Mediascapes journal 26/2025

Smart Alerts for Complex Risks: A Dual-Risk Framework for Understanding AI-Driven Crisis Communication in the Computational Age[*]

Kulsawasd Jitkajornwanich[**]
Texas Tech University

Kerk F. Kee[***]
Texas Tech University

This paper develops a framework for "smart alerts" that explains how artificial intelligence (AI) and computational social media analytics are reshaping crisis communication, amplifying detection speed and message personalization while introducing new categories of technological risk. We theorize a dual-risk structure: (1) primary hazards (e.g., floods, wildfires) that alerts aim to mitigate, and (2) secondary risks embedded in AI-mediated communication systems (false positives, bias, privacy, deepfakes). Using a speculative design approach and an illustrative technical case study of Twitter-based flood detection in Thailand, we show how human–AI collaboration models (AI-assisted, human-supervised, and parallel processing) can be operationalized from data ingestion and geocoding to visualization and verification. We propose three cross-cutting design and governance mechanisms: graduated confidence communication, multi-source verification, and adaptive governance architectures. They jointly balance the speed–accuracy dilemma while safeguarding equity and democratic accountability. The framework advances crisis and strategic communication by (a) reframing time in predictive messaging (from reactive to anticipatory communication), (b) specifying organizational design patterns for decision rights and oversight in AI-enabled warning systems, and (c) articulating implementable practices that can sustain public trust. We conclude with implications for empirical evaluation and policy design.

Keywords: Smart alerts, AI-enabled crisis communication, human–AI collaboration, predictive risk communication, multi-source verification, adaptive governance architectures

[*] Article submitted on 22/09/2025. Article accepted on 20/12/2025.
[**] kulsawasd.jitkajornwanich@ttu.edu
[***] kerk.kee@ttu.edu

Introduction

The perfect storm of artificial intelligence, social media platforms, and computational communication methods is transforming how societies detect, communicate, and respond to disasters and emergencies. As climate change intensifies the frequency and severity of natural disasters, traditional emergency management systems face unexpected challenges in providing timely, accurate, and actionable crisis communication (Alexander, 2014; Vogler & Meissner, 2024). The limitations of traditional disaster response mechanisms, which typically require hours of data processing and verification before issuing public warnings, have become apparent in contexts where minutes can determine life-or-death situations.

This paper presents a framework for understanding how AI-enabled social media analytics can revolutionize crisis communication while simultaneously introducing new categories of risk and ethical complexity. Drawing from computational communication research and disaster management literature, we explore the dual nature of risk communication in the digital/computational age: how emerging technologies both enhance our capacity to detect and communicate about disasters while creating novel forms of risk embedded within the communication processes themselves (Beck, 2009; Klinga & Lundgren, 2024). The framework addresses a critical gap in current literature by examining not only how AI and social media can improve disaster response, but also how over-reliance on these technologies might create new vulnerabilities in emergency management systems (Meißner & Diers-Lawson, 2022).

The research questions we are exploring include: How can AI-enabled social media analytics transform early warning systems while managing risks of mis- and dis-information and false positives? What speculative frameworks best capture the relationship between human decision-making and automated systems in crisis communication? How might future dependencies on AI-driven disaster analytics create new forms of systemic risk that communicators and policymakers have to anticipate? These questions are urgent given recent technological developments in generative AI, which expand analytical capabilities and at the same time make it harder to verify the analytical outcomes.

Our analysis employs a speculative design approach, examining both promising applications and concerning implications of AI-enabled crisis communication through multiple perspectives. We propose a theoretical framework that positions crisis communication at the intersection of technological capability, institutional authority, and public trust, while acknowledging the uncertainties in predicting how these relationships will develop. The paper contributes to strategic communication scholarship by offering an analysis of how emerging technologies might transform fundamental assumptions/theories about risk communication, institutional legitimacy, and public engagement during emergencies. We next synthesize prior research, delineate the systemic risks introduced by AI-mediated communication, and then advance a dual-risk framework operationalized through a Thailand flood-detection case and implementation guidance.

