Received: 26 July 2026 | Accepted: 25 August 2026 | Published: 17 November 2026

ARK: 24285/RCC.v10i20.313

ARTICLE

The Role of Information Management Technology in Crisis Decision-Making: An Analytical Study of Dimensions, Mechanisms, and Challenges

Chouieb Lyamine[1]
https://orcid.org/0009-0008-5906-5091
Mouloud Mammeri University of Tizi-Ouzou, Tizi-Ouzou, Algeria
E-mail: lyamine.chouieb@ummto.dz

Slimi Sassia[2]
https://orcid.org/0009-0007-3662-7306
Mouloud Mammeri University of Tizi-Ouzou, Tizi-Ouzou, Algeria
E-mail: sassia.slimi@ummto.dz

Informações da publicação

ARK: 24285/RCC.v10i20.313

ISSN: 2763-6496

Keywords:
Information Management Technology.
Crisis Decision-Making.
Bounded Rationality.
Common Operational Picture.
Administrative Governance.

Abstract:
In an increasingly volatile and interconnected global landscape, strategic crisis decision-making occurs under extreme temporal compression, high structural uncertainty, and severe operational threat. Legacy intuition-driven governance paradigms are demonstrably inadequate for managing contemporary complex disruptions. This analytical study examines the transformative role of Information Management Technology (IMT)—encompassing Big Data analytics, Geographic Information Systems (GIS), Artificial Intelligence (AI), and Internet of Things (IoT) sensor networks—in re-architecting modern crisis decision-making processes. Synthesizing theoretical foundations from Bounded Rationality Theory, Information Processing Theory, Organizational Sensemaking, and the Data-Information-Knowledge-Wisdom (DIKW) continuum, this paper systematically evaluates IMT deployment across the proactive detection, operational response, and post-crisis learning phases. The analysis demonstrates that IMT expands human cognitive capacity, mitigates equivocality, and constructs real-time Common Operational Pictures (COP), shifting crisis governance from reactive improvisations to intelligence-driven strategic interventions. Nevertheless, system effectiveness remains vulnerable to critical operational bottlenecks, including cognitive information overload, infodemics, cybersecurity threats, and socio-organizational resistance to algorithmic governance. These dynamics are further examined within developing administrative environments, such as Algeria, where legacy bureaucratic silos and digital infrastructural disparities present unique deployment challenges. To optimize technology-mediated crisis response, organizations must institutionalize open-data interoperability standards, enforce human-in-the-loop algorithmic oversight, implement redundant telecommunication infrastructures, and cultivate proactive digital crisis leadership. Ultimately, IMT serves as a vital cognitive and operational scaffold, provided technological integration is aligned with resilient, human-centered governance structures.

[1] Doctoral student at the Faculty of Humanities and Social Sciences, Mouloud Mammeri University of Tizi-Ouzou, Tizi-Ouzou, Algeria (2018). Master's degree from Mohamed Seddik Ben Yahia University, Jijel, Algeria (2017).
[2] Professor at Mouloud Mammeri University of Tizi-Ouzou, Tizi-Ouzou, Algeria (2009). Master's degree from the Faculty of Humanities and Social Sciences, University of Algiers 2 Abu El Kacem Saadallah, Algiers, Algeria (1997). PhD from the University of Algiers 2 Abu El Kacem Saadallah, Algiers, Algeria (2009).

© 2026 The authors
This article is licensed under the Creative Commons Attribution 4.0 International License — CC BY 4.0

1. Introduction

Modern organizations operate within an environment characterized by volatility, uncertainty, complexity, and ambiguity (VUCA). Crises—whether manifesting as natural disasters, industrial accidents, epidemiological outbreaks, supply chain collapses, or geopolitical disruptions—represent acute operational shocks that threaten an organization's structural viability, strategic objectives, and institutional legitimacy (Bundy et al., 2017, p. 1662). In these critical moments, executive decision-makers must formulate, evaluate, and execute strategic interventions under severe conditions: intense time pressure, high stakes, ambiguous information, and cascading operational failures (Coombs, 2015, p. 104).

Historically, crisis decision-making relied heavily on centralized command structures, executive intuition, and manual information processing. However, the sheer volume, velocity, and variety of data generated during contemporary emergencies render legacy decision-making paradigms obsolete. The emergence of Information Management Technology (IMT)—encompassing Big Data Analytics, Geographic Information Systems (GIS), Artificial Intelligence (AI), Internet of Things (IoT) sensor networks, and Enterprise Resource Planning (ERP) engines—has fundamentally redefined the mechanics of emergency governance (Laudon & Laudon, 2020, p. 198).

IMT functions as an architectural conduit that systematically collects, filters, processes, and disseminates critical information, transforming unstructured raw signals into actionable strategic intelligence. Despite the widespread deployment of these technologies, significant gaps remain in understanding how IMT interacts with cognitive human limitations, organizational workflows, and institutional environments during acute stress.

This paper provides an analytical framework examining the role of IMT in crisis decision-making. Specifically, it aims to:

1. Deconstruct the theoretical mechanisms through which IMT mitigates human cognitive constraints and enhances organizational information processing during crises;
2. Analyze the functional applications of IMT across the three primary phases of crisis management: proactive detection, operational response, and post-crisis learning;
3. Explicate the architectural components and data-fusion pipelines that underpin modern Crisis Information Systems (CIS);
4. Examine the contextual realities, infrastructural readiness, and administrative challenges of adopting IMT in developing and emerging economic frameworks, focusing on the Algerian administrative landscape; and
5. Identify the technological, socio-organizational, and security challenges that hinder optimal technology-mediated crisis response, offering strategic recommendations to enhance decision resilience.

© 2026 The authors
This article is licensed under the Creative Commons Attribution 4.0 International License — CC BY 4.0

Figure 1
Conceptual framework of the study



2. Theoretical and conceptual foundations

To understand how Information Management Technology influences decision-making during crises, we must ground the analysis in established organizational, cognitive, and information science frameworks. Crises create severe information pathologies; theoretical models explain how technology acts as an essential cognitive and structural intervention.

