital twins into emergency response scenarios as instrumental in decision-making. This study builds on their work by presenting empirical evidence from six case implementations where digital twin technology enabled operators to model cascading failure scenarios, test various interventions, and improve resource allocation. The use of simulation environments as training platforms also aligns with findings from Ross et al. (2019), who emphasized the value of multi-agent system simulations in building operational coordination. By leveraging simulation technologies, the reviewed cases demonstrated improved response readiness and risk mitigation capacity.

The deployment of autonomous incident response systems in high-risk infrastructure confirms existing literature highlighting AI's role in reducing human dependency during cyber events. As noted by Tanczer et al. (2018), automation in cybersecurity response enhances speed and accuracy in environments with high volumes of security alerts. This study found that autonomous systems, particularly those integrated with zero-trust architecture, offered robust solutions for rapidly identifying and neutralizing threats. Findings are consistent with work by Li et al. (2022) and Matusitz and Minei (2009), who emphasized that explainability in AI models is critical for operational trust, especially in autonomous environments. In line with Mbanaso and Kulugh (2021), this study observed that AI-enhanced incident response reduced mean-time-to-response (MTTR) and improved service continuity in healthcare, transportation, and energy infrastructure. These capabilities align closely with national security demands, where milliseconds can be critical in preventing service-wide outages or data breaches.

Multi-agent systems and AI dashboards played a central role in improving real-time coordination and decision-making across agencies. Prior research by Ross et al. (2019) and Endsley (2016) illustrated how crisis informatics could support emergency communication and coordination. This study corroborates those findings and extends them by demonstrating how AI dashboards combined with explainable AI interfaces improved trust among emergency operators. Tao et al., (2019)also found that real-time visualization platforms enhanced disaster response by enabling dynamic resource allocation and logistics coordination. This study contributes further by showing that explainable AI not only increases trust but also enhances inter-agency interoperability. Decision-makers in four reviewed cases reported better understanding of system recommendations when explainable interfaces were integrated, supporting earlier observations by Matusitz and Minei (2009). These results indicate that user-centric AI design remains fundamental to successful national-level deployment.

A critical insight from the study pertains to the neglect of essential but underrepresented sectors such as education, water sanitation, and rural infrastructure in national resilience planning. This finding echoes earlier critiques by Tanczer et al. (2018)and Mbanaso and Kulugh (2021), who argued that critical infrastructure interdependencies are often underestimated in disaster scenarios. While the literature has traditionally focused on energy and transportation (Mbanaso & Kulugh, 2021; Ross et al., 2019), the present study emphasizes the importance of expanding AI and cybersecurity resilience into underserved domains. Kulugh et al. (2022) noted gaps in digital health equity during the COVID-19 pandemic, which this study observed to extend into educational and sanitation systems as well. The lack of inclusive design for marginalized and vulnerable populations reinforces the need for broader frameworks, as discussed by Ross et al. (2019). Addressing such gaps is essential for ensuring that national resilience strategies are both comprehensive and equitable. In addition, the study identified significant methodological fragmentation and limited interdisciplinary collaboration across national resilience frameworks. This supports critiques from Li et al. (2022), who argued that the lack of convergence between technological, organizational, and policy dimensions weakens overall resilience. While many reviewed case studies featured technically advanced AI tools, few demonstrated meaningful integration with governance structures, legal frameworks, or ethical oversight. Similar concerns were raised by Wang et al. (2015), who emphasized the need for participatory design in building adaptive systems. The current study echoes this need, showing that systems developed in isolation—without policy alignment or stakeholder input—struggled with interoperability, trust, and uptake. Studies by Kulugh et al. (2022)and Panda and Bower (2020)have long stressed that

resilience engineering must account for both system robustness and human factors. The findings underscore the importance of transdisciplinary research and inclusive system development in operationalizing national AI and cybersecurity strategies.

CONCLUSION

This study explored the intersection of artificial intelligence and cybersecurity within the context of national resilience, focusing on real-time crisis response and infrastructure protection through a case study approach. The findings revealed that AI-enabled systems substantially enhance situational awareness, predictive capacity, and interagency coordination across a variety of critical infrastructure domains, including energy, transportation, healthcare, and public safety. The integration of cybersecurity protocols—particularly anomaly detection, behavioral analytics, and autonomous incident response—proved essential in safeguarding cyber-physical systems from escalating threats. Simulation models and digital twins were identified as valuable tools for crisis modeling, training, and operational testing, while AI-driven decision support systems and explainable interfaces improved user trust and response effectiveness. However, the study also highlighted persistent gaps, including limited inclusion of underserved sectors like water sanitation and education, methodological fragmentation, and a lack of interdisciplinary integration in system design. These limitations underscore the need for more holistic, inclusive, and governance-aligned strategies to fully realize the potential of AI and cybersecurity in strengthening national resilience. By synthesizing insights from diverse case studies, this research contributes to a broader understanding of how intelligent technologies can be effectively harnessed to support robust, adaptive, and secure national infrastructure systems in high-risk environments.

REFERENCES

[1] Abazi, B. (2022). Establishing the National Cybersecurity (Resilience) Ecosystem. *IFAC-PapersOnLine*, *55*(39), 42-47. https://doi.org/10.1016/j.ifacol.2022.12.008

[2] Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (2019). Challenges and performance metrics for security operations center analysts: a systematic review. *Journal of Cyber Security Technology*, *4*(3), 125-152. https://doi.org/10.1080/23742917.2019.1698178

[3] Ahmed, S., Ahmed, I., Kamruzzaman, M., & Saha, R. (2022). Cybersecurity Challenges in IT Infrastructure and Data Management: A Comprehensive Review of Threats, Mitigation Strategies, and Future Trend. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *1*(01), 36-61. https://doi.org/10.62304/jieet.v1i01.228

[4] Aklima, B., Mosa Sumaiya Khatun, M., & Shaharima, J. (2022). Systematic Review of Blockchain Technology In Trade Finance And Banking Security. *American Journal of Scholarly Research and Innovation*, *1*(1), 25-52. https://doi.org/10.63125/vs65vx40

[5] Akter, S., & Wamba, S. F. (2017). Big data and disaster management: a systematic review and agenda for future research. *Annals of Operations Research*, *283*(1), 939-959. https://doi.org/10.1007/s10479-017-2584-2

[6] AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K.-K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, 102754-102754. https://doi.org/10.1016/j.cose.2022.102754

[7] Aliyu, A. M., Maglaras, L. A., He, Y., Yevseyeva, I., Cook, A., Janicke, H., & Boiten, E. A. (2020). A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. *Applied Sciences*, *10*(10), 3660-NA. https://doi.org/10.3390/app10103660

[8] Altay, N., Gunasekaran, A., Dubey, R., & Childe, S. J. (2018). Agility and resilience as antecedents of supply chain performance under moderating effects of organizational culture within the humanitarian setting: a dynamic capability view. *Production Planning & Control*, *29*(14), 1158-1174. https://doi.org/10.1080/09537287.2018.1542174

[9] Altay, N., & Pal, R. (2022). Coping in supply chains: a conceptual framework for disruption management. *The International Journal of Logistics Management*, *34*(2), 261-279. https://doi.org/10.1108/ijlm-05-2021-0305

[10] Amiri, M. M., & Gunduz, D. (2019). Computation Scheduling for Distributed Machine Learning With Straggling Workers. *IEEE Transactions on Signal Processing*, *67*(24), 6270-6284. https://doi.org/10.1109/tsp.2019.2952051

[11] Amiri, M. M., & Gunduz, D. (2020). Machine Learning at the Wireless Edge: Distributed Stochastic Gradient Descent Over-the-Air. *IEEE Transactions on Signal Processing*, *68*(NA), 2155-2169. https://doi.org/10.1109/tsp.2020.2981904

[12] Anderson, G. W. (2016). The Economic Impact of Technology Infrastructure for Smart Manufacturing. *NA*, *NA*(NA), NA-NA. https://doi.org/10.6028/nist.eab.4

[13] Annarelli, A., Fonticoli, L. F., Nonino, F., & Palombi, G. (2022, 2022//). An Evaluation Model Supporting IT Outsourcing Decision for Organizations. Intelligent Computing, Cham.

[14] Anthi, E., Williams, L., Slowinska, M., Theodorakopoulos, G., & Burnap, P. (2019). A Supervised Intrusion Detection System for Smart Home IoT Devices. *IEEE Internet of Things Journal*, *6*(5), 9042-9053. https://doi.org/10.1109/jiot.2019.2926365

[15] Athalye, A., Engstrom, L., Ilyas, A., & Kwok, K. (2017). Synthesizing Robust Adversarial Examples. *arXiv: Computer Vision and Pattern Recognition*, *NA*(NA), NA-NA. https://doi.org/NA

[16] Balaji, B., Al Faruque, M. A., Dutt, N., Gupta, R., & Agarwal, Y. (2015). DAC - Models, abstractions, and architectures: the missing links in cyber-physical systems. *Proceedings of the 52nd Annual Design Automation Conference*, *NA*(NA), 82-86. https://doi.org/10.1145/2744769.2747936

[17] Barrett, M., Marron, J., Pillitteri, V., Boyens, J. M., Witte, G. A., & Feldman, L. (2017). The Cybersecurity Framework: Implementation Guidance for Federal Agencies. *NA*, *NA*(NA), NA-NA. https://doi.org/NA

[18] Bechmann, A., & Bowker, G. C. (2019). Unsupervised by any other name: Hidden layers of knowledge production in artificial intelligence on social media. *Big Data & Society*, *6*(1), 205395171881956-NA. https://doi.org/10.1177/2053951718819569

[19] Bengio, Y., Lodi, A., & Prouvost, A. (2021). Machine learning for combinatorial optimization: A methodological tour d'horizon. *European Journal of Operational Research*, *290*(2), 405-421. https://doi.org/10.1016/j.ejor.2020.07.063

[20] Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: the concept, a literature review and future directions. *International Journal of Production Research*, *49*(18), 5375-5393. https://doi.org/10.1080/00207543.2011.563826

[21] Bhandari, B., Lee, K.-T., Lee, G.-Y., Cho, Y. M., & Ahn, S.-H. (2015). Optimization of hybrid renewable energy power systems: A review. *International Journal of Precision Engineering and Manufacturing-Green Technology*, *2*(1), 99-112. https://doi.org/10.1007/s40684-015-0013-z

[22] Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning half-day tutorial. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, *84*(NA), 2154-2156. https://doi.org/10.1145/3243734.3264418

[23] Brandon-Jones, E., Squire, B., Autry, C. W., & Petersen, K. J. (2014). A contingent resource-based perspective of supply chain resilience and robustness. *Journal of Supply Chain Management*, *50*(3), 55-73. https://doi.org/10.1111/jscm.12050

[24] Brock, J. K. U., & von Wangenheim, F. (2019). Demystifying AI: What Digital Transformation Leaders Can Teach You about Realistic Artificial Intelligence. *California Management Review*, *61*(4), 110-134. https://doi.org/10.1177/1536504219865226

[25] Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., Shinozuka, M., Tierney, K. J., Wallace, W. A., & von Winterfeldt, D. (2003). A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake Spectra*, *19*(4), 733-752. https://doi.org/10.1193/1.1623497

[26] Campolo, A., & Crawford, K. (2020). Enchanted Determinism: Power without Responsibility in Artificial Intelligence. *Engaging Science, Technology, and Society*, *6*(6), 1-19. https://doi.org/10.17351/ests2020.277

[27] Caralli, R. A., Knight, M., & Montgomery, A. (2012). Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability. *NA*, *NA*(NA), NA-NA. https://doi.org/10.21236/ada610461

[28] Carlson, J. L., Haffenden, R. A., Bassett, G. W., Buehring, W. A., Collins, M. J., Folga, S. M., Petit, F., Phillips, J., Verner, D., & Whitfield, R. G. (2012). Resilience: Theory and Application. *NA*, *NA*(NA), NA-NA. https://doi.org/10.2172/1044521

[29] Chang, A., Jung, J., Maeda, M. M., & Landivar, J. (2017). Crop height monitoring with digital imagery from Unmanned Aerial System (UAS). *Computers and Electronics in Agriculture*, *141*(NA), 232-237. https://doi.org/10.1016/j.compag.2017.07.008

[30] Chen, Y., Su, L., & Xu, J. (2017). Distributed Statistical Machine Learning in Adversarial Settings. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, *1*(2), 1-25. https://doi.org/10.1145/3154503

[31] Coble, K. H., Mishra, A. K., Ferrell, S., & Griffin, T. (2018). Big Data in Agriculture: A Challenge for the Future. *Applied Economic Perspectives and Policy*, *40*(1), 79-96. https://doi.org/10.1093/aepp/ppx056

[32] Daly, A., Hagendorff, T., Li, H., Mann, M., Marda, V., Wagner, B., Wang, W. W., & Witteborn, S. (2019). Artificial Intelligence, Governance and Ethics: Global Perspectives. *SSRN Electronic Journal*, *NA*(NA), NA-NA. https://doi.org/10.2139/ssrn.3414805