To guide the readers, the paper proceeds in five stages. First, the literature review synthesizes research on social media, AI-enabled detection, and human–AI collaboration to establish the conceptual foundations of smart-alert systems. Second, the analytical approach clarifies how the paper integrates a secondary re-analysis of the Thailand case with a speculative design–driven framework to surface generalizable design principles. Third, the conceptual sections develop the dual-risk structure and examine human–AI collaboration dynamics that shape the detection, verification, and communication of emerging hazards. Fourth, the Thailand case analysis and the subsequent Context and Transferability section show how these dynamics materialize in practice and how they must be adapted across sociotechnical, institutional, and linguistic domains. Fifth, the Strategic Frameworks for Implementation and the Adaptive Governance Architectures for Smart-Alert Systems sections articulate operational and institutional mechanisms (e.g., graduated confidence communication, multi-source verification, and adaptive governance architectures) that help organizations balance primary and secondary risks in real-world deployments.

Literature Review

Social Media as Crisis Information Infrastructure

This section synthesizes research across social media analytics, AI-enabled detection, and human–AI interaction to establish the conceptual foundations for the dual-risk framework developed later in the paper. Scholarship in crisis informatics has increasingly shown that social media now operates as both an informational sensor network and a dynamic communication arena during emergencies. Rather than functioning solely as downstream channels for official alerts, platforms such as X (formerly known as Twitter), Facebook, TikTok, and LINE enable publics to co-produce situational awareness through real-time observations, problem reporting, emotional expression, and community coordination (Mirbabaie et al., 2020). This collective behavior establishes a distributed early-warning system in which crisis-relevant signals frequently surface before formal authorities issue updates or confirm events (Reuter & Kaufhold, 2018).

Yet the same affordances that enable rapid signal emergence (e.g., low barriers to posting, high visibility, and algorithmic amplification) also introduce volatility. Studies show that during uncertain, high-stress events, information flows mutate quickly, generating mixtures of verified facts, speculation, emotional narratives, and misleading content (Gu et al., 2022). Public attention can swing dramatically in response to dramatic imagery, sensational framing, or rapid-fire sharing, creating feedback loops that heighten pressure on institutions to respond. This dual role of social media as both accelerator and distorter complicates institutional efforts to maintain authoritative communication in real time.

AI-Enabled Detection and Predictive Analytics

Concurrently, advancements in AI-driven detection systems have attempted to systematize the use of social metadata for disaster monitoring by leveraging natural language processing, image processing, computer vision, anomaly detection, and geospatial inference to identify hazards earlier than traditional infrastructures. Recent reviews (Reuter et al., 2023) indicate that these systems often succeed at surfacing meaningful crisis signals (e.g., localized flooding, wildfire spread, infrastructure disruption) faster than human analysts or official sensors.

However, the incorporation of AI also expands the crisis communication risk landscape. Machine-learning models depend on probabilistic inference, incomplete data, and historically biased training sets, generating error distributions that are difficult for non-experts to interpret. Research in human–AI interaction demonstrates that individuals alternately over-trust or over-scrutinize automated outputs, depending on prior expectations, the visual presentation of AI results, and the sociotechnical context in which decisions are made (Wu et al., 2024). These dynamics create vulnerabilities not only in detection accuracy but also in public confidence, as erroneous alerts or false negatives can cascade into legitimacy crises for institutions.

Synthetic Media and Misinformation

A rapidly evolving layer of complexity stems from the emergence of synthetic media and deepfakes, driven by generative AI. High-fidelity deepfakes can convincingly simulate political leaders, emergency managers, meteorologists, or even eyewitnesses, mimicking voices, facial expressions, and emotional cues with increasing realism. Recent empirical work demonstrates that deepfake audio and video can meaningfully distort risk perception, hinder institutional verification processes, and trigger public confusion, particularly during fast-moving disasters when information needs are acute and time pressure is high (Vaccari & Chadwick, 2020).

Further, comparative analyses show that AI-generated misinformation spreads faster than human-crafted content, elicits stronger emotional and threat responses, and is harder for users to evaluate heuristically in crisis contexts (Vaccari & Chadwick, 2020; Vosoughi et al., 2018). This transforms misinformation management from a downstream message-correction task into an upstream authenticity and provenance challenge, heightening the secondary risks associated with premature alerts, adversarial manipulation, and cross-platform spillover.