2.1 Bounded Rationality Theory and Computational Augmentation

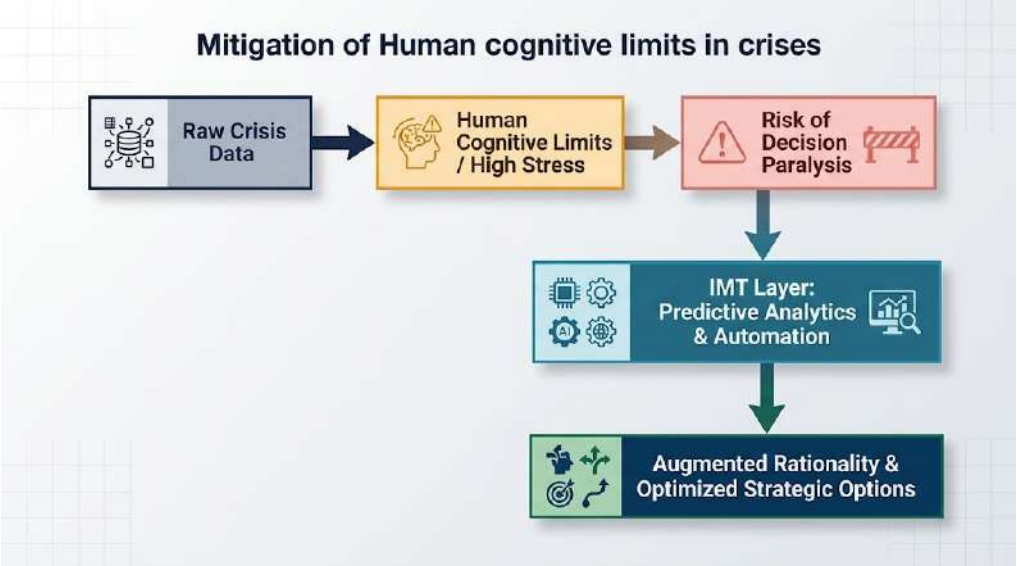
Herbert Simon's (1997, p. 84) Bounded Rationality Theory asserts that human decision-makers intend to be rational, but their rationality is constrained by three factors:

- Cognitive capacity limits in processing information,
- Incomplete or ambiguous information, and
- Severe time constraints.

During a crisis, these limitations become hyper-accentuated. Decision-makers experience extreme cognitive load, severe stress, and emotional fatigue, leading to cognitive heuristics, confirmation bias, premature cognitive closure, or decision paralysis (Simon, 1997, p. 91).

© 2026 The authors
This article is licensed under the Creative Commons Attribution 4.0 International License — CC BY 4.0

Figure 2
Mitigation of human cognitive limits in crises



IMT acts as an external cognitive prosthesis that expands human rationality. By automating data extraction, performing rapid multi-variable calculations, and deploying predictive algorithms (e.g., Monte Carlo simulations or Bayesian inference networks), IMT processes millions of data points per second. This computational augmentation mitigates cognitive load, enabling decision-makers to evaluate complex scenarios and transition from crude intuitive guesses to structured, data-informed choices (Laudon & Laudon, 2020, p. 205).

2.2 Information Processing Theory: Uncertainty vs. Equivocality

Galbraith's (1973, p. 36) Information Processing Theory conceptualizes organizations as information-processing networks designed to cope with uncertainty and equivocality:

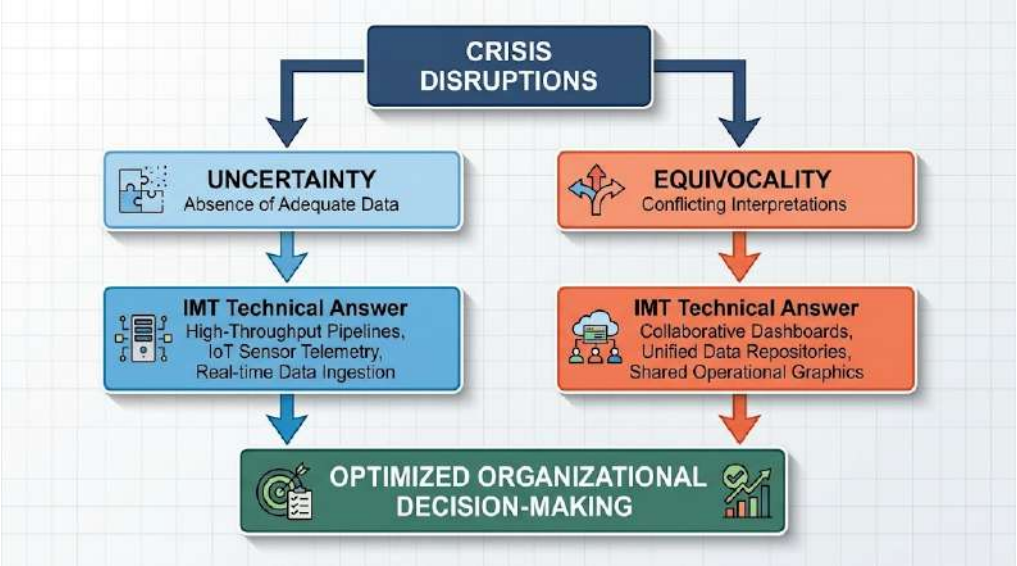
Uncertainty is defined as the gap between the amount of information required to perform a task and the amount of information already possessed by the organization.

Equivocality refers to the existence of multiple, conflicting, and ambiguous interpretations of a given situation.

Crises generate high levels of both uncertainty and equivocality. Information Management Technology addresses these challenges through two distinct pathways:

© 2026 The authors
This article is licensed under the Creative Commons Attribution 4.0 International License — CC BY 4.0

Figure 3
Information Management Technology responses to uncertainty and equivocality



1. **Uncertainty Reduction:** High-throughput data pipelines, IoT telemetry, and real-time remote surveillance collect objective environmental data, bridging the information gap (Galbraith, 1973, p. 48).
2. **Equivocality Reduction:** Shared operational pictures (COP), collaborative digital decision spaces, and integrated executive dashboards provide a single source of truth. This aligns disparate organizational units under a unified interpretive framework, reducing conflicting narratives (Tushman & Nadler, 1978, p. 613).

2.3 Organizational Sensemaking in Technology-Mediated Environments

Karl Weick's (1995, p. 54) Sensemaking Theory conceptualizes crisis response as an ongoing, dynamic process where actors structure ambiguous events to construct meaning: *"How can I know what I think until I see what I say?"* In high-velocity crisis settings, sensemaking precedes decision-making; if an organization misinterprets the nature of an evolving crisis, even flawless logical execution leads to failure.

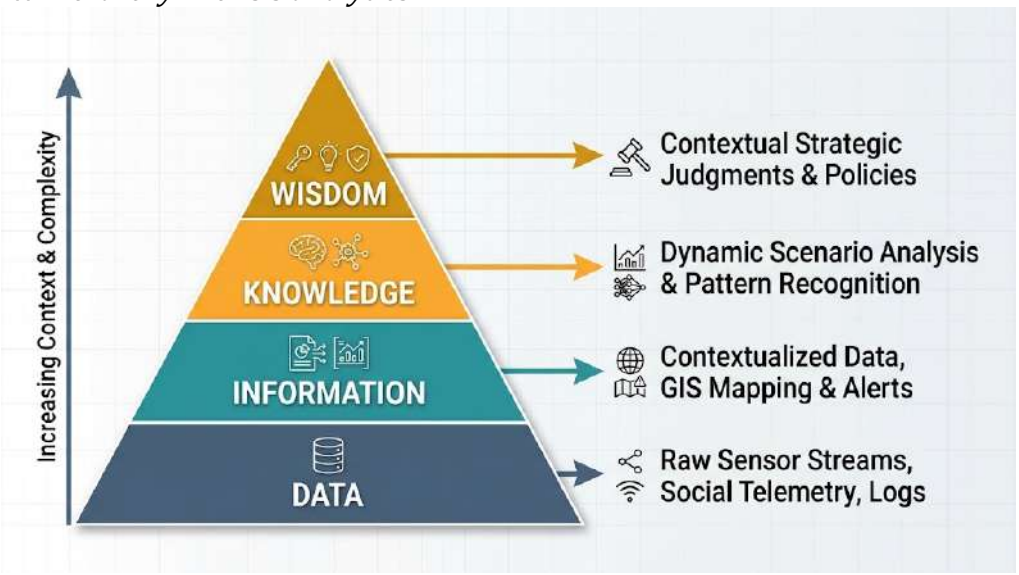
IMT transforms organizational sensemaking from a purely retrospective human activity into a continuous, real-time computational process (Weick, 1995, p. 62). Advanced data visualization tools, GIS mapping layers, and automated anomaly detection act as cognitive frames. They extract weak signals from complex environments, highlighting emergent patterns that would otherwise escape human perception. Technology establishes a continuous feedback loop: as field sensors transmit real-time data, digital visual interfaces update dynamically, enabling decision-makers to iteratively adjust their mental models to match shifting operational realities.

2.4 The DIKW Hierarchy in Crisis Analytics

The Data-Information-Knowledge-Wisdom (DIKW) pyramid provides an operational framework for understanding how raw inputs transform into high-level strategic directives during an emergency (Rowley, 2007, p. 165).

© 2026 The authors
This article is licensed under the Creative Commons Attribution 4.0 International License — CC BY 4.0

Figure 4
The DIKW hierarchy in crisis analytics



- **Data:** Unstructured, raw observations collected during a crisis (e.g., raw stream gauge levels, unverified social media posts, thermal imaging logs).
- **Information:** Structured, contextualized data (e.g., an automated system alerting that river water levels have exceeded critical flood thresholds by 1.5 meters).
- **Knowledge:** Synthesized insights produced by cross-referencing information with historical metrics, spatial maps, and predictive models (e.g., identifying specific residential zones at risk of inundation within three hours).
- **Wisdom:** Actionable strategic judgment exercised by human executive leaders using technology-derived knowledge (e.g., ordering targeted evacuations while rerouting emergency services to preserve critical infrastructure).

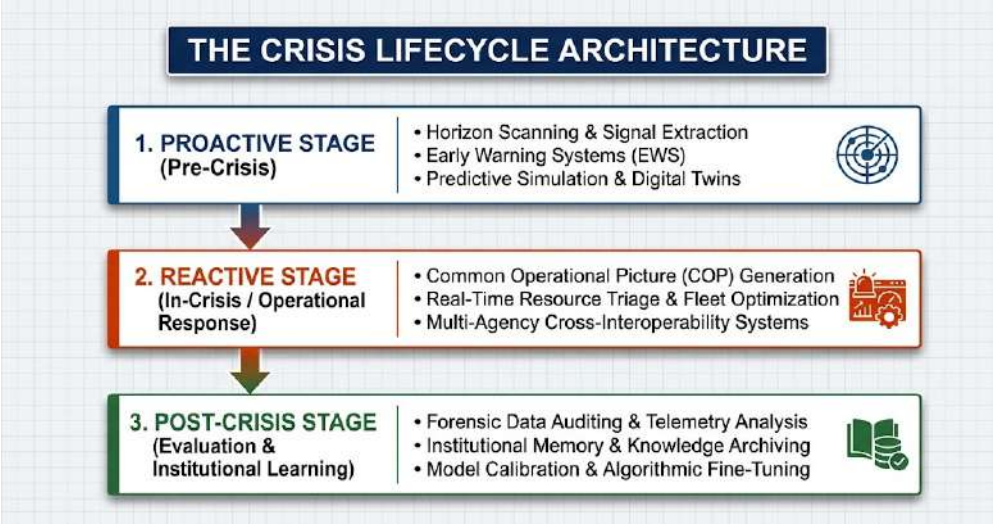
IMT automates the rapid progression from Data to Information and Knowledge, reserving the high-level cognitive domain of Wisdom for human decision-makers (Laudon & Laudon, 2020, p. 212).

3. Functional dimensions of IMT across the crisis lifecycle

Crisis management is not a single, isolated intervention; it is a continuous cycle. The strategic utility of Information Management Technology manifests differently across the three major operational phases: proactive (pre-crisis), reactive (in-crisis), and evaluative (post-crisis) (Bundy et al., 2017, p. 1668; Coombs, 2015, p. 110).

© 2026 The authors
This article is licensed under the Creative Commons Attribution 4.0 International License — CC BY 4.0

Figure 5
The crisis lifecycle architecture



3.1 The Proactive Stage: Signal Extraction, Early Warning, and Predictive Simulation

The primary objective during the pre-crisis phase is to identify latent vulnerabilities and weak signals before they escalate into open disruptions (Coombs, 2015, p. 112).

Horizon Scanning and Weak Signal Extraction

Crises rarely occur without warning; they are typically preceded by subtle anomalies across environmental, technical, or organizational telemetry. Modern IMT systems deploy web-scraping algorithms, natural language processing (NLP), and IoT sensor monitoring to conduct continuous horizon scanning. These platforms filter environmental noise to extract early indicators of instability, such as sudden shifts in public sentiment, minor structural oscillations in industrial equipment, or unusual epidemiological clusters.

Automated Early Warning Systems (EWS)

Integrated Early Warning Systems convert continuous environmental monitoring into automated protective actions. Utilizing spatial sensor networks, automated seismic monitors, and satellite telemetry, modern EWS platforms process data in real time and automatically trigger safety protocols—such as halting high-speed transit networks, closing industrial valves, and sending automated broadcasts to emergency personnel—well before human operators can analyze the raw data.

Predictive Simulation and Digital Twins

Advanced crisis management increasingly relies on Digital Twin technology—virtual, real-time digital replicas of physical assets, urban environments, or supply chains. Powered by computational fluid dynamics and agent-based modeling, Digital Twins allow decision-makers to run predictive simulations under various stress scenarios. Command

© 2026 The authors
This article is licensed under the Creative Commons Attribution 4.0 International License — CC BY 4.0

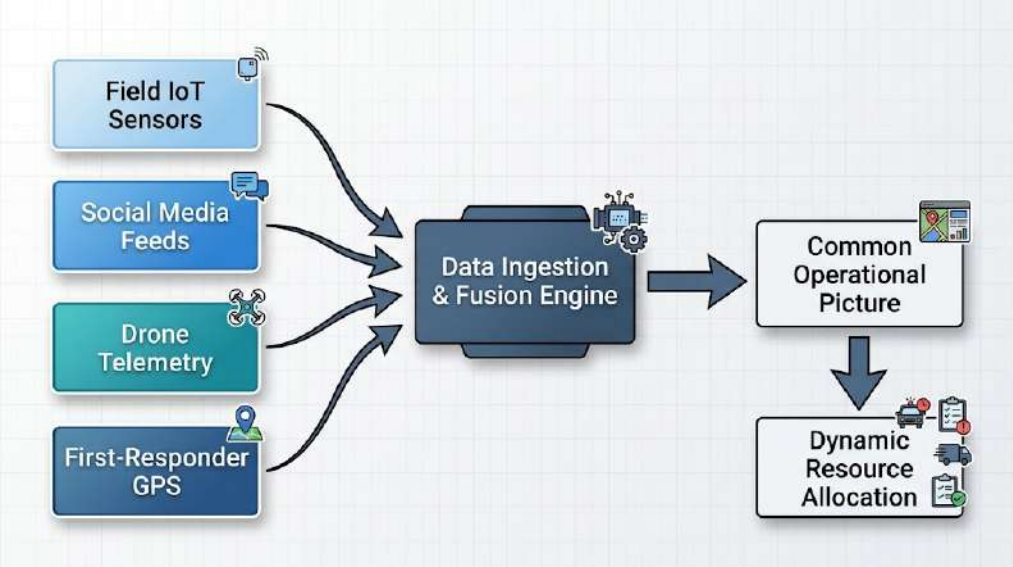
teams can model the impact of a dam failure, chemical spill, or grid failure, assessing potential cascades and pre-planning evacuation routes before a real-world disaster occurs.

3.2 The Operational Stage: Real-Time Command, Coordination, and Dynamic Response

When a crisis erupts, the strategic priority shifts to immediate containment, situational awareness, and efficient resource deployment (Bundy et al., 2017, p. 1672).

Figure 6

Multi-source data fusion and the common operational picture



Common Operational Picture (COP) Generation

In complex emergencies, different operational units (e.g., police, fire services, medical teams, municipal infrastructure authorities) often work with fragmented views of the situation. Modern Crisis Information Systems aggregate disparate data feeds into a centralized Common Operational Picture (COP). Geographic Information Systems (GIS) layer real-time spatial data—such as active hazards, road blockages, position tracks of emergency vehicles, and population densities—onto unified digital displays. This shared operational view reduces administrative silos, minimizes duplicate efforts, and aligns cross-agency responses.

Dynamic Resource Allocation and Fleet Optimization

Allocating scarce emergency assets under extreme pressure requires real-time optimization. Dynamic Decision Support Systems (DDSS) combine GPS tracking, traffic management feeds, and operational constraints to optimize resource deployment. Machine learning algorithms calculate optimal response vectors, prioritize high-risk service requests, and dynamically re-route supply units around physical hazards, significantly cutting response times.

© 2026 The authors
This article is licensed under the Creative Commons Attribution 4.0 International License — CC BY 4.0

Crisis Communication Infrastructure

Modern crisis management systems integrate multi-channel notification engines that broadcast tailored, location-specific instructions directly to affected populations via SMS alerts, mobile push notifications, and emergency broadcasts. Simultaneously, social media monitoring platforms capture public reactions, flag emerging rumors, and identify local cries for help, enabling response teams to counter misinformation and direct rescues to unserved areas (Coombs, 2015, p. 118).

3.3 The Post-Crisis Stage: Forensic Auditing, Organizational Learning, and Adaptation

The post-crisis period focuses on evaluating response efficacy, establishing accountability, and integrating institutional lessons (Bouakaz & Bouguelgoul, 2022, p. 108).

Forensic Telemetry Auditing

Modern digital crisis management architectures automatically log every decision, system action, data stream, and communication trace with immutable time-stamps. This creates an unalterable digital audit trail that allows post-incident investigation teams to systematically reconstruct the event timeline. Analysts can evaluate precisely what information was available at key moments, identify operational bottlenecks, and determine whether decision-makers followed established protocols.

Institutional Memory and Knowledge Repositories

Human operational memory degrades rapidly after intense crisis situations, leading to loss of tacit insights as personnel transition out of emergency roles (Ghiat, 2020, p. 42). IMT addresses this by capturing unstructured operational logs, communications, and debriefing reports, converting them into searchable knowledge repositories. Case-based reasoning (CBR) engines index these historical records, allowing future teams to draw upon past crisis responses when similar emergencies occur.

Model Recalibration and Continuous Optimization

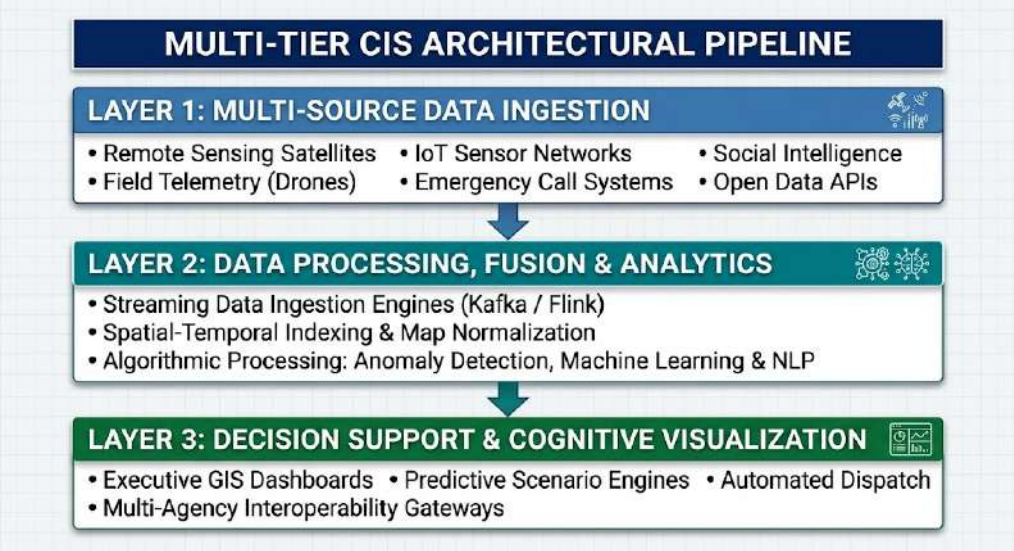
Post-crisis analysis provides empirical data used to refine predictive algorithms and simulation parameters. By comparing model predictions with actual crisis outcomes, data engineers can recalibrate predictive algorithms, fine-tune spatial risk models, and update standard operating procedures (SOPs), ensuring the organization's information architecture improves continuously.

4. Technical architecture and data fusion engines in modern CIS

The technical architecture of modern Crisis Information Systems (CIS) relies on a multi-tier data pipeline designed to maintain stability, high availability, and real-time responsiveness during network strain and extreme operational conditions.

© 2026 The authors
This article is licensed under the Creative Commons Attribution 4.0 International License — CC BY 4.0

Figure 7
Multi-tier CIS architectural pipeline



4.1 Ingestion Layer: Heterogeneous Data Collection

The baseline tier must continuously ingest structured, semi-structured, and unstructured data streams from diverse, geographically distributed sources:

- **Internet of Things (IoT) Telemetry:** Environmental telemetry from hydrological sensors, industrial pressure monitors, structural health sensors, and atmospheric detectors.
- **Remote Sensing and Aerial Imagery:** High-resolution satellite images and synthetic aperture radar (SAR) feeds combined with real-time video streams from Unmanned Aerial Vehicles (UAVs).
- **Social Intelligence (SOCINT):** Geotagged social media posts, public RSS feeds, and crowd-sourced emergency reports processed using Natural Language Processing (NLP) to extract location data and urgent calls for help.
- **Institutional Operational Systems:** Internal databases, supply inventory tracking systems, and emergency call logs.

4.2 Fusion and Processing Layer: Algorithmic Synthesis

Raw, multi-source crisis data is often redundant, noisy, and unverified. The fusion layer transforms these noisy streams into clean operational inputs:

- **Stream Processing Engines:** Systems like Apache Kafka and Apache Flink ingest high-velocity data feeds with minimal latency.
- **Spatial-Temporal Indexing:** Heterogeneous data points are spatialized and time-stamped, aligning disparate information to exact physical locations and chronological markers.
- **Artificial Intelligence and Machine Learning Modules:** Computer vision models analyze drone footage to assess structural damage, while machine learning algorithms filter out spam and false alarms from public social feeds, verifying incoming reports before routing them to dispatch teams.

© 2026 The authors
This article is licensed under the Creative Commons Attribution 4.0 International License — CC BY 4.0

4.3 Presentation and Action Layer: Decision Visualization Interfaces

The top tier translates complex processed analytics into clean visual interfaces designed for high-stress operational environments:

- **Interactive GIS Overlays:** Real-time spatial maps that display hazard perimeters, affected infrastructure, resource locations, and population densities.
- **Automated Risk Triage Dashboards:** Visual panels that highlight system anomalies, display critical thresholds, and provide dynamic risk-score calculations for different operational sectors.
- **Interactive Scenario Builder:** Interfaces that allow executive leaders to model "what-if" choices (e.g., closing a bridge or rerouting power) and view real-time estimates of impact on emergency response times and public safety.

5. Technological context and empirical realities in developing economies: focus on Algeria

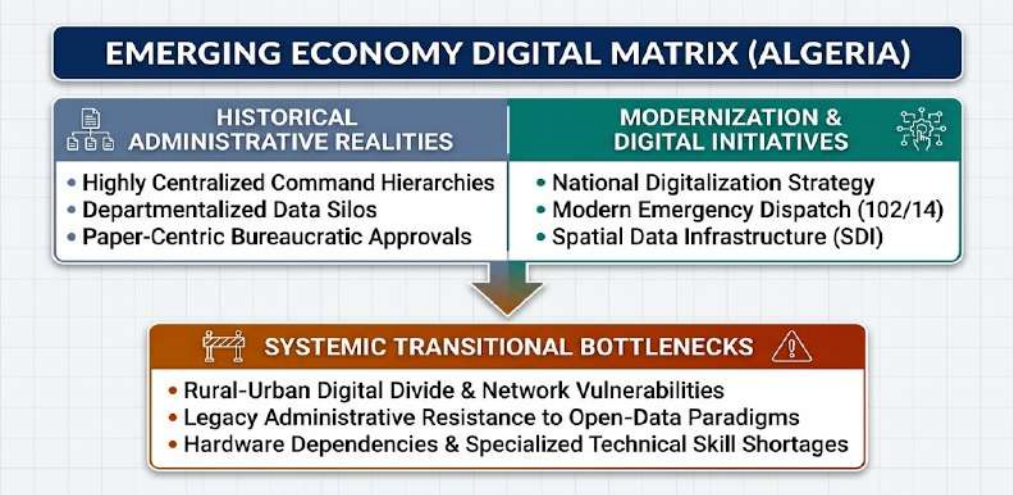
While advanced economies deploy high-speed, integrated information ecosystems for emergency response, developing and emerging economies navigate a distinct set of structural realities. Socio-technical constraints, historical administrative practices, and infrastructure gaps significantly shape how Information Management Technologies perform during crises (Ali, 2021, p. 98; Djellio, 2003, p. 81).

5.1 The Administrative Context and Digital Modernization in Algeria

The administrative landscape in Algeria provides an informative case study of an emerging economy transitioning from legacy, paper-centric governance models toward modernized digital public infrastructures (Ali, 2021, p. 102). Historically, administrative structures across the MENA region relied on highly centralized command hierarchies and rigid bureaucratic approvals. This structure can restrict intra-agency data sharing and delay decision-making during fast-moving crises (Djellio, 2003, p. 88).

Figure 8

Emerging economy digital matrix (Algeria)



© 2026 The authors
This article is licensed under the Creative Commons Attribution 4.0 International License — CC BY 4.0

In recent years, strategic national initiatives—such as Algeria's National Digitalization Strategy—have aimed to modernize emergency infrastructure, upgrade public sector ICT networks, and establish unified digital platforms (Ali, 2021, p. 105). Efforts to build national Spatial Data Infrastructures (SDI) and upgrade emergency response frameworks (such as the modernized dispatch systems used by Civil Protection centers) demonstrate a clear commitment to technology-driven crisis governance (Bouakaz & Bouguelgoul, 2022, p. 112).

5.2 Contextual Bottlenecks in Emerging Administrative Environments

Despite these digital modernization efforts, implementing IMT for crisis decision-making in developing administrative environments faces structural challenges:

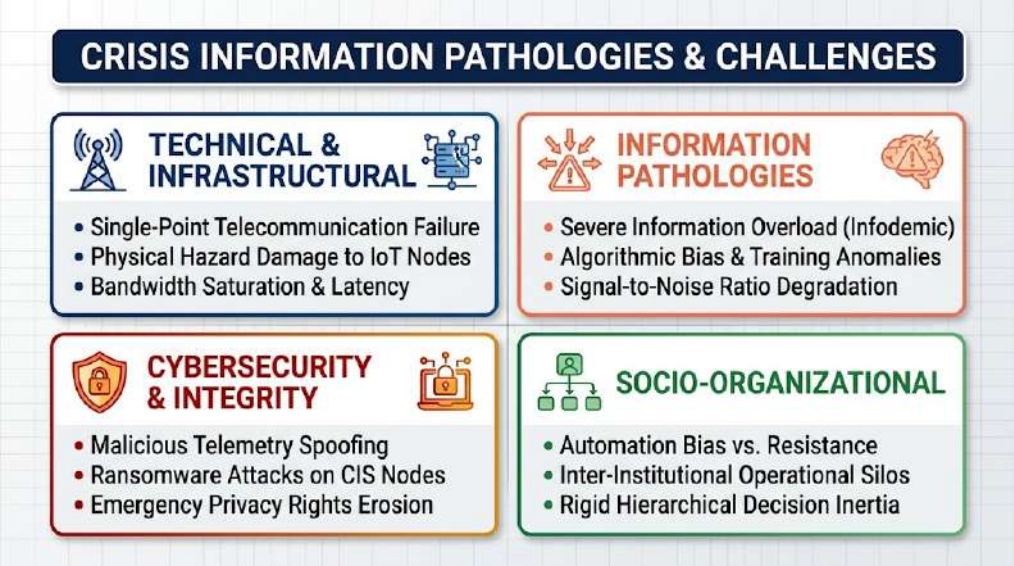
1. **Fragmented Data Infrastructure and Interoperability Silos:** Information systems are frequently built in departmental silos. Fire services, public health agencies, municipal authorities, and security services often run disparate software applications that cannot exchange real-time data automatically. This fragmentation limits the creation of a dynamic Common Operational Picture (COP) (Djellio, 2003, p. 90; Ghiat, 2020, p. 50).
2. **The Urban-Rural Digital Divide:** High-bandwidth connectivity and advanced sensor networks are heavily concentrated in major metropolitan areas (e.g., Algiers, Oran, Constantine). Remote, high-risk regions—such as desert areas or mountainous zones prone to wildfires and flash floods—frequently suffer from fragile network coverage. This dynamic leaves regional decision-makers reliant on legacy communication channels during critical events (Ali, 2021, p. 108).
3. **Organizational Culture and Bureaucratic Resistance:** The transition from traditional hierarchical authority to decentralized, data-driven decision-making often encounters cultural inertia. Administrative personnel may resist algorithmic recommendations or hesitate to share departmental data across organizational boundaries, viewing raw information as an asset to be guarded rather than a shared operational resource (Ghiat, 2020, p. 54).
4. **Skills Shortages and Maintenance Dependencies:** Deploying advanced analytics, managing spatial databases, and securing critical IT infrastructure require specialized technical talent. Public sector administrative institutions in emerging economies often struggle to recruit and retain high-level software engineers, GIS experts, and cybersecurity specialists, leading to operational reliance on external software vendors (Bouakaz & Bouguelgoul, 2022, p. 115).

6. Strategic, technical, and socio-organizational challenges

Deploying Information Management Technology during high-stakes crises introduces operational trade-offs and risks. Technology improves operational capacity, but it also creates vulnerabilities that can undermine effective decision-making if left unaddressed.

© 2026 The authors
This article is licensed under the Creative Commons Attribution 4.0 International License — CC BY 4.0

Figure 9
Crisis information pathologies and challenges



6.1 Technical and Infrastructural Vulnerabilities

Information systems depend on physical infrastructure that is itself vulnerable to natural and man-made disasters:

- **Telecommunications Breakdown:** Earthquakes, severe storms, and industrial explosions can destroy local cell towers, fiber-optic cables, and electrical grids, taking online CIS platforms offline precisely when they are needed most.
- **Hardware Degradation:** Edge IoT sensors deployed in hostile environments (e.g., severe heat, extreme moisture, or high chemical toxicity) are prone to physical failure, calibration drift, and signal loss, which can introduce corrupted data streams into predictive models.

6.2 Information Pathologies: Cognitive Overload and the Infodemic

While missing information creates uncertainty, an overabundance of unstructured data causes severe operational friction:

- **Information Overload:** During an acute crisis, decision-makers can be overwhelmed by thousands of incoming alerts, messages, and data streams. This cognitive saturation increases stress and delays critical choices (Laudon & Laudon, 2020, p. 215).
- **Infodemics and Misinformation:** Modern emergencies are often accompanied by rapid spreads of unverified rumors, altered media, and intentional disinformation across public networks. If unverified reports slip past data-filtering layers, emergency resources can be wasted responding to false alarms (Coombs, 2015, p. 122).
- **Algorithmic Bias:** Machine learning models trained on historical datasets may inadvertently incorporate systemic biases. For instance, an emergency dispatch algorithm trained primarily on urban data might miscalculate risk scores or response times when deployed in rural contexts.

© 2026 The authors
This article is licensed under the Creative Commons Attribution 4.0 International License — CC BY 4.0

6.3 Cybersecurity Weaknesses and Data Integrity Risk

As crisis response infrastructures become increasingly digitized, they become targets for malicious threat actors:

- **Telemetry Spoofing and Cyber Attacks:** State-sponsored actors or criminal syndicates can compromise emergency networks using ransomware or inject false telemetry into public safety databases, disrupting emergency responses and triggering mass confusion.
- **Privacy and Surveillance Concerns:** Emergency measures often require tracking population movements via mobile phone location metrics or deploying facial recognition systems. Without clear governance frameworks, temporary emergency surveillance tools risk becoming permanent intrusions on civil liberties.

6.4 Socio-Organizational and Cultural Resistance

The primary barriers to effective IMT adoption are frequently human and organizational rather than technological:

- **Automation Bias vs. System Distrust:** Personnel often exhibit one of two dangerous extremes: total over-reliance on automated recommendations without critical review (*automation bias*), or complete distrust of algorithmic models in favor of personal intuition (*technological resistance*).
- **Data Hoarding Culture:** Bureaucratic structures often treat data as institutional property. Departmental leaders may resist sharing key datasets with external emergency services, limiting the development of a real-time Common Operational Picture (COP) (Djellio, 2003, p. 91; Ghiat, 2020, p. 56).

7. Comparative analytical synthesis

The following comparative matrices summarize the dimensions, challenges, and theoretical applications of Information Management Technology in crisis governance.

Table 1

Comparative matrix of IMT functional dimensions across crisis stages

Functional Phase	Strategic Focus	Primary Technological Tools	Key Information Inputs	Primary Decision Output	Key Limitations
Proactive (Pre-Crisis)	Early detection, threat mapping, pre-disaster planning	Predictive Analytics, Digital Twins, Satellite Remote Sensing, IoT Environmental Sensors	Satellite imagery, seismic telemetry, social sentiment feeds, historical trends	Dynamic hazard maps, automated early warnings, evacuation route simulations	Signal noise, false alarms, high initial capital investment
Reactive (In-Crisis)	Rapid response, operational coordination, asset allocation	GIS Dashboards, Dynamic Dispatch Engines, Unified Emergency Networks (C4I)	Real-time GPS tracks, emergency calls (102/14), field drone streams	Automated asset deployment, shared operational view, real-time rerouting	Infrastructure damage, severe bandwidth constraints, infodemics

© 2026 The authors
This article is licensed under the Creative Commons Attribution 4.0 International License — CC BY 4.0

Functional Phase	Strategic Focus	Primary Technological Tools	Key Information Inputs	Primary Decision Output	Key Limitations
Post-Crisis (Learning)	Impact assessment, post-incident auditing, structural learning	Data Archiving Systems, Case-Based Reasoning Engines, Log Audit Software	Immutable system logs, incident timelines, post-disaster damage surveys	Updated SOPs, calibrated predictive models, institutional case records	Data retention gaps, organizational memory loss, debriefing bias

Table 2

Comparative synthesis of key theoretical frameworks

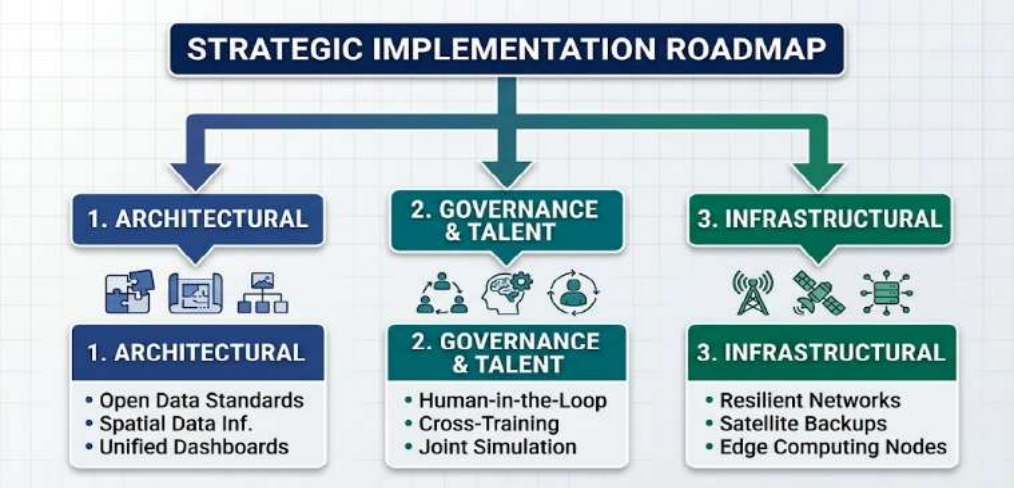
Theoretical Framework	Primary Conceptual Focus	Mechanism of Technological Intervention	Core Impact on Crisis Decision-Making	Key Literature Reference
Bounded Rationality	Human cognitive limits under severe stress and time pressure	Automates calculations, runs simulations, and filters complex data streams	Mitigates cognitive overload; shifts decision-making from intuition to data-informed options	Simon (1997, p. 84)
Information Processing	Reducing structural uncertainty and interpretive equivocality	Aggregates multi-source feeds into a Common Operational Picture (COP)	Closes the information gap and aligns cross-agency perspectives	Galbraith (1973, p. 36)
Organizational Sensemaking	Constructing shared meaning from ambiguous, fast-moving events	Provides real-time dynamic visualizations, spatial mapping, and anomaly highlights	Enables continuous updating of mental models to match changing operational realities	Weick (1995, p. 54)
DIKW Hierarchy	Transforming raw operational data into actionable strategic wisdom	Converts unstructured sensor logs into structured knowledge representations	Automates data-to-knowledge synthesis, allowing leaders to focus on high-level strategic judgments	Rowley (2007, p. 165)

8. Strategic recommendations and policy roadmap

To maximize the benefits of Information Management Technology while mitigating its structural and socio-technical risks, organizations and public policy leaders should adopt the following strategic roadmap:

© 2026 The authors
This article is licensed under the Creative Commons Attribution 4.0 International License — CC BY 4.0

Figure 10
Strategic implementation roadmap



8.1 Institutionalize Open-Data Standards and Interoperability Frameworks

- **Mandate Unified Data Protocols:** Governments should establish binding national open-data standards (e.g., XML/JSON schemas for emergency APIs) to ensure smooth real-time data exchange across fire services, health authorities, police forces, and municipal infrastructures.
- **Build National Spatial Data Infrastructures (SDI):** Emerging economies, including Algeria, should accelerate SDI development to provide a shared, authoritative geographic base layer for all public emergency agencies (Ali, 2021, p. 110).

8.2 Establish Human-in-the-Loop (HITL) Algorithmic Governance

- **Maintain Human Oversight for High-Stakes Decisions:** Automated algorithms should handle signal filtration, triage scoring, and predictive simulations, but human executive teams must retain sole authorization over critical actions like regional evacuations or asset destruction.
- **Regular Algorithmic Audits:** Subject crisis management models to periodic bias audits and stress-tests to verify performance across diverse geographical and socio-economic demographics.

8.3 Strengthen Infrastructure Resilience and Redundancy

- **Deploy Multi-Path Communication Networks:** Critical command centers must maintain redundant, multi-path communication channels, incorporating satellite broadband networks (e.g., Starlink, GEO satellites), mesh radios, and decentralized edge computing units to guarantee continuity if primary telecom grids fail.
- **Harden Edge Computing Infrastructures:** Move processing capabilities closer to physical sensors (edge nodes) to ensure field teams can run localized analytics even when disconnected from central servers.

8.4 Foster Digital Crisis Leadership and Joint Simulation Training

© 2026 The authors
This article is licensed under the Creative Commons Attribution 4.0 International License — CC BY 4.0

- **Conduct Simulation Drills:** Transition operational training from traditional desktop exercises to immersive, digital simulations using real-time predictive dashboards and Digital Twin scenarios.
- **Bridge Technical-Administrative Skill Gaps:** Build joint training pipelines for emergency leaders, public administrators, and data scientists to build shared technical literacy and reduce organizational resistance during actual crises (Ghiat, 2020, p. 57).

9. Conclusion

Information Management Technology has fundamentally transformed modern crisis decision-making. By expanding the limits of human cognition, providing clear structural frameworks for sensemaking, and converting massive streams of unstructured data into actionable strategic intelligence, modern IMT enables organizations to respond to acute disruptions with greater speed, accuracy, and operational coordination.

However, technology alone cannot guarantee effective crisis response. Technology functions as an amplifier of underlying organizational dynamics: when deployed within fragmented, highly siloed, or technologically resistant administrative environments, even sophisticated information systems struggle to deliver their full potential. Furthermore, reliance on digital systems introduces vulnerabilities, including information overload, infodemics, cyber risks, and single-point infrastructural failures.

For emerging economies—including Algeria and the broader MENA region—the path forward requires balancing capital investments in digital infrastructure with targeted institutional reforms. Bridging intra-agency silos, standardizing data protocols, establishing robust governance frameworks, and fostering a digital-centric emergency leadership culture are critical steps. By aligning advanced technological architectures with resilient human decision-making processes, organizations can build robust crisis governance capabilities equipped to navigate an increasingly complex world.

References

Ali, K. (2021). Digital transformation and crisis response in Algerian public administration. *Algerian Journal of Security and Development, 10*(1), 95–112.

Bouakaz, R., & Bouguelgoul, M. (2022). The role of modern information systems in crisis management. *Journal of North African Studies, 15*(2), 101–118.

Bundy, J., Pfarrer, M. D., Short, C. E., & Coombs, W. T. (2017). Crises and crisis management: Integration, interpretation, and research development. *Journal of Management, 43*(6), 1661–1692. https://doi.org/10.1177/0149206316680030

Coombs, W. T. (2015). *Ongoing crisis communication: Planning, managing, and responding* (4th ed.). SAGE Publications.

Djellio, A. (2003). *Organizational communication and administrative reform in developing nations*. University Publications Office.

Galbraith, J. R. (1973). *Designing complex organizations*. Addison-Wesley.

Ghiat, B. (2020). *Administrative change and information technology in Algerian enterprises*. National Library Publications.

Laudon, K. C., & Laudon, J. P. (2020). *Management information systems: Managing the digital firm* (16th ed.). Pearson.

© 2026 The authors
This article is licensed under the Creative Commons Attribution 4.0 International License — CC BY 4.0

Rowley, J. (2007). The wisdom hierarchy: Representations of the DIKW hierarchy. *Journal of Information Science, 33*(2), 163–180. https://doi.org/10.1177/0165551506070706

Simon, H. A. (1997). *Administrative behavior: A study of decision-making processes in administrative organization* (4th ed.). The Free Press.

Tushman, M. L., & Nadler, D. A. (1978). Information processing as an integrating concept in organizational design. *Academy of Management Review, 3*(3), 613–624. https://doi.org/10.5465/amr.1978.4305756

Weick, K. E. (1995). *Sensemaking in organizations*. SAGE Publications.