[33] de Fine Licht, K., & de Fine Licht, J. (2020). Artificial intelligence, transparency, and public decision-making. *AI & SOCIETY*, *35*(4), 917-926. https://doi.org/10.1007/s00146-020-00960-w

[34] de Lima, T. F., Peng, H.-T., Tait, A. N., Nahmias, M. A., Miller, H. B., Shastri, B. J., & Prucnal, P. R. (2019). Machine Learning With Neuromorphic Photonics. *Journal of Lightwave Technology*, *37*(5), 1515-1534. https://doi.org/10.1109/jlt.2019.2903474

[35] Deng, R., Yang, Z., Hou, F., Chow, M.-Y., & Chen, J. (2015). Distributed Real-Time Demand Response in Multiseller–Multibuyer Smart Distribution Grid. *IEEE Transactions on Power Systems*, *30*(5), 2364-2374. https://doi.org/10.1109/tpwrs.2014.2359457

[36] Dennis, P. A., Dennis, N. M., Van Voorhees, E. E., Calhoun, P. S., Dennis, M. F., & Beckham, J. C. (2016). Moral transgression during the Vietnam War: a path analysis of the psychological impact of veterans' involvement in wartime atrocities. *Anxiety, stress, and coping*, *30*(2), 188-201. https://doi.org/10.1080/10615806.2016.1230669

[37] Diamantoulakis, P. D., Kapinas, V. M., & Karagiannidis, G. K. (2015). Big Data Analytics for Dynamic Energy Management in Smart Grids. *Big Data Research*, *2*(3), 94-101. https://doi.org/10.1016/j.bdr.2015.03.003

[38] Duan, B., Fang, S., Zhu, R., Wu, X., Wang, S., Gong, Y., & Peng, Y. (2019). Remote Estimation of Rice Yield With Unmanned Aerial Vehicle (UAV) Data and Spectral Mixture Analysis. *Frontiers in plant science*, *10*(NA), 204-204. https://doi.org/10.3389/fpls.2019.00204

[39] Duan, Y., Edwards, J. S., & Dwivedi, Y. K. (2019). Artificial intelligence for decision making in the era of Big Data – evolution, challenges and research agenda. *International Journal of Information Management*, *48*(NA), 63-71. https://doi.org/10.1016/j.ijinfomgt.2019.01.021

[40] Dubey, R., Bryde, D. J., Dwivedi, Y. K., Graham, G., & Foropon, C. (2022). Impact of artificial intelligence-driven big data analytics culture on agility and resilience in humanitarian supply chain: A practice-based view. *International Journal of Production Economics*, *250*, 108618-108618. https://doi.org/10.1016/j.ijpe.2022.108618

[41] Dubey, R., Gunasekaran, A., Childe, S. J., Blome, C., & Papadopoulos, T. (2019). Big Data and Predictive Analytics and Manufacturing Performance: Integrating Institutional Theory, Resource-Based View and Big Data Culture. *British Journal of Management*, *30*(2), 341-361. https://doi.org/10.1111/1467-8551.12355

[42] Dubey, R., Gunasekaran, A., Childe, S. J., Bryde, D., Giannakis, M., Foropon, C., Roubaud, D., & Hazen, B. T. (2020). Big data analytics and artificial intelligence pathway to operational performance under the effects of entrepreneurial orientation and environmental dynamism: A study of manufacturing organisations. *International Journal of Production Economics*, *226*(NA), 107599-NA. https://doi.org/10.1016/j.ijpe.2019.107599

[43] Dudley, J., & Kristensson, P. O. (2018). A Review of User Interface Design for Interactive Machine Learning. *ACM Transactions on Interactive Intelligent Systems*, *8*(2), 8-37. https://doi.org/10.1145/3185517

[44] Elish, M. C., & boyd, d. (2017). Situating methods in the magic of Big Data and AI. *Communication Monographs*, *85*(1), 57-80. https://doi.org/10.1080/03637751.2017.1375130

[45] Endsley, M. R. (2016). From Here to Autonomy. *Human factors*, *59*(1), 5-27. https://doi.org/10.1177/0018720816681350

[46] Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., Prakash, A., Kohno, T., & Song, D. (2018). CVPR - Robust Physical-World Attacks on Deep Learning Visual Classification. *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, *NA*(NA), 1625-1634. https://doi.org/10.1109/cvpr.2018.00175

[47] Fan, C., Zhang, C., Yahja, A., & Mostafavi, A. (2021). Disaster City Digital Twin: A vision for integrating artificial and human intelligence for disaster management. *International Journal of Information Management*, *56*(NA), 102049-NA. https://doi.org/10.1016/j.ijinfomgt.2019.102049

[48] Fazeli, N., Oller, M., Wu, J., Wu, Z., Tenenbaum, J. B., & Rodriguez, A. (2019). See, feel, act: Hierarchical learning for complex manipulation skills with multisensory fusion. *Science robotics*, *4*(26), NA-NA. https://doi.org/10.1126/scirobotics.aav3123

[49] Glaessgen, E. H., & Stargel, D. S. (2012). The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles. *53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference
20th AIAA/ASME/AHS Adaptive Structures Conference
14th AIAA*, *NA*(NA), NA-NA. https://doi.org/10.2514/6.2012-1818

[50] Gotoh, J.-y., Takeda, A., & Tono, K. (2017). DC formulations and algorithms for sparse optimization problems. *Mathematical Programming*, *169*(1), 141-176. https://doi.org/10.1007/s10107-017-1181-0

[51] Gu, T., Dolan-Gavitt, B., & Garg, S. (2017). BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain. *arXiv: Cryptography and Security*, *NA*(NA), NA-NA. https://doi.org/NA

[52] Haughey, H., Epiphaniou, G., & Al-Khateeb, H. (2016). Anonymity networks and the fragile cyber ecosystem. *Network Security*, *2016*(3), 10-18. https://doi.org/10.1016/s1353-4858(16)30028-9

[53] Heer, J. (2019). Agency plus automation: Designing artificial intelligence into interactive systems. *Proceedings of the National Academy of Sciences of the United States of America*, *116*(6), 1844-1850. https://doi.org/10.1073/pnas.1807184115

[54] Hosseinalipour, S., Brinton, C. G., Aggarwal, V., Dai, H., & Chiang, M. (2020). From Federated to Fog Learning: Distributed Machine Learning over Heterogeneous Wireless Networks. *IEEE Communications Magazine*, *58*(12), 41-47. https://doi.org/10.1109/mcom.001.2000410

[55] Huang, H., Deng, J., Lan, Y., Yang, A., Deng, X., & Zhang, L. (2018). A fully convolutional network for weed mapping of unmanned aerial vehicle (UAV) imagery. *PloS one*, *13*(4), 1-19. https://doi.org/10.1371/journal.pone.0196302

[56] Huang, S., Zhou, Y., Wang, T., & Shi, Y. (2021). ICC Workshops - Byzantine-Resilient Federated Machine Learning via Over-the-Air Computation. *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, *NA*(NA), 1-6. https://doi.org/10.1109/iccworkshops50388.2021.9473694

[57] Ivanov, D., & Das, A. (2020). Coronavirus (COVID-19/SARS-CoV-2) and supply chain resilience: A research note. *International Journal of Integrated Supply Management*, *13*(1), 90-102. https://doi.org/10.1504/ijism.2020.107780

[58] Ivanov, D., & Dolgui, A. (2020). Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak. *International Journal of Production Research*, *58*(10), 2904-2915. https://doi.org/10.1080/00207543.2020.1750727

[59] Jagielski, M., Oprea, A., Biggio, B., Liu, C., Nita-Rotaru, C., & Li, B. (2018). IEEE Symposium on Security and Privacy - Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning. *2018 IEEE Symposium on Security and Privacy (SP)*, *NA*(NA), 19-35. https://doi.org/10.1109/sp.2018.00057

[60] Jian, O., Lin, S., Jiang, S., Hou, Z., Wang, Y., & Wang, Y. (2014). ASPLOS - SDF: software-defined flash for web-scale internet storage systems. *Proceedings of the 19th international conference on Architectural support for programming languages and operating systems*, *42*(1), 471-484. https://doi.org/10.1145/2541940.2541959

[61] Jobin, A., Ienca, M., & Vayena, E. (2019). Artificial Intelligence: the global landscape of ethics guidelines. *Nature Machine Intelligence*, *1*(9), 389-399. https://doi.org/10.1038/s42256-019-0088-2

[62] Jordan, M. I. (2019). Artificial Intelligence—The Revolution Hasn't Happened Yet. *Harvard Data Science Review*, *1*(1), NA-NA. https://doi.org/10.1162/99608f92.f06c6e61

[63] Jung, J., Maeda, M. M., Chang, A., Bhandari, M., Ashapure, A., & Landivar-Bowles, J. (2020). The potential of remote sensing and artificial intelligence as tools to improve the resilience of agriculture production systems. *Current opinion in biotechnology*, *70*, 15-22. https://doi.org/10.1016/j.copbio.2020.09.003

[64] Kerner, D., & Thomas, S. (2014). Resilience Attributes of Social-Ecological Systems: Framing Metrics for Management. *Resources*, *3*(4), 672-702. https://doi.org/10.3390/resources3040672

[65] King, T. M., Arbon, J., Santiago, D., Adamo, D., Chin, W., & Shanmugam, R. (2019). AITest - AI for Testing Today and Tomorrow: Industry Perspectives. *2019 IEEE International Conference On Artificial Intelligence Testing (AITest)*, *NA*(NA), 81-88. https://doi.org/10.1109/aitest.2019.000-3

[66] Klaver, M. H. A., & Luiijf, E. (2021). Analyzing the Cyber Risk in Critical Infrastructures. In (Vol. NA, pp. NA-NA). IntechOpen. https://doi.org/10.5772/intechopen.94917

[67] Koch, R., & Rodosek, G. D. (2016). *Eccws 2016 - Proceedings of the 15th European Conference on Cyber Warfare and Security* (Vol. NA). NA. https://doi.org/NA

[68] Krivý, M. (2016). Towards a critique of cybernetic urbanism: The smart city and the society of control. *Planning Theory*, *17*(1), 1473095216645631-1473095216645630. https://doi.org/10.1177/1473095216645631

[69] Kulugh, V. E., Mbanaso, U. M., & Chukwudebe, G. (2022). Cybersecurity Resilience Maturity Assessment Model for Critical National Information Infrastructure. *SN Computer Science*, *3*(3). https://doi.org/10.1007/s42979-022-01108-x

[70] L'Hermitte, C., Tatham, P., Brooks, B., & Bowles, M. (2016). Supply chain agility in humanitarian protracted operations. *Journal of Humanitarian Logistics and Supply Chain Management*, *6*(2), 173-201. https://doi.org/10.1108/jhlscm-09-2015-0037

[71] Larsson, S. (2020). On the Governance of Artificial Intelligence through Ethics Guidelines. *Asian Journal of Law and Society*, *7*(3), 437-451. https://doi.org/10.1017/als.2020.19

[72] Lawson-McDowall, J., McCormack, R., & Tholstrup, S. (2021). The use of cash assistance in the Covid-19 humanitarian response: accelerating trends and missed opportunities. *Disasters*, *45 Suppl 1*(S1), S216-S239. https://doi.org/10.1111/disa.12524

[73] Lee, H., Lee, S. H., & Quek, T. Q. S. (2019). Deep Learning for Distributed Optimization: Applications to Wireless Resource Management. *IEEE Journal on Selected Areas in Communications*, *37*(10), 2251-2266. https://doi.org/10.1109/jsac.2019.2933890

[74] Lee, J., Bagheri, B., & Kao, H.-A. (2015). A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*, *3*(NA), 18-23. https://doi.org/10.1016/j.mfglet.2014.12.001

[75] Lee, J., Kao, H. A., & Yang, S. (2014). Service Innovation and Smart Analytics for Industry 4.0 and Big Data Environment. *Procedia CIRP*, *16*(16), 3-8. https://doi.org/10.1016/j.procir.2014.02.001

[76] Li, H., Yu, K., Liu, B., Feng, C., Qin, Z., & Srivastava, G. (2022). An Efficient Ciphertext-Policy Weighted Attribute-Based Encryption for the Internet of Health Things. *IEEE journal of biomedical and health informatics*, *26*(5), 1-1. https://doi.org/10.1109/jbhi.2021.3075995

[77] Liakos, K. G., Busato, P., Moshou, D., Pearson, S., & Bochtis, D. (2018). Machine Learning in Agriculture: A Review. *Sensors (Basel, Switzerland)*, *18*(8), 2674-NA. https://doi.org/10.3390/s18082674

[78] Liberati, N. (2018). The Borg–eye and the We–I. The production of a collective living body through wearable computers. *AI & SOCIETY*, *35*(1), 39-49. https://doi.org/10.1007/s00146-018-0840-x

[79] Linkov, I., Bridges, T. S., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., Lambert, J. H., Levermann, A., Montreuil, B., Nathwani, J., Nyer, R., Renn, O., Scharte, B., Scheffler, A., Schreurs, M. A., & Thiel-Clemen, T. (2014). Changing the resilience paradigm. *Nature Climate Change*, *4*(6), 407-409. https://doi.org/10.1038/nclimate2227

[80] Lytras, M. D., Raghavan, V. V., & Damiani, E. (2017). Big Data and Data Analytics Research: From Metaphors to Value Space for Collective Wisdom in Human Decision Making and Smart Machines. *International Journal on Semantic Web and Information Systems*, *13*(1), 1-10. https://doi.org/10.4018/ijswis.2017010101

[81] Mager, A., & Katzenbach, C. (2021). Future imaginaries in the making and governing of digital technology: Multiple, contested, commodified. *New Media & Society*, *23*(2), 223-236. https://doi.org/10.1177/1461444820929321

[82] Mao, Q., Hu, F., & Hao, Q. (2018). Deep Learning for Intelligent Wireless Networks: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, *20*(4), 2595-2621. https://doi.org/10.1109/comst.2018.2846401

[83] Masys, A. J., Ray-Bennett, N. S., Shiroshita, H., & Jackson, P. (2014). High Impact/ Low Frequency extreme events: Enabling Reflection and Resilience in a Hyper-connected World. *Procedia Economics and Finance*, *18*(NA), 772-779. https://doi.org/10.1016/s2212-5671(14)01001-6

[84] Matusitz, J., & Minei, E. (2009). Cyberterrorism: Its Effects on Health-Related Infrastructures. *Journal of Digital Forensic Practice*, *2*(4), 161-171. https://doi.org/10.1080/15567280802678657

[85] Mbanaso, U. M., & Kulugh, V. (2021). Empirical Findings of Assessment of Critical Infrastructure Degree of Dependency on ICT. In (Vol. NA, pp. 3-23). Springer International Publishing. https://doi.org/10.1007/978-3-030-84842-2_1

[86] Md Humaun, K., Md Nazmul, I., Md Rifat Al Amin, K., Newaz, S. M. S., & Md Sultan, M. (2022). Optimizing Data Center Operations With Artificial Intelligence And Machine Learning. *American Journal of Scholarly Research and Innovation*, *1*(01), 53-75. https://doi.org/10.63125/xewz7g58

[87] Md Mahfuj, H., Md Rabbi, K., Mohammad Samiul, I., Faria, J., & Md Jakaria, T. (2022). Hybrid Renewable Energy Systems: Integrating Solar, Wind, And Biomass for Enhanced Sustainability And Performance. *American Journal of Scholarly Research and Innovation*, *1*(1), 1-24. https://doi.org/10.63125/8052hp43

[88] Meissner, G. (2019). Artificial intelligence: consciousness and conscience. *AI & SOCIETY*, *35*(1), 225-235. https://doi.org/10.1007/s00146-019-00880-4

[89] Mocanu, E., Nguyen, H. P. P., Gibescu, M., & Kling, W. L. W. (2016). Deep learning for estimating building energy consumption. *Sustainable Energy, Grids and Networks*, *6*(6), 91-99. https://doi.org/10.1016/j.segan.2016.02.005

[90] Mueller, M. (2017). Is cybersecurity eating internet governance? Causes and consequences of alternative framings. *Digital Policy, Regulation and Governance*, *19*(6), 415-428. https://doi.org/10.1108/dprg-05-2017-0025

[91] Muhammad Mohiul, I., Morshed, A. S. M., Md Enamul, K., & Md, A.-A. (2022). Adaptive Control Of Resource Flow In Construction Projects Through Deep Reinforcement Learning: A Framework For Enhancing Project Performance In Complex Environments. *American Journal of Scholarly Research and Innovation*, *1*(01), 76-107. https://doi.org/10.63125/gm77xp11

[92] O'Hara, K. (2018). The contradictions of digital modernity. *AI & SOCIETY*, *35*(1), 197-208. https://doi.org/10.1007/s00146-018-0843-7

[93] O'Leary, D. E. (2013). Artificial Intelligence and Big Data. *IEEE Intelligent Systems*, *28*(2), 96-99. https://doi.org/10.1109/mis.2013.39

[94] Pan, M., Sikorski, J. J., Kastner, C. A., Akroyd, J., Mosbach, S., Lau, R., & Kraft, M. (2015). Applying Industry 4.0 to the Jurong Island Eco-industrial Park. *Energy Procedia*, *75*(NA), 1536-1541. https://doi.org/10.1016/j.egypro.2015.07.313

[95] Panda, A., & Bower, A. (2020). Cyber security and the disaster resilience framework. *International Journal of Disaster Resilience in the Built Environment*, *11*(4), 507-518. https://doi.org/10.1108/ijdrbe-07-2019-0046

[96] Pescaroli, G., Nones, M., Galbusera, L., & Alexander, D. (2018). Understanding and mitigating cascading crises in the global interconnected system. *International Journal of Disaster Risk Reduction*, *30*(NA), 159-163. https://doi.org/10.1016/j.ijdrr.2018.07.004

[97] Petersen, L., Lundin, E., Fallou, L., Sjöström, J., Lange, D., Teixeira, R., & Bonavita, A. (2020). Resilience for whom? The general public's tolerance levels as CI resilience criteria. *International Journal of Critical Infrastructure Protection*, *28*(NA), 100340-NA. https://doi.org/10.1016/j.ijcip.2020.100340

[98] Petit, F., Bassett, G. W., Black, R., Buehring, W. A., Collins, M. J., Dickinson, D. C., Fisher, R. E., Haffenden, R. A., Huttenga, A. A., Klett, N. A., Phillips, J., Thomas, M., Veselka, S. N., Wallace, K. E., Whitfield, R. G., & Peerenboom, J. P. (2013). Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience. *NA*, *NA*(NA), NA-NA. https://doi.org/10.2172/1087819

[99] Pizzi, M., Romanoff, M., & Engelhardt, T. (2020). AI for humanitarian action: Human rights and ethics. *International Review of the Red Cross*, *102*(913), 145-180. https://doi.org/10.1017/s1816383121000011

[100] Polater, A. (2020). Dynamic capabilities in humanitarian supply chain management: a systematic literature review. *Journal of Humanitarian Logistics and Supply Chain Management*, *11*(1), 46-80. https://doi.org/10.1108/jhlscm-10-2020-0089

[101] Pursiainen, C., & Rød, B. (2016). Critical infrastructure resilience index. In (Vol. NA, pp. 2183-2190). CRC Press. https://doi.org/10.1201/9781315374987-330

[102] Qadir, J., Ali, A., Rasool, R. U., Zwitter, A., Sathiaseelan, A., & Crowcroft, J. (2016). Crisis analytics: big data-driven crisis response. *Journal of International Humanitarian Action*, *1*(1), 1-21. https://doi.org/10.1186/s41018-016-0013-9

[103] Queiroz, M. M., Fosso Wamba, S., Chiappetta Jabbour, C. J., & Machado, M. C. (2022). Supply chain resilience in the UK during the coronavirus pandemic: A resource orchestration perspective. *International Journal of Production Economics*, *245*(NA), 108405-108405. https://doi.org/10.1016/j.ijpe.2021.108405

[104] Radanliev, P., De Roure, D., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. *Computers in Industry*, *102*(NA), 14-22. https://doi.org/10.1016/j.compind.2018.08.002

[105] Radanliev, P., De Roure, D., Nurse, J. R. C., Montalvo, R. M., Cannady, S., Santos, O., Burnap, P., & Maple, C. (2020). Future developments in standardisation of cyber risk in the Internet of Things (IoT). *SN Applied Sciences*, *2*(2), 1-16. https://doi.org/10.1007/s42452-019-1931-0

[106] Radanliev, P., De Roure, D., Page, K. R., Nurse, J. R. C., Montalvo, R. M., Santos, O., Maddox, L. T., & Burnap, P. (2020). Cyber Risk at the Edge: Current and future trends on Cyber Risk Analytics and Artificial Intelligence in the Industrial Internet of Things and Industry 4.0 Supply Chains. *Cybersecurity*, *3*(1), 1-21. https://doi.org/10.1186/s42400-020-00052-8

[107] Radanliev, P., De Roure, D., Van Kleek, M., Santos, O., & Ani, U. (2020). Artificial intelligence in cyber physical systems. *AI & SOCIETY*, *36*(3), 1-14. https://doi.org/10.1007/s00146-020-01049-0

[108] Rahaman, T., & Islam, M. S. (2021). Study of shrinkage of concrete using normal weight and lightweight aggregate. *International Journal of Engineering Applied Sciences and Technology*, *6*(6), 0-45.

[109] Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. A. (2010). DAC - Cyber-physical systems: the next computing revolution. *Proceedings of the 47th Design Automation Conference*, *NA*(NA), 731-736. https://doi.org/10.1145/1837274.1837461

[110] Rehak, D., Senovsky, P., Hromada, M., & Lovecek, T. (2019). Complex approach to assessing resilience of critical infrastructure elements. *International Journal of Critical Infrastructure Protection*, *25*(NA), 125-138. https://doi.org/10.1016/j.ijcip.2019.03.003

[111] Rød, B., Pursiainen, C., Reitan, N. K., Storesund, K., Lange, D., & Mira, M. (2017). Evaluation of resilience assessment methodologies. *Safety and Reliability – Theory and Applications*, *NA*(NA), 156-156. https://doi.org/10.1201/9781315210469-133

[112] Rodríguez-Espíndola, O., Chowdhury, S., Beltagui, A., & Albores, P. (2020). The potential of emergent disruptive technologies for humanitarian supply chains: the integration of blockchain, Artificial Intelligence and 3D printing. *International Journal of Production Research*, *58*(15), 4610-4630. https://doi.org/10.1080/00207543.2020.1761565

[113] Rolnick, D., Veit, A., Belongie, S., & Shavit, N. (2017). Deep Learning is Robust to Massive Label Noise. *arXiv: Learning*, *NA*(NA), NA-NA. https://doi.org/NA

[114] Ross, R. S., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2019). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. *NA*, *2*(NA), NA-NA. https://doi.org/10.6028/nist.sp.800-160v2

[115] Sadik, S., Ahmed, M., Sikos, L. F., & Islam, A. K. M. N. (2020). Toward a sustainable cybersecurity ecosystem. *Computers*, *9*(3), 74-NA. https://doi.org/10.3390/computers9030074

[116] Schackelford, S. J. (2016). Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk. *Chapman Law Review*, *19*(2), 445-NA. https://doi.org/NA

[117] Schilke, O. (2013). On the contingent value of dynamic capabilities for competitive advantage: The nonlinear moderating effect of environmental dynamism. *Strategic Management Journal*, *35*(2), 179-203. https://doi.org/10.1002/smj.2099

[118] Scholten, K., Scott, P. S., & Fynes, B. (2014). Mitigation Processes – Antecedents for Building supply chain resilience. *Supply Chain Management: An International Journal*, *19*(2), 211-218. https://doi.org/10.1108/scm-06-2013-0191

[119] Schroeder, G. N., Steinmetz, C., Rodrigues, R. N., Henriques, R. V. B., Rettberg, A., & Pereira, C. E. (2021). A Methodology for Digital Twin Modeling and Deployment for Industry 4.0. *Proceedings of the IEEE*, *109*(4), 556-567. https://doi.org/10.1109/jproc.2020.3032444

[120] Serban, A. C., & Lytras, M. D. (2020). Artificial Intelligence for Smart Renewable Energy Sector in Europe—Smart Energy Infrastructures for Next Generation Smart Cities. *IEEE Access*, *8*, 77364-77377. https://doi.org/10.1109/access.2020.2990123

[121] Shao, J., & Zhang, J. (2020). Communication-Computation Trade-off in Resource-Constrained Edge Inference. *IEEE Communications Magazine*, *58*(12), 20-26. https://doi.org/10.1109/mcom.001.2000373

[122] Shen, Z. M. (2021). Strengthening supply chain resilience during COVID-19: A case study of JD.com. *Journal of Operations Management*, *69*(3), 359-383. https://doi.org/10.1002/joom.1161

[123] Shneiderman, B. (2016). Opinion: The dangers of faulty, biased, or malicious algorithms requires independent oversight. *Proceedings of the National Academy of Sciences of the United States of America*, *113*(48), 13538-13540. https://doi.org/10.1073/pnas.1618211113

[124] Singh, S., Prakash, C., & Ramakrishna, S. (2020). Three-dimensional printing in the fight against novel virus COVID-19: Technology helping society during an infectious disease pandemic. *Technology in society*, *62*(62), 101305-NA. https://doi.org/10.1016/j.techsoc.2020.101305

[125] Skatchkovsky, N., Jang, H., & Simeone, O. (2021). Spiking Neural Networks—Part III: Neuromorphic Communications. *IEEE Communications Letters*, *25*(6), 1746-1750. https://doi.org/10.1109/lcomm.2021.3050212

[126] So, J., Guler, B., & Avestimehr, A. S. (2021). Byzantine-Resilient Secure Federated Learning. *IEEE Journal on Selected Areas in Communications*, *39*(7), 2168-2181. https://doi.org/10.1109/jsac.2020.3041404

[127] Sohel, A., Alam, M. A., Hossain, A., Mahmud, S., & Akter, S. (2022). Artificial Intelligence In Predictive Analytics For Next-Generation Cancer Treatment: A Systematic Literature Review Of Healthcare Innovations In The USA. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *1*(01), 62-87. https://doi.org/10.62304/jieet.v1i01.229

[128] Sohrabi, F., Attiah, K. M., & Yu, W. (2021). Deep Learning for Distributed Channel Feedback and Multiuser Precoding in FDD Massive MIMO. *IEEE Transactions on Wireless Communications*, *20*(7), 4044-4057. https://doi.org/10.1109/twc.2021.3055202

[129] Ssekulima, E. B., Anwar, M. B., Al Hinai, A., & Moursi, M. S. E. (2016). Wind speed and solar irradiance forecasting techniques for enhanced renewable energy integration with the grid: a review. *IET Renewable Power Generation*, *10*(7), 885-989. https://doi.org/10.1049/iet-rpg.2015.0477

[130] Subramanian, M., Wojtusciszyn, A., Favre, L., Boughorbel, S., Shan, J., Letaief, K. B., Pitteloud, N., & Chouchane, L. (2020). Precision medicine in the era of artificial intelligence: implications in chronic disease management. *Journal of translational medicine*, *18*(1), 472-NA. https://doi.org/10.1186/s12967-020-02658-5

[131] Sun, H., Yuan, C., Qian, Q., He, S., & Luo, Q. (2022). Digital resilience among individuals in school education settings: a concept analysis based on a scoping review. *Frontiers in psychiatry*, *13*, 858515.

[132] Sun, Y., Babu, P., & Palomar, D. P. (2017). Majorization-Minimization Algorithms in Signal Processing, Communications, and Machine Learning. *IEEE Transactions on Signal Processing*, *65*(3), 794-816. https://doi.org/10.1109/tsp.2016.2601299

[133] Sze, V., Chen, Y.-H., Yang, T.-J., & Emer, J. (2017). Efficient Processing of Deep Neural Networks: A Tutorial and Survey. *Proceedings of the IEEE*, *105*(12), 2295-2329. https://doi.org/10.1109/jproc.2017.2761740

[134] Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2013). Intriguing properties of neural networks. *arXiv: Computer Vision and Pattern Recognition*, *NA*(NA), NA-NA. https://doi.org/NA

[135] Taddeo, M. (2017). Trusting Digital Technologies Correctly. *Minds and Machines*, *27*(4), 565-568. https://doi.org/10.1007/s11023-017-9450-5

[136] Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. *Nature*, *556*(7701), 296-298. https://doi.org/10.1038/d41586-018-04602-6

[137] Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, *1*(12), 557-560. https://doi.org/10.1038/s42256-019-0109-1

[138] Tan, L., Xiao, H., Yu, K., Aloqaily, M., & Jararweh, Y. (2021). A blockchain-empowered crowdsourcing system for 5G-enabled smart cities. *Computer Standards & Interfaces*, *76*(NA), 103517-NA. https://doi.org/10.1016/j.csi.2021.103517

[139] Tan, L., Yu, K., Ming, F., Cheng, X., & Srivastava, G. (2022). Secure and Resilient Artificial Intelligence of Things: A HoneyNet Approach for Threat Detection and Situational Awareness. *IEEE Consumer Electronics Magazine*, *11*(3), 69-78. https://doi.org/10.1109/mce.2021.3081874

[140] Tanczer, L. M., Steenmans, I., Elsden, M., Blackstock, J. J., & Carr, M. (2018). Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge? *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, *NA*(NA), 1-9. https://doi.org/10.1049/cp.2018.0033

[141] Tao, F., Zhang, H., Liu, A., & Nee, A. Y. C. (2019). Digital Twin in Industry: State-of-the-Art. *IEEE Transactions on Industrial Informatics*, *15*(4), 2405-2415. https://doi.org/10.1109/tii.2018.2873186

[142] Thompson, M. A., Ryan, M. J., Slay, J., & McLucas, A. (2016). A New Resilience Taxonomy. *INCOSE International Symposium*, *26*(1), 1318-1330. https://doi.org/10.1002/j.2334-5837.2016.00229.x

[143] Thramboulidis, K. (2015). A cyber-physical system-based approach for industrial automation systems. *Computers in Industry*, *72*(NA), 92-102. https://doi.org/10.1016/j.compind.2015.04.006

[144] Tiirmaa-Klaar, H. (2016). Building national cyber resilience and protecting critical information infrastructure. *Journal of Cyber Policy*, *1*(1), 94-106. https://doi.org/10.1080/23738871.2016.1165716

[145] Tonoy, A. A. R. (2022). Mechanical Properties and Structural Stability of Semiconducting Electrides: Insights For Material. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *1*(01), 18-35. https://doi.org/10.62304/jieet.v1i01.225

[146] Tripp, J. C., McDevitt-Murphy, M. E., & Henschel, A. V. (2015). Firing a weapon and killing in combat are associated with suicidal ideation in OEF/OIF veterans. *Psychological trauma : theory, research, practice and policy*, *8*(5), 626-633. https://doi.org/10.1037/tra0000085

[147] Ullah, S., Akhtar, P., & Zaefarian, G. (2018). Dealing with endogeneity bias: The generalized method of moments (GMM) for panel data. *Industrial Marketing Management*, *71*(NA), 69-78. https://doi.org/10.1016/j.indmarman.2017.11.010

[148] Van den Homberg, M. J. C., Gevaert, C. M., & Georgiadou, Y. (2020). The Changing Face of Accountability in Humanitarianism: Using Artificial Intelligence for Anticipatory Action. *Politics and Governance*, *8*(4), 456-467. https://doi.org/10.17645/pag.v8i4.3158

[149] Vanajakumari, M., Kumar, S., & Gupta, S. (2016). An Integrated Logistic Model for Predictable Disasters. *Production and Operations Management*, *25*(5), 791-811. https://doi.org/10.1111/poms.12533

[150] Voyant, C., Notton, G., Kalogirou, S. A., Nivet, M. L., Paoli, C., Motte, F., & Fouilloy, A. (2017). Machine learning methods for solar radiation forecasting: A review. *Renewable Energy*, *105*(105), 569-582. https://doi.org/10.1016/j.renene.2016.12.095

[151] Wan, J., Yan, H., Li, D., Zhou, K., & Zeng, L. (2013). Cyber-Physical Systems for Optimal Energy Management Scheme of Autonomous Electric Vehicle. *The Computer Journal*, *56*(8), 947-956. https://doi.org/10.1093/comjnl/bxt043

[152] Wang, L., Törngren, M., & Onori, M. (2015). Current status and advancement of cyber-physical systems in manufacturing. *Journal of Manufacturing Systems*, *37*(NA), 517-527. https://doi.org/10.1016/j.jmsy.2015.04.008

[153] Wang, S., Wan, J., Li, D., & Zhang, C. (2016). Implementing smart factory of Industrie 4.0: an outlook. *International Journal of Distributed Sensor Networks*, *2016*(1), 3159805-NA. https://doi.org/NA

[154] Warnat-Herresthal, S., Schultze, H., Shastry, K., Manamohan, S., Mukherjee, S., Garg, V., Sarveswara, R., Händler, K., Pickkers, P., Aziz, N. A., Ktena, S., Tran, F., Bitzer, M., Ossowski, S., Casadei, N., Herr, C., Petersheim, D., Behrends, U., Kern, F., . . . Rieß, O. (2021). Swarm Learning for decentralized and confidential clinical machine learning. *Nature*, *594*(7862), 265-270. https://doi.org/10.1038/s41586-021-03583-3

[155] Wiesner-Hanks, T., Wu, H., Stewart, E. L., DeChant, C., Kaczmar, N., Lipson, H., Gore, M. A., & Nelson, R. (2019). Millimeter-Level Plant Disease Detection From Aerial Photographs via Deep Learning and Crowdsourced Data. *Frontiers in plant science*, *10*(NA), 1550-NA. https://doi.org/10.3389/fpls.2019.01550

[156] Wisco, B. E., Marx, B. P., May, L. B. S. C., Martini, B., Krystal, J. H., Southwick, S. M., & Pietrzak, R. H. (2017). Moral injury in U.S. combat veterans: Results from the national health and resilience in veterans study. *Depression and anxiety*, *34*(4), 340-347. https://doi.org/10.1002/da.22614

[157] Xiao, L., Wang, J., Dong, Y., & Wu, J. (2015). Combined forecasting models for wind energy forecasting: A case study in China. *Renewable and Sustainable Energy Reviews*, *44*(NA), 271-288. https://doi.org/10.1016/j.rser.2014.12.012

[158] Xie, H., Qin, Z., Li, G. Y., & Juang, B.-H. (2021). Deep Learning Enabled Semantic Communication Systems. *IEEE Transactions on Signal Processing*, *69*(NA), 2663-2675. https://doi.org/10.1109/tsp.2021.3071210

[159] Xin, R., Kar, S., & Khan, U. A. (2020). Decentralized Stochastic Optimization and Machine Learning: A Unified Variance-Reduction Framework for Robust Performance and Fast Convergence. *IEEE Signal Processing Magazine*, *37*(3), 102-113. https://doi.org/10.1109/msp.2020.2974267

[160] Yang, K., Shi, Y., & Ding, Z. (2019). Data Shuffling in Wireless Distributed Computing via Low-Rank Optimization. *IEEE Transactions on Signal Processing*, *67*(12), 3087-3099. https://doi.org/10.1109/tsp.2019.2912139

[161] Yang, K., Shi, Y., Zhou, Y., Yang, Z., Fu, L., & Chen, W. (2020). Federated Machine Learning for Intelligent IoT via Reconfigurable Intelligent Surface. *IEEE Network*, *34*(5), 16-22. https://doi.org/10.1109/mnet.011.2000045

[162] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated Machine Learning: Concept and Applications. *ACM Transactions on Intelligent Systems and Technology*, *10*(2), 12-19. https://doi.org/10.1145/3298981

[163] Yeom, J., Jung, J., Chang, A., Ashapure, A., Maeda, M. M., Maeda, A., & Landivar, J. (2019). Comparison of Vegetation Indices Derived from UAV Data for Differentiation of Tillage Effects in Agriculture. *Remote Sensing*, *11*(13), 1548-NA. https://doi.org/10.3390/rs11131548

[164] Younus, M. (2022). Reducing Carbon Emissions in The Fashion And Textile Industry Through Sustainable Practices and Recycling: A Path Towards A Circular, Low-Carbon Future. *Global Mainstream Journal of*

Business, Economics, Development & Project Management, *1*(1), 57-76. https://doi.org/10.62304/jbedpm.v1i1.226

[165] Yu, W., Jacobs, M. A., Chavez, R., & Yang, J. (2019). Dynamism, disruption orientation, and resilience in the supply chain and the impacts on financial performance: A dynamic capabilities perspective. *International Journal of Production Economics*, *218*(NA), 352-362. https://doi.org/10.1016/j.ijpe.2019.07.013

[166] Zeng, J., Chan, C.-h., & Schäfer, M. S. (2020). Contested Chinese Dreams of AI? Public Discourse About Artificial Intelligence on Wechat and People's Daily Online. *Information, Communication & Society*, *NA*(NA), 1-22. https://doi.org/NA

[167] Zhou, S. K., Greenspan, H., Davatzikos, C., Duncan, J. S., van Ginneken, B., Madabhushi, A., Prince, J. L., Rueckert, D., & Summers, R. M. (2021). A Review of Deep Learning in Medical Imaging: Imaging Traits, Technology Trends, Case Studies With Progress Highlights, and Future Promises. *Proceedings of the IEEE. Institute of Electrical and Electronics Engineers*, *109*(5), 820-838. https://doi.org/10.1109/jproc.2021.3054390

[168] Zhou, X., Zheng, H., Xu, X., He, J., Ge, X. K., Yao, X., Cheng, T., Zhu, Y., Cao, W., & Tian, Y. (2017). Predicting grain yield in rice using multi-temporal vegetation indices from UAV-based multispectral and digital imagery. *ISPRS Journal of Photogrammetry and Remote Sensing*, *130*(NA), 246-255. https://doi.org/10.1016/j.isprsjprs.2017.05.003

[169] Zhu, Q., Rieger, C., & Basar, T. (2011). A hierarchical security architecture for cyber-physical systems. *2011 4th International Symposium on Resilient Control Systems*, *NA*(NA), 15-20. https://doi.org/10.1109/isrcs.2011.6016081