Human-AI Collaboration and Crisis Decision-Making Under Uncertainty

Large-scale crisis communication systems increasingly depend on hybrid human–AI workflows, in which AI provides interpretive or predictive support for human-led decisions. Research consistently shows that hybrid models outperform either human-only or automation-only systems in high-uncertainty environments. However, collaboration introduces new epistemic and operational challenges. Human decision-makers may exhibit automation bias (accepting AI outputs with insufficient scrutiny) or algorithm aversion (discounting AI outputs after observing errors), both of which can distort decisions during emergencies.

The AIsmosis framework (Bozdag, 2023) offers an important conceptual complement here. Rather than seeing humans and AI as discrete actors that exchange information in linear stages, AIsmosis describes how responsibilities, interpretations, and decision heuristics gradually "seep" between human and algorithmic components. This highlights why errors or blind spots in one part of the system can migrate into others, producing compound failures that are difficult to trace. In crisis communication systems, this seepage means that thresholds, confidence scores, and signal classifications can implicitly shape human judgment, even when officials believe they are exercising independent oversight.

Synthesis: Toward a Dual-Risk Understanding of AI-Driven Crisis Communication

Across these literatures, a consistent insight emerges: the same technological advances that promise earlier detection and more adaptive communication simultaneously introduce new forms of secondary risk. Social media accelerates informational visibility but magnifies noise; AI enhances detection but embeds probabilistic uncertainty; synthetic media expands expressive richness but destabilizes authenticity; and hybrid human–AI collaboration boosts capacity but complicates responsibility and trust.

Together, these developments establish the analytical foundation for a dual-risk perspective: modern crisis communication systems must manage not only the primary hazard (floods, fires, storms, public health threats) but also the risks produced by the detection, interpretation, and communication processes themselves. This synthesis sets the stage for the next section, which presents a framework for understanding how AI-enabled crisis systems generate, mediate, and potentially mitigate dual-risk dynamics through governance, verification pathways, and adaptive communication strategies.

Analytical Approach and Methodological Positioning

This section clarifies how the paper integrates a secondary re-analysis of the Thailand case with a speculative design–driven conceptual approach, forming the methodological bridge between the literature review and the theoretical framework that follows. This paper integrates two complementary methodological components: a secondary case analysis and a speculative design–driven conceptual framework. First, we conduct a targeted re-analysis of an existing technical case, the Thailand Twitter-based flood detection system by Jitkajornwanich et al. (2018), focusing not on reproducing its engineering details but on extracting design principles, governance implications, and risk dynamics relevant to contemporary smart-alert systems. This constitutes a situated analytical reinterpretation, where previously published technical outcomes are examined through the lenses of crisis communication theory, human–AI collaboration, and uncertainty management.

Second, we adapt methods from speculative design to articulate a forward-looking dual-risk framework, using conceptual constructs (e.g., multi-source validation, graduated confidence communication) not as labels but as scaffolds for imagining plausible, near-future communication architectures. Together, these components provide both an empirical anchor and a normative, anticipatory framework for evaluating AI-enabled alert systems.

Role of Speculative Design in the Framework

Speculative design in this paper does not aim to forecast technological futures exactly but to clarify the design space of emerging AI-driven warning systems. It allows us to reason about conditions that do not yet exist at scale (e.g., automated multi-source verification, confidence-scaled public alerts) by formalizing the trade-offs, uncertainties, and governance challenges that such systems would introduce. The speculative component therefore functions as a methodological bridge that connects what we observe in the Thailand case (the challenges of noisy signals, variable precision, and verification pressure) to what institutions will face as they adopt increasingly automated infrastructures. This approach elevates the framework from description to conceptual intervention, helping identify where risks accumulate and how they might be mitigated.

Positioning the Paper as a Hybrid Conceptual–Empirical Contribution

This methodological configuration positions the paper between empirical and conceptual category. The re-analysis of the Thailand case provides an empirical grounding that demonstrates how early-warning systems operate within real sociotechnical constraints, while the speculative design component offers an anticipatory lens for identifying risks and governance requirements that are only partially visible in current deployments. This hybrid approach is appropriate given the rapidly evolving nature of AI-enabled crisis communication, where the empirical record remains incomplete and conceptual tools are needed to articulate future design requirements and institutional consequences.

Conceptualizing Dual Risk Structures

Building on the analytical approach above, this section introduces the paper's central conceptual contribution: the dual-risk structure that characterizes AI-enabled crisis communication systems and shapes the design tensions that follow. We define dual-risk structures in AI-enabled crisis communication as the need to manage, in tandem, (a) primary risks (the hazard itself: wildfire, flood, hurricane) and (b) secondary risks embedded in the communication system (verification errors, privacy–surveillance, bias/equity, ethical/cultural fit). The framework treats these as interdependent: interventions that lower primary risk (e.g., faster alerts) may raise secondary risk (e.g., false alarms, legitimacy loss). Accordingly, our design problem is to balance these risks through human–AI role design, confidence-matched messaging, verification across heterogeneous data sources, and adaptive oversight. The dual-risk framework builds from the insights surfaced in the Thai case but extends beyond them through speculative design, allowing us to articulate risk structures that are only partially visible in current implementations.

This dual-risk framing also clarifies how AI-enabled alert systems transform crisis communication into a multi-layered, interdependent process. Primary risks unfold in physical time and space, whereas secondary risks accumulate within sociotechnical infrastructures, such as algorithms, platform governance, institutional protocols, and public trust dynamics. Secondary risks include, but are not limited to, verification failures, bias and inequitable outcomes, privacy and surveillance concerns, and erosion of institutional trust, as summarized in Table 1 below. By conceptualizing these as mutually constitutive rather than separate domains, the framework makes visible why speed and accuracy cannot be optimized independently, why error tolerance becomes a normative rather than technical decision, and why institutions must design for uncertainty rather than attempting to eliminate it. This perspective provides the conceptual foundation for the subsequent sections on human–AI collaboration, verification, confidence-matched messaging, and governance.

Figure 1 and *Table 1* summarize the dual-risk structure and visually situate the design and governance components that the subsequent sections unpack in detail. Graduated Confidence Communication (GCC) refers to aligning public alert messages with model confidence; Multi-Source Verification (MSV) addresses the validation of AI-generated signals across data sources; and Adaptive Governance Architectures (AGA) captures institutional oversight and accountability mechanisms. The categories summarized in Table 1 represent analytically separable manifestations of secondary risk within the broader dual-risk structure illustrated in Figure 1. These components are intentionally cross-cutting: while each is shown as addressing specific secondary risks, they function jointly and reinforce one another across the system.

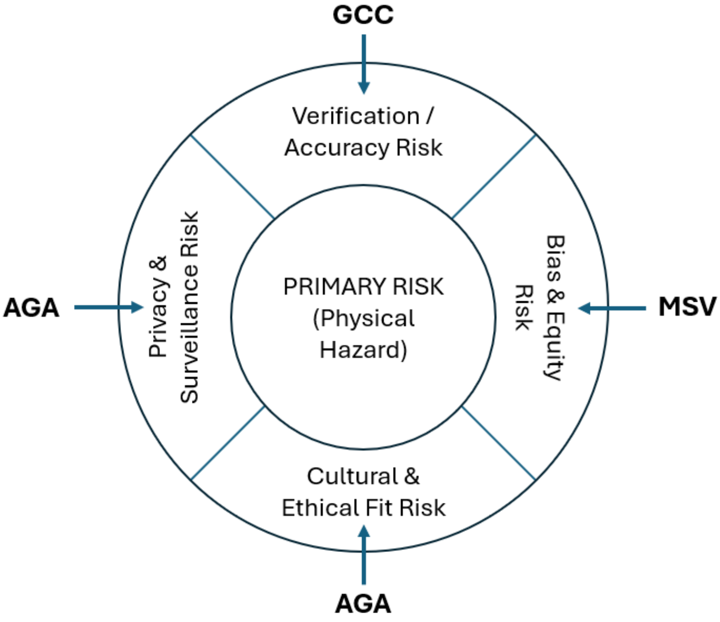
GCC
Verification / Accuracy Risk
Privacy & Surveillance Risk
AGA
PRIMARY RISK (Physical Hazard)
Bias & Equity Risk
MSV
Cultural & Ethical Fit Risk
AGA

Figure 1 - Dual-Risk Structure of AI-Enabled Smart-Alert Systems. Primary and secondary risks are shown as analytically distinct but dynamically interdependent, with feedback effects that can amplify crisis outcomes. Arrows indicate primary mitigation pathways rather than exclusive or ranked solutions; all three mechanisms operate jointly across multiple secondary risks.

Secondary Risk Category	*Description*	*Primary Mitigation via GCC*	*Primary Mitigation via MSV*	*Primary Mitigation via AGA*
Verification / Accuracy	Signal noise, inconsistent data, false positives/ negatives	Communicates uncertainty with confidence bands	Cross-checks with heterogeneous models and data sources	Establishes thresholds and oversight
Bias & Equity	Uneven platform adoption, representational bias	Reduces overconfidence bias	Includes multiple validation channels and incorporates human in the loop	Ensures equitable error distribution
Privacy & Surveillance	Data sensitivity, monitoring concerns	Limits unnecessary alerts and escalation	Minimizes intrusive and maximizes transparent data collection	Provides institutional safeguards
Cultural & Ethical Fit	Misaligned messaging, legitimacy loss	Tailors message confidence to appropriate context	Uses local knowledge in verification	Ensures culturally grounded governance

Table 1 - Mapping Secondary Risks to Framework Components

Human-AI Collaboration Models

Having established the dual-risk structure, this section examines how humans and AI systems interact within that structure, highlighting the collaboration dynamics that influence real-time detection, verification, and messaging. Rather than positioning AI and human decision-makers in opposition, the framework emphasizes complementary capabilities and collaborative decision-making structures. AI systems excel at rapid data processing, pattern recognition across large datasets, and consistent application of predefined criteria. Human decision-makers contribute contextual understanding, ethical reasoning, communication skills, and accountability mechanisms that AI systems currently lack. Effective crisis communication systems should leverage these complementary strengths while maintaining clear lines of responsibility and oversight.

The framework identifies three primary collaboration models: AI-assisted human decision-making, where AI provides analytical support for human-led communication decisions; human-supervised AI communication, where AI systems generate initial responses subject to human review and approval; and parallel processing systems, where AI and human analysis proceed simultaneously with integration occurring at the communication stage. Each model involves different trade-offs between speed, accuracy, accountability, and resource requirements.

An additional conceptual lens that enriches this section is the AIsmosis framework proposed by Bozdag (2023), which describes how algorithmic processes and human practices increasingly “seep into” one another, producing hybrid assemblages where the boundaries of agency, accountability, and authorship become blurred. AIsmosis is useful for crisis communication because it shows that collaboration between humans and AI is rarely discrete or cleanly partitioned into separate stages; instead, human judgment, algorithmic recommendation, automated filtering, and institutional protocols continuously shape one another.

Incorporating this perspective clarifies how our three collaboration modes (i.e., AI–assisted decision-making, human-supervised AI communication, and parallel human–AI processing) operate not as rigid categories but as fluid configurations that shift depending on data quality, urgency, and risk tolerance. It also reinforces our dual-risk argument: as human and AI roles intermingle, errors, biases, or gaps in one domain can migrate into another, creating new secondary risks. Applying the AIsmosis lens therefore underscores the necessity of explicit governance structures, audit trails, and decision-rights clarity to prevent invisible drift of responsibility and to maintain legitimacy in AI-mediated emergency messaging.

Critical to all collaboration models is the maintenance of human agency and accountability in final communication decisions. While AI systems may process information and generate recommendations faster than human analysts, the framework insists that human decision-makers must retain ultimate authority over public communication during emergencies. This principle reflects both practical concerns about AI reliability and ethical commitments to democratic accountability in government emergency response. The framework recognizes that maintaining human oversight while leveraging AI capabilities requires careful institutional design and clear protocols for when and how human judgment should override AI recommendations.

Temporal Complexity and Predictive Communication

The framework addresses the unique challenges posed by AI's capacity for predictive analysis and speculative warnings about potential future events. Traditional crisis communication has focused primarily on communicating about events that are currently occurring or imminent. AI analytics enable communication about events that may occur based on probabilistic assessments of current conditions and historical patterns. This predictive capability creates new opportunities for proactive emergency preparation while raising complex questions about appropriate communication strategies for uncertain risks.

The framework distinguishes between categorical predictions (event will occur), probabilistic predictions (event has X% likelihood of occurring), and speculative scenarios (event could occur under certain conditions). Each category requires different communication approaches, with categorical predictions warranting immediate action recommendations, probabilistic predictions requiring risk-benefit analysis, and speculative scenarios focusing on preparation and monitoring. The framework emphasizes that communication strategies must be matched to prediction certainty levels to maintain public trust and encourage appropriate responses.

Temporal considerations also extend to the evolving nature of AI capabilities and the need for communication systems that can adapt to technological change. The framework anticipates that AI analytical capabilities will continue expanding rapidly, potentially enabling prediction of events or conditions that are currently unforeseeable. Crisis communication systems must therefore be designed with sufficient flexibility to incorporate new AI capabilities while maintaining consistent public understanding and trust.

Emerging Opportunities and Applications

Multi-Modal Data Integration. Contemporary AI systems demonstrate unprecedented capabilities for integrating diverse data sources to create comprehensive situational awareness during developing emergencies. Social media platforms generate textual content, images, video, audio, geolocation data, engagement metrics, and temporal patterns that can be analyzed simultaneously to identify and characterize emerging situations (Alam et al., 2018). When combined with traditional data sources including satellite imagery, meteorological sensors, seismic monitoring, and institutional reporting, AI systems can potentially detect disasters faster and more accurately than any single data source alone.

The integration of emotional and sentiment analysis adds another dimension to disaster detection capabilities. Social media users experiencing or witnessing emergency situations often express fear, urgency, surprise, or other emotional responses that can provide additional signals about developing events. Engagement metrics such as sharing rates, reaction types, and comment patterns may indicate public perception of threat levels and the effectiveness of official communication. These behavioral indicators can inform both detection algorithms and communication strategy optimization.

Geospatial analysis capabilities enable AI systems to map disaster progression in real-time using crowdsourced location data extracted from social media posts, even when users have not explicitly enabled location sharing. The Thailand flood detection system demonstrated techniques for extracting location information from textual content, enabling detailed mapping of affected areas based on user reports (Jitkajornwanich et al., 2018). Advanced geocoding algorithms can identify specific streets, neighborhoods, or landmarks mentioned in social media posts and translate these references into precise coordinates for mapping and visualization.

Personalized Risk Communication. AI analytics create possibilities for personalized crisis communication that adapts message content, timing, and delivery channels to individual recipient characteristics and circumstances. Machine learning algorithms can analyze individual social media behavior, location patterns, demographic information, and communication preferences to optimize emergency message design and delivery. This personalization capability could significantly improve message effectiveness while raising complex privacy and equity concerns.

Individual risk tolerance preferences could be incorporated into personalized warning systems, allowing some users to receive alerts about low-probability events while others receive notifications only for high-confidence predictions. This approach addresses the fundamental tension between false positives and false negatives by allowing individual users to calibrate their personal alert thresholds. However, implementing such systems requires sophisticated user interface design and clear communication about the implications of different threshold settings.

Personalized communication could also adapt message design to reduce panic and encourage appropriate responses based on individual psychological profiles and historical response patterns. AI systems might learn which message framings, visual elements, or information structures are most effective for different user groups or populations. This capability could potentially reduce the amplification of fear and anxiety that sometimes accompanies emergency communication while ensuring that critical safety information reaches its intended audience effectively.

Proactive Communication and Scenario Planning. AI-enabled predictive analytics create opportunities for proactive communication about potential future risks before they materialize into actual emergencies. Weather pattern analysis, social media trend monitoring, and environmental sensor data can identify conditions that historically correlate with specific types of disasters, enabling early warning communication that help populations prepare for possible events. This predictive capability extends the temporal scope of crisis communication from reactive response to proactive preparation.

Speculative scenario communication could help populations understand and prepare for novel or unprecedented risk combinations that AI analysis identifies as potentially emerging. Climate change creates new combinations of environmental conditions that may produce disaster scenarios outside historical experience. AI systems capable of analyzing complex interactions between multiple risk factors could identify potential scenarios that human analysts might not anticipate, enabling communication about preparation strategies for previously unimaginable events.

Case Study Analysis: Twitter-Based Flood Detection in Thailand

Based on the early flood warning system developed by Jitkajornwanich et al. (2018) in Thailand, the following case analysis illustrates how the dual-risk dynamics and collaboration patterns described above materialize in a real-world sociotechnical context, showing both the strengths and limitations of social-media–based early detection. We treat the Thailand system not as a technical prototype to be described in detail but as an empirical illustration that, when reinterpreted, reveals generalizable principles and tensions relevant to AI-enabled crisis detection.

Technical Implementation

The Thailand flood-detection prototype illustrates how social media can serve as an early indicator of emerging hazards in contexts where official monitoring infrastructure is uneven or delayed. The system continuously collected Thai-language tweets that referenced flood-related terms and used a language-aware location extraction process to approximate where users were reporting problems. Because geotagged tweets are rare in Thailand, the system inferred locations by matching textual references to known administrative units (e.g., neighborhoods, districts, provinces) and broadening the search when finer-grain data were unavailable. This hierarchical approach balanced geospatial precision with computational efficiency, demonstrating a key design trade-off for smart-alert systems: finer-grain geocoding increases specificity but slows detection, while coarser matching accelerates alerts but may expand uncertainty zones.

The system also compared real-time tweet volumes against historically observed baselines to estimate whether emerging floods were statistically meaningful anomalies. This calibration tied directly to local communication patterns allowed the system to differentiate between routine chatter and genuine hazard-related spikes. Importantly, the goal was not to produce a fully automated warning tool but to show how platform-native signals, when processed thoughtfully, can complement official monitoring by detecting disruptions earlier than traditional channels.

User Behavior Analysis

Analysis of user activity revealed the distinctive communicative role that Twitter played during flood events in Thailand. Users frequently posted hyperlocal observations such as rising water levels, blocked roads, or drainage failures. These are information that rarely appears in formal reports but is crucial for situational awareness. Many users also engaged in “collective problem reporting,” tagging local authorities, journalists, or municipal accounts, which created organic feedback loops between residents and institutions. These interactions reinforced the notion that social media serves not only as a sensor network but also as a participatory crisis communication ecosystem, where communities help surface risks that institutions may not yet have verified.

At the same time, user behavior exhibited variability that affects early-warning reliability. During severe monsoon periods, for instance, high posting volumes reflected both genuine hazard conditions and heightened public anxiety, making it harder to distinguish meaningful signals from ambient noise. This underscores the importance of integrating behavioral baselines into smart-alert pipelines, a requirement relevant across cultural and linguistic contexts.

Visualization of Flood Signals

The visualization module went beyond standard Google Maps API implementation by aggregating geocoded tweet densities into simple heatmaps. The prototype translated social media activity into simple, interpretable visual outputs that indicated the approximate intensity and location of flood signals. Rather than providing precise maps or predictive modeling, the visualizations offered coarse but actionable indicators of where attention was increasing. These displays illustrated how even minimal geospatial inference, when aggregated across thousands of posts, can reveal patterns that would otherwise be difficult to perceive.

The visualizations served a conceptual purpose: they demonstrated how smart-alert systems must communicate degrees of confidence, not absolute certainty. Color scales, thresholds, and signal categories allowed the system to present emerging risks while making uncertainty explicit. This aligns directly with the design principles discussed in later sections, especially *Graduated Confidence Communication (GCC)*.

Validation and Implications for Early Detection

Comparison with official data from Thailand’s Royal Irrigation Department and the Bangkok Metropolitan Administration showed that social-media-derived signals frequently appeared minutes to hours before formal alerts or press releases. Although the system was not designed for operational forecasting, