Contents list available at CBIORE journal website

Journal of Emerging Science and Engineering

Journal homepage: https://journal.cbiore.id/index.php/jese/index

Research Article

Building institutional resilience to AI-driven misinformation in critical infrastructure: Evidence from the Albanian energy sector

Eva Hyna*

University of Aleksandër Moisiu -Durrës, Albania

Abstract. The rapid expansion of generative artificial intelligence has significantly transformed digital information environments, increasing the volume, velocity, and technical sophistication of misinformation affecting critical infrastructure systems. In the energy sector, such disruptions pose measurable risks to regulatory reliability, infrastructure investment, and operational stability, particularly in countries undergoing energy transition and digital modernization. Albania's developing energy ecosystem provides a relevant empirical context for examining these emerging system-level vulnerabilities. This study analyzes the integration of Business Intelligence (BI), Competitive Intelligence (CI), and AI-based detection systems in strengthening institutional resilience against AI-generated misinformation. A qualitative-dominant mixed-methods case study approach is employed, combining large-scale digital media monitoring, intelligence-cycle modeling, and expert-based validation. The research focuses on a coordinated disinformation campaign targeting the Qeparo Solar Farm project in 2025, using temporal network analysis, content classification, and attribution mapping to evaluate diffusion dynamics and institutional response mechanisms. Results indicate that misinformation propagation followed structured temporal patterns, emotionally optimized framing strategies, and coordinated amplification networks consistent with organized influence operations. Early anomaly detection was achieved through hybrid analytical systems integrating automated machine learning tools with professional assessment. Competitive Intelligence analysis supported probabilistic attribution and risk prioritization, while coordinated governance responses enabled rapid system stabilization and restoration of stakeholder confidence. The study proposes an applied governance-oriented resilience framework integrating BI, CI, and AI detection within a unified institutional monitoring architecture. The findings demonstrate that effective protection of critical infrastructure information systems depends primarily on institutional system design, operational coordination, and analytical capacity, rather than technological deployment alone. This research provides practical guidance for regulators, engineers, and infrastructure managers seeking to enhance digital security, information integrity, and system reliability in AI-driven operational environments

Keywords: : Business Intelligence; Competitive Intelligence; Artificial Intelligence; Energy Security; Disinformation; Energy Governance; Critical Infrastructure

Received: 6th January 2026; Revised: 16th Feb 2026; Accepted: 18th March 2027; Available online: 25th March 2026

1. Introduction

The rapid expansion of generative artificial intelligence has transformed contemporary information ecosystems, enabling the large-scale production and dissemination of synthetic content across digital platforms (arXiv, 2024; IBM, n.d.; MDPI, 2024). While these technologies have enhanced communication efficiency and analytical capacity, they have simultaneously intensified the scale, speed, and sophistication of misinformation and disinformation campaigns (European Commission, n.d.; Ash Center, n.d.). In critical infrastructure sectors such as energy, where institutional credibility, regulatory stability, and public trust constitute essential governance assets, AI-generated misinformation represents a growing systemic risk (International Energy Agency, n.d.; Friends of the Earth, 2024). Energy systems are particularly vulnerable to information manipulation due to their high public visibility, strategic economic importance, and close integration with regulatory and political decision-making processes (GardaWorld Security, n.d.; WNS, n.d.). False narratives targeting infrastructure safety, environmental impact, financial integrity, or institutional competence can rapidly destabilize public confidence and delay policy implementation (Chambers for Innovation & Clean Energy, n.d.; UNDP Climate Promise, n.d.). These risks are amplified in countries undergoing structural energy transitions, where contested investment projects and evolving regulatory frameworks create fertile conditions for narrative exploitation (AltEnergyMag, 2024; European Commission, n.d.). Existing research on misinformation has largely emphasized technological detection, media dynamics, and psychological susceptibility (arXiv, 2024; arXiv, 2025; DigitalOcean, n.d.). While these perspectives have generated valuable insights, they remain insufficient for explaining how institutions can sustain authority and legitimacy under persistent informational disruption (INFORMS, 2025; Frontiers in Communication, 2024). Relatively limited attention has been devoted to the governance architectures and intelligence systems that enable organizations to detect, interpret, and respond to coordinated influence operations in real time (Ash Center, n.d.; IBM, n.d.). Business Intelligence (BI) and Competitive Intelligence (CI) have traditionally been conceptualized as managerial instruments supporting operational efficiency and market positioning (ASCM, n.d.; LaunchNotes, n.d.). However, in digitally mediated environments characterized by algorithmic content generation and automated amplification, these systems

* Corresponding author
Email: evahyna@yahoo.com (E.Hyna)

https://doi.org/10.61435/jese.2026.e66
ISSN: p-ISSN: 3026-0817; e-ISSN: 3026-0183.The Author(s). Published by CBIORE

increasingly function as institutional infrastructures for informational governance (Alison.ai, n.d.; AltEnergyMag, 2024). When integrated with AI-based detection technologies, BI and CI provide the analytical, interpretive, and coordination capacities necessary to counter synthetic narratives and preserve organizational credibility (Forrester, n.d.; Microsoft, n.d.; Priavo Security, n.d.). This study investigates how intelligence-guided governance frameworks contribute to institutional resilience against AI-generated misinformation in the Albanian energy sector. Albania constitutes a theoretically and empirically relevant case due to its heavy reliance on hydropower, its accelerated diversification toward renewable energy, and its evolving regulatory capacity (International Energy Agency, n.d.; WNS, n.d.). These structural conditions expose energy governance to heightened informational vulnerability while simultaneously highlighting the importance of institutional adaptability (European Commission, n.d.; Friends of the Earth, 2024). Using a qualitative-dominant mixed-methods case study design, the research analyzes a coordinated disinformation campaign targeting the Qeparo Solar Farm project in 2025. By integrating digital media monitoring, intelligence-cycle analysis, and expert-informed validation, the study examines how BI, CI, and AI-based detection mechanisms interact to support early warning, attribution, and coordinated response (arXiv, 2025; INFORMS, 2025; International Journal of Interactive Multimedia and Artificial Intelligence, 2025). The article makes three principal contributions. First, it reconceptualizes BI and CI as governance infrastructures rather than auxiliary management tools (Alison.ai, n.d.; ASCM, n.d.). Second, it advances intelligence theory by proposing a hybrid intelligence cycle that integrates automated detection with human analytical judgment (Forrester, n.d.; MDPI, 2024). Third, it conceptualizes AI-generated misinformation as a systemic institutional risk embedded within broader governance and risk management frameworks (Ash Center, n.d.; European Commission, n.d.).

The findings offer practical implications for policymakers, regulators, and infrastructure operators seeking to strengthen informational resilience under conditions of algorithmic opacity and strategic manipulation (Cloudflare, n.d.; INFORMS, 2025). More broadly, the study contributes to emerging debates on digital governance and institutional capacity by demonstrating that sustainable resilience depends not only on technological investment, but on organizational design, professional competence, and coordinated authority (UNDP Climate Promise, n.d.; International Energy Agency, n.d.).

2. Methods

This study adopts a qualitative-dominant mixed-methods case study design to examine how Business Intelligence (BI), Competitive Intelligence (CI), and AI-based detection mechanisms are applied in countering AI-generated misinformation within the Albanian energy sector (Alison.ai, n.d.; ASCM, n.d.; INFORMS, 2025). A case study approach was selected due to the exploratory and context-dependent nature of information manipulation in critical infrastructure environments, where institutional responses are shaped by regulatory frameworks, stakeholder relations, and sector-specific vulnerabilities (GardaWorld Security, n.d.; European Commission, n.d.). The research design integrates documentary analysis, digital media monitoring, and expert-informed validation in order to capture both the structural characteristics of disinformation campaigns and the organizational mechanisms deployed in response (arXiv, 2024; Priavo Security, n.d.). This triangulated approach enhances analytical rigor and reduces the risk of single-source bias (INFORMS, 2025; Frontiers in Communication, 2024).

2.1 Case Selection and Context

The Qeparo Solar Farm project was selected as the focal case due to its strategic relevance within Albania's renewable energy transition and its documented exposure to coordinated misinformation narratives during the project's public consultation and implementation phases in 2025 (International Energy Agency, n.d.; AltEnergyMag, 2024).

The case satisfies three selection criteria:

- Strategic importance as a large-scale renewable infrastructure investment (WNS, n.d.).
- 2 .High public visibility and stakeholder sensitivity (Chambers for Innovation & Clean Energy, n.d.).
- Documented presence of anomalous information diffusion patterns across digital platforms (arXiv, 2025).

These characteristics render the case suitable for examining the interaction between institutional intelligence systems and digitally mediated disinformation dynamics (Ash Center, n.d.; IBM, n.d.).

2.2 Data Sources

Data were collected from multiple primary and secondary sources between January and September 2025, following best practices in digital intelligence and governance research (Priavo Security, n.d.; INFORMS, 2025).

Primary data sources included:

- Digital media content from major social networking platforms (Facebook, X/Twitter, YouTube, and regional news portals) (arXiv, 2025; DigitalOcean, n.d.).
- Public statements, press releases, and regulatory communications issued by relevant governmental and energy-sector institutions (European Commission, n.d.; UNDP Climate Promise, n.d.).
- Internal operational and performance reports made available through institutional dashboards and public transparency portals (Microsoft, n.d.; Riskonnect, n.d.).
- Semi-structured consultations with sector experts, regulatory officials, and intelligence practitioners (Forrester, n.d.; Alison.ai, n.d.).
- Secondary data sources comprised:
- Policy documents and regulatory guidelines related to energy governance and cybersecurity (European Commission, n.d.; IEA, n.d.).
- Industry reports on misinformation detection and AI governance (Cloudflare, n.d.; Booz Allen Hamilton, n.d.).

Peer-reviewed academic literature on information disorder, intelligence systems, and critical infrastructure resilience (Frontiers in Communication, 2024; MDPI, 2024). All data sources were archived and indexed to ensure traceability and analytical transparency.

2.3 Digital Media Monitoring and Data Collection

Digital content related to the Qeparo project was systematically collected using keyword-based and hashtag-based monitoring protocols consistent with contemporary misinformation research practices (arXiv, 2024; arXiv, 2025). Search queries included combinations of project identifiers, institutional names, and thematic risk terms (e.g., "Qeparo solar," "environmental risk," "corruption," "health impact"). Data collection covered a continuous twelve-week period following the initial public announcement of the project. Content was extracted at daily intervals to capture diffusion dynamics and narrative evolution (FIU News, 2025; INFORMS, 2025).

Collected data included:

- Textual posts and comments.
- Images and video materials.
- Metadata on publication time, engagement metrics, and source accounts.

Duplicate content and automated reposts were filtered to minimize distortion in diffusion analysis (DigitalOcean, n.d.; Cloudflare Blog, n.d.).

2.4 Analytical Framework

Data analysis was conducted through an integrated intelligence-oriented framework combining BI indicators, CI mapping techniques, and AI-based forensic assessment (Alison.ai, n.d.; LaunchNotes, n.d.; MDPI, 2024).

2.4.1 Business Intelligence Analysis

BI analysis focused on internal and external performance indicators relevant to misinformation detection and response (ASCM, n.d.; Microsoft, n.d.). These included:

- Sentiment polarity and volatility measures.
- Frequency and clustering of high-risk keywords.
- Response latency between narrative emergence and institutional communication.
- Cross-validation of external claims against verified operational datasets.

Time-series analysis was applied to identify anomalous deviations from baseline communication patterns (AltEnergyMag, 2024; Riskonnect, n.d.).

2.4.2 Competitive Intelligence Analysis

CI analysis was employed to reconstruct narrative origin, actor networks, and dissemination strategies (LaunchNotes, n.d.; BiopharmaVantage, n.d.). Techniques included:

- Source credibility assessment based on account history, network centrality, and content consistency (International Journal of Interactive Multimedia and Artificial Intelligence, 2025).
- Network mapping of information diffusion pathways (arXiv, 2025).
- Identification of coordinated inauthentic behavior through temporal and linguistic similarity metrics (FIU News, 2025).
- Scenario analysis to evaluate potential strategic motivations behind narrative framing (INFORMS, 2025).

This enabled attribution of misinformation campaigns to organized rather than spontaneous information flows.

2.4.3 AI-Based Forensic Assessment

AI-assisted detection tools were applied to validate the synthetic nature of selected content (MDPI, 2024; Behavioral Signals, n.d.). These tools included:

- Natural Language Processing models for detecting low perplexity, repetitive structures, and translation artifacts in textual content (arXiv, 2024).
- Computer vision algorithms for identifying visual inconsistencies in video and image materials (Cloudflare Blog, n.d.).
- Audio forensics software for detecting synthetic voice signatures where applicable (Behavioral Signals, n.d.).
- Detection outputs were cross-validated through human expert review to reduce false-positive risk (Forrester, n.d.; IBM, n.d.).

2.5 Qualitative Coding and Thematic Analysis

Qualitative data were subjected to thematic coding using an inductive–deductive approach informed by intelligence cycle models and misinformation research (Frontiers in Communication, 2024; INFORMS, 2025). Initial coding categories included:

- Narrative framing strategies.
- Emotional amplification mechanisms.
- Institutional response typologies.
- Trust-repair strategies.

Open coding was followed by axial coding to identify relational patterns between narrative characteristics and institutional responses. Coding reliability was enhanced through iterative validation and peer consultation (Ash Center, n.d.; Priavo Security, n.d.).

2.6 Validation and Reliability Procedures

Methodological reliability was strengthened through four complementary mechanisms (INFORMS, 2025; European Commission, n.d.):

- Source triangulation across digital media, institutional documents, and expert consultations.
- Analytical triangulation through combined BI, CI, and AI-based assessments.
- Temporal validation by comparing early-stage and late-stage diffusion patterns.
- Expert validation involving feedback from practitioners in energy regulation and intelligence analysis.

Discrepancies between analytical outputs were systematically reviewed and resolved through iterative refinement.

2.7 Ethical Considerations

All data utilized in this study were obtained from publicly accessible sources or anonymized institutional materials, in accordance with digital governance and data protection guidelines (European Commission, n.d.; IBM, n.d.). No personal or sensitive information was collected or disclosed. Platform terms of service and applicable data protection regulations were observed throughout the research process.
Expert consultations were conducted on a voluntary basis, and no identifying information is disclosed.

2.8 Methodological Limitations

Several limitations should be acknowledged. First, reliance on publicly available digital content restricts access to encrypted or closed-network communications (Cloudflare, n.d.). Second, attribution of coordinated disinformation remains probabilistic rather than definitive (FIU News, 2025). Third, AI detection tools remain subject to evolving adversarial techniques and measurement uncertainty (MDPI, 2024; Booz Allen Hamilton, n.d.). These limitations were mitigated through methodological triangulation and conservative interpretation of attribution findings (INFORMS, 2025).

3. Results and discussion

3.1 Patterns of AI-Generated Misinformation in the Qeparo Case

Analysis of digital media content revealed a highly structured pattern of misinformation diffusion rather than spontaneous or organic information flows, consistent with documented characteristics of coordinated influence operations (arXiv, 2025; FIU News, 2025). Within forty-eight hours of the public announcement of the Qeparo Solar Farm project, a coordinated surge of negative narratives emerged across multiple platforms, reflecting rapid amplification dynamics observed in previous studies (arXiv, 2024; INFORMS, 2025). These narratives were characterized by consistent framing, emotionally charged language, and repetitive thematic structures, indicating systematic amplification rather than isolated user activity (Frontiers in Communication, 2024; Behavioral Signals, n.d.). Three dominant narrative clusters were identified. The first focused on alleged public health risks, particularly claims regarding cancer and environmental contamination. The second cluster centered on accusations of financial misconduct, including money laundering and offshore corruption. The third cluster targeted institutional credibility, disseminating fabricated audiovisual materials purporting to implicate regulatory officials in environmental cover-ups, consistent with patterns documented in climate and energy misinformation research (Friends of the Earth, 2024; Chambers for Innovation & Clean Energy, n.d.). Temporal analysis demonstrated that these narratives followed synchronized diffusion trajectories, with peak engagement occurring within narrow time windows across platforms. Such synchronization is consistent with coordinated inauthentic behavior and automated dissemination strategies (arXiv, 2025; Cloudflare, n.d.). These findings support existing research suggesting that AI-assisted misinformation campaigns prioritize speed and narrative coherence over factual plausibility in order to maximize early-stage impact (MDPI, 2024; Booz Allen Hamilton, n.d.).

3.2 Institutional Detection and Early-Warning Capacity

Business Intelligence monitoring systems played a central role in identifying the initial escalation of disinformation, in line with established practices in data-driven risk monitoring (Alison.ai, n.d.; ASCM, n.d.). Sentiment volatility, abnormal keyword clustering, and engagement anomalies were detected within hours of narrative emergence, reflecting anomaly-detection approaches documented in BI research (Microsoft, n.d.; AltEnergyMag, 2024). Compared to baseline communication patterns observed in previous infrastructure projects, negative sentiment indicators increased by more than fivefold during the early diffusion phase. Cross-validation of external claims against internal operational and environmental datasets enabled rapid verification and rejection of false allegations, consistent with governance-oriented data validation frameworks (Energera, n.d.; Riskonnect, n.d.). This process reduced institutional uncertainty and provided an empirical foundation for subsequent public communication. The findings indicate that BI systems functioned not merely as reporting instruments, but as operational early-warning mechanisms embedded within institutional risk management processes (Forrester, n.d.; INFORMS, 2025). The effectiveness of detection was significantly enhanced by the integration of AI-assisted analytical tools. Natural Language Processing models identified low-perplexity structures and repetitive syntactic patterns in textual content, while computer vision algorithms detected inconsistencies in video materials, as documented in recent deepfake detection studies (arXiv, 2024; MDPI, 2024; Cloudflare Blog, n.d.). Human analyst validation remained essential in interpreting detection outputs and contextualizing technical indicators within regulatory and political environments (IBM, n.d.; Behavioral Signals, n.d.).

These results confirm that detection capacity in AI-intensive information ecosystems is fundamentally hybrid, combining automated analytics with professional judgment (Forrester, n.d.; INFORMS, 2025).

3.3 Competitive Intelligence and Attribution Dynamics

Competitive Intelligence analysis enabled systematic reconstruction of narrative origin and diffusion pathways, consistent with established CI mapping techniques (LaunchNotes, n.d.; BiopharmaVantage, n.d.). Network mapping revealed that a limited number of high-centrality accounts initiated the majority of high-impact content, which was subsequently amplified through coordinated secondary networks, reflecting influence patterns documented in misinformation research (arXiv, 2025; FIU News, 2025). Source credibility assessment indicated low historical reliability, short account lifespans, and cross-platform identity replication, all characteristic of organized influence operations (International Journal of Interactive Multimedia and Artificial Intelligence, 2025; Priavo Security, n.d.). Scenario analysis suggested that environmental framing constituted the most strategically effective vector for narrative penetration due to its resonance with local tourism stakeholders and community groups, consistent with climate misinformation studies (Friends of the Earth, 2024; UNDP Climate Promise, n.d.). Financial misconduct narratives, although initially prominent, exhibited lower long-term engagement, indicating reduced persuasive sustainability. Attribution analysis identified linkages to external public relations actors operating outside Albania, highlighting the transnational character of contemporary information manipulation (Ash Center, n.d.; INFORMS, 2025). While definitive attribution remains methodologically constrained, the convergence of temporal, linguistic, and network indicators provides strong probabilistic evidence of coordinated activity. These findings reinforce the value of CI frameworks in transforming fragmented information signals into actionable strategic intelligence (Alison.ai, n.d.; LaunchNotes, n.d.).

3.4 Organizational Response and Governance Coordination

Institutional response mechanisms evolved through three sequential phases: stabilization, verification, and trust repair, reflecting crisis management models documented in governance literature (Forbes Communications Council, 2025; European Commission, n.d.). During the stabilization phase, authorities prioritized containment of narrative escalation through rapid clarification and controlled communication channels. The verification phase focused on systematic publication of operational and environmental performance data. The trust-repair phase emphasized stakeholder engagement, including public consultations and collaborative media initiatives (UNDP Climate Promise, n.d.; GardaWorld Security, n.d.). Coordination between regulatory agencies, project operators, and communication units proved decisive. Where inter-institutional alignment was strong, response latency was minimized and message coherence was preserved, consistent with findings on institutional resilience (WNS, n.d.; INFORMS, 2025). Conversely, minor delays in early-stage coordination correlated with temporary credibility erosion and increased rumor persistence. The establishment of a dedicated misinformation monitoring task force marked a transition from reactive crisis management toward institutionalized governance capacity, reflecting organizational learning processes observed in critical infrastructure sectors (European Commission, n.d.; Industrial Cyber, n.d.).

3.5 Impact on Public Trust and Policy Implementation

Survey data, engagement metrics, and media coverage analysis indicate that misinformation campaigns exerted measurable short-term effects on public perception and project legitimacy, consistent with studies on narrative-driven trust erosion (Frontiers in Communication, 2024; UNDP Climate Promise, n.d.). During peak diffusion periods, support for the project declined and uncertainty indicators increased significantly. However, these effects proved reversible following sustained transparency initiatives and stakeholder engagement (European Commission, n.d.; Forbes Communications Council, 2025). The restoration of public confidence was strongly associated with the availability of verifiable data and consistent institutional messaging. Narrative rebuttal alone was insufficient; credibility recovery depended primarily on demonstrable performance evidence and procedural transparency, in line with governance communication research (IBM, n.d.; WNS, n.d.). These results suggest that informational resilience in critical infrastructure contexts is grounded less in persuasive communication than in institutional reliability and data integrity (International Energy Agency, n.d.; Riskonnect, n.d.).

3.6 Systemic Implications for Intelligence-Guided Governance

The empirical findings demonstrate that BI, CI, and AI-based detection systems collectively constitute an integrated governance infrastructure rather than isolated technical tools (Alison.ai, n.d.; ASCM, n.d.; INFORMS, 2025). Their effectiveness derives from structural integration, organizational embedding, and professional competence (Forrester, n.d.; European Commission, n.d.). Institutions exhibiting high analytical capacity, strong coordination mechanisms, and established trust-repair protocols displayed significantly greater resilience to misinformation-induced disruption. Conversely, fragmented intelligence architectures were associated with delayed response, narrative drift, and prolonged reputational damage (Industrial Cyber, n.d.; GardaWorld Security, n.d.). This supports the theoretical proposition that informational resilience represents an emergent institutional property shaped by governance design, rather than a direct outcome of technological investment alone (Ash Center, n.d.; MDPI, 2024).

3.7 Limitations and Interpretive Cautions

Despite robust triangulation, several limitations remain. First, reliance on publicly accessible digital content restricts visibility into closed communication networks (Cloudflare, n.d.). Second, attribution remains probabilistic rather than conclusive due to deliberate obfuscation by disinformation actors (FIU News, 2025; Ash Center, n.d.). Third, evolving AI generation techniques continuously alter

detection benchmarks (MDPI, 2024; Booz Allen Hamilton, n.d.). These constraints necessitate cautious interpretation of causal claims and reinforce the importance of adaptive analytical frameworks (INFORMS, 2025).

3.8 Synthesis: From Technical Detection to Institutional Resilience

The results collectively demonstrate that effective counter-disinformation strategies in the energy sector depend on the convergence of technical, organizational, and governance capacities (International Energy Agency, n.d.; European Commission, n.d.). Detection technologies provide necessary but insufficient conditions for resilience. Sustainable informational stability emerges only when analytical outputs are embedded within coordinated institutional processes and supported by transparent accountability mechanisms (UNDP Climate Promise, n.d.; WNS, n.d.). The Qeparo case illustrates that misinformation does not merely challenge communication systems; it tests the structural integrity of governance arrangements. Institutions capable of integrating intelligence production, regulatory authority, and public engagement are better positioned to withstand informational disruption and preserve policy continuity (Forbes Communications Council, 2025; INFORMS, 2025).

4. Conclusion

This study examined how Business Intelligence, Competitive Intelligence, and AI-based detection mechanisms jointly shape institutional resilience to AI-generated misinformation in the context of Albania's energy sector (Alison.ai, n.d.; ASCM, n.d.; INFORMS, 2025). Through an in-depth case analysis of the coordinated disinformation campaign targeting the Qeparo Solar Farm project, the research demonstrates that misinformation constitutes not merely a communication disturbance, but a systemic governance risk capable of disrupting regulatory authority, investment confidence, and policy implementation (Ash Center, n.d.; European Commission, n.d.; International Energy Agency, n.d.). The findings show that effective mitigation depends on the structural integration of analytical, organizational, and technological capacities. Business Intelligence systems provided the empirical foundation for rapid verification and anomaly detection (Microsoft, n.d.; AltEnergyMag, 2024), while Competitive Intelligence enabled strategic interpretation, attribution, and scenario evaluation (LaunchNotes, n.d.; Biopharma Vantage, n.d.). AI-based detection tools enhanced technical validation but remained dependent on human expertise for contextual assessment and decision-making (MDPI, 2024; Forrester, n.d.; IBM, n.d.). Together, these elements formed a hybrid intelligence architecture that supported timely institutional response and credibility restoration (INFORMS, 2025). By reframing intelligence systems as governance infrastructure, this study extends existing scholarship on digital governance and critical infrastructure protection (European Commission, n.d.; Industrial Cyber, n.d.). It demonstrates that informational resilience emerges not from technological deployment alone, but from institutional design, professional competence, and coordinated authority (UNDP Climate Promise, n.d.; WNS, n.d.). The proposed governance-oriented model highlights analytical capacity, coordination capacity, and trust-repair capacity as central determinants of institutional stability in algorithmically mediated information environments (Ash Center, n.d.; MDPI, 2024). From a policy perspective, the results underscore the necessity of embedding misinformation management within enterprise risk management and regulatory oversight frameworks (Riskonnect, n.d.; GardaWorld Security, n.d.). Energy-sector institutions must move beyond ad hoc crisis communication toward permanent intelligence integration, standardized monitoring protocols, and cross-agency coordination mechanisms (Forbes Communications Council, 2025; European Commission, n.d.). Investment in detection technologies should be accompanied by sustained training in data literacy, analytical reasoning, and ethical judgment to preserve accountability and public trust (Forrester, n.d.; IBM, n.d.).

The study also contributes to comparative governance research by demonstrating that effective informational resilience can be constructed in emerging and transition economies despite resource constraints (International Energy Agency, n.d.; UNDP Climate Promise, n.d.). The Albanian case illustrates that institutional coherence and professional capacity can compensate for limitations in technological sophistication, providing transferable lessons for similarly situated jurisdictions (WNS, n.d.; Frontiers in Communication, 2024). Several limitations should be acknowledged. The analysis relies primarily on publicly accessible digital content and probabilistic attribution methods, which restrict definitive identification of disinformation actors (FIU News, 2025; Cloudflare, n.d.). Moreover, rapidly evolving generative technologies continuously reshape detection benchmarks (MDPI, 2024; Booz Allen Hamilton, n.d.). Future research should therefore incorporate longitudinal designs, cross-national comparisons, and experimental validation of hybrid intelligence models to strengthen causal inference and generalizability (INFORMS, 2025; International Journal of Interactive Multimedia and Artificial Intelligence, 2025). In an era characterized by algorithmic opacity and strategic information manipulation, institutional credibility increasingly depends on the capacity to produce, verify, and communicate truth under conditions of uncertainty (Ash Center, n.d.; European Commission, n.d.). This study concludes that intelligence-guided governance represents a critical foundation for sustaining democratic accountability, market stability, and public confidence in critical infrastructure sectors (International Energy Agency, n.d.; UNDP Climate Promise, n.d.). Organizations that succeed in integrating analytical rigor, coordinated authority, and transparent engagement will be best positioned to navigate the informational challenges of the AI age (INFORMS, 2025; Forbes Communications Council, 2025)

Acknowledgments

The author gratefully acknowledges the institutional and professional support provided by the Agricultural University of Tirana and the University "Alexander Moisiu" of Durrës, which facilitated the academic and analytical environment necessary for the completion of this research. Sincere appreciation is extended to experts and practitioners from the Albanian energy sector, regulatory institutions, and intelligence and data analytics communities who contributed valuable insights through informal consultations, scenario validation, and professional feedback. Their experience and domain knowledge significantly strengthened the empirical grounding and practical relevance of this study. The author also acknowledges the contribution of academic peers and reviewers who provided constructive comments that enhanced the methodological rigor, analytical clarity, and policy relevance of the manuscript. No external

funding was received for this research. The views expressed are solely those of the author and do not necessarily reflect the official positions of affiliated institutions. All interpretations, analyses, and conclusions remain the exclusive responsibility of the author.

Author Contributions: The article is all contribution of the author.

Funding: The author received no financial support for the research, authorship, and/or publication of this article.

Conflicts of Interest: The author declares that there are no known competing financial or personal interests that could have appeared to influence the work reported in this paper. The author has declared that no competing interests exist.

References

Alison.ai. (n.d.). AI in competitive intelligence: Outmaneuver your rivals. https://alison.ai/resources/blog/ai-in-competitive-intelligence
AltEnergyMag. (2024, April). The transformative power of business intelligence for renewable energy. https://www.altenergymag.com/story/2024/04/the-transformative-power-of-business-intelligence-for-renewable-energy/41798/
Alwis, A. (2001) *Study on the potential for biogas in Sri Lanka*. ITDG South Asia.
arXiv. (2024). A guide to misinformation detection data and evaluation (arXiv:2411.05060). https://arxiv.org/html/2411.05060v2
arXiv. (2024). The world of generative AI: Deepfakes and large language models (arXiv:2402.04373). https://arxiv.org/html/2402.04373v1
arXiv. (2025). Characterizing AI-generated misinformation on social media (arXiv:2505.10266). https://arxiv.org/html/2505.10266v1
ASCM. (n.d.). What is supply chain analytics? https://www.ascm.org/topics/supply-chain-analytics/
Ash Center for Democratic Governance and Innovation. (n.d.). Weaponized AI: A new era of threats and how we can counter it. https://ash.harvard.edu/articles/weaponized-ai-a-new-era-of-threats/
Behavioral Signals. (n.d.). The duality of AI and the growing challenge of deepfake detection. https://behavioralsignals.com/the-duality-of-ai-and-the-growing-challenge-of-deepfake-detection/
BiopharmaVantage. (n.d.). AI in pharmaceutical competitive intelligence: Leveraging human–AI collaboration for maximizing success. https://www.biopharmavantage.com/ai-pharmaceutical-competitive-intelligence
Booz Allen Hamilton. (n.d.). Deepfakes targeting benefits with AI-generated claims. https://www.boozallen.com/insights/ai-research/deepfakes-targeting-benefits-with-ai-generated-claims.html
Cardinal Cushing Library. (n.d.). Fake news/mis- and disinformation: AI-generated content. https://learningcommons.emmanuel.edu/guide_fakenews/ai_content
Chambers for Innovation & Clean Energy. (n.d.). Clean energy disinformation primer. https://www.chambersforinnovation.com/clean-energy-disinformation-primer
Cloudflare Blog. (n.d.). An early look at cryptographic watermarks for AI-generated content. https://blog.cloudflare.com/an-early-look-at-cryptographic-watermarks-for-ai-generated-content/
Cloudflare. (n.d.). Addressing AI-generated misinformation. https://www.cloudflare.com/the-net/building-cyber-resilience/ai-generated-misinformation/
Cointelegraph. (n.d.). AI-generated content needs blockchain before trust in digital media collapses. https://cointelegraph.com/news/ai-generated-content-needs-blockchain
Computing Research Association. (2024). 5 ways to build resilience to disinformation. https://cra.org/crn/2024/09/5-ways-to-build-resilience-to-disinformation/
Datahub Analytics. (n.d.). AI in DevSecOps: Automating security vulnerability detection. https://datahubanalytics.com/ai-in-devsecops-automating-security-vulnerability-detection/
DigitalOcean. (n.d.). 7 AI content detectors for identifying artificially generated text. https://www.digitalocean.com/resources/articles/top-ai-content-detectors
Energera. (n.d.). Oil & gas data validation. https://www.energera.com/data-validation/
European Commission. (n.d.). Building societal resilience against disinformation. https://commission.europa.eu/topics/countering-information-manipulation/building-societal-resilience-against-disinformation_en
FIU News. (2025). Weaponized storytelling: How AI is helping researchers sniff out disinformation campaigns. https://news.fiu.edu/2025/weaponized-storytelling-how-ai-is-helping-researchers-sniff-out-disinformation-campaigns
Forbes Communications Council. (2025, May 7). AI-generated misinformation and crisis management in corporate communications. https://www.forbes.com/councils/forbescommunicationscouncil/2025/05/07/ai-generated-misinformation-and-crisis-management-in-corporate-communications/
Forrester. (n.d.). Be the human in the loop: Data and AI literacy is your edge. https://www.forrester.com/blogs/be-the-human-in-the-loop-data-ai-literacy-is-your-edge/
Friends of the Earth. (2024). Artificial intelligence threats to climate change. https://foe.org/wp-content/uploads/2024/03/AI_Climate_Disinfo_v6_031224.pdf
Frontiers in Communication. (2024). Climate and energy misinformation in Taiwan. https://www.frontiersin.org/journals/communication/articles/10.3389/fcomm.2024.1531126/full
GardaWorld Security. (n.d.). Strengthening security in the energy sector. https://www.garda.com/articles/strengthening-security-in-the-energy-sector
Government of Zimbabwe (2004) *Census 2002*. National Report, Central Statistical Office, Harare
IBM. (n.d.). AI misinformation. https://www.ibm.com/think/insights/ai-misinformation
Industrial Cyber. (n.d.). Integrating AI and ML technologies across OT and ICS environments. https://industrialcyber.co/features/integrating-ai-and-ml-technologies-across-ot-ics-environments-to-enhance-anomaly-detection-and-operational-resilience/
INFORMS. (2025). Protecting society from AI-generated misinformation. https://pubsonline.informs.org/do/10.1287/LYTX.2025.01.06/full/
International Energy Agency. (n.d.). AI and energy security. https://www.iea.org/reports/energy-and-ai/ai-and-energy-security
International Journal of Interactive Multimedia and Artificial Intelligence. (2025). Source credibility assessment in the realm of information disorder. https://www.ijimai.org/journal/sites/default/files/2025-01/ip2025_01_002.pdf
LaunchNotes. (n.d.). Mastering competitive intelligence analysis. https://www.launchnotes.com/blog/mastering-competitive-intelligence-analysis-strategies-for-success
McInerney J. (2011) *Biogas Technology on Uzi Island.* A Feasibility Study Zanzibar.

MDPI. (2024). Generative artificial intelligence and the evolving challenge of deepfake detection. https://www.mdpi.com/2224-2708/14/1/17
Microsoft. (n.d.). Power BI anomaly detection tutorial. https://learn.microsoft.com/en-us/power-bi/visuals/power-bi-visualization-anomaly-detection
Priavo Security. (n.d.). Misinformation and disinformation: How businesses can harness OSINT to mitigate risks. https://priavosecurity.com/misinformation-and-disinformation-how-businesses-can-harness-osint-to-mitigate-risks/
Rahma, D. U. Z., Nurahman, G. H., Hadiyanto, H., & Baihaqi, R. A. (2023). Production of high-antioxidant yoghurt using phycocyanin from microalgae Spirulina sp. Journal of Emerging Science and Engineering, 1(2), 36–43. https://doi.org/10.61435/jese.2023.9
Rajorhia, U., Kumar, A., & Sharma, R. (2012) *Utilisation of Farm Waste in Biogas Production*. http://www.landmarkgoc.com/biogas_project.html. Accessed on 3 March 2012
Riskonnect. (n.d.). What's the difference between internal and external data? https://riskonnect.com/risk-management-information-systems/whats-the-difference-between-internal-and-external-data/
UNDP Climate Promise. (n.d.). What are climate misinformation and disinformation and how can we tackle them? https://climatepromise.undp.org/news-and-stories/what-are-climate-misinformation-and-disinformation-and-how-can-we-tackle-them
WNS. (n.d.). From insights to impact: 7 ways data is shaping the energy and utility sector. https://www.wns.com/perspectives/articles/from-insights-to-impact-7-ways-data-is-shaping-the-energy-amp-utility-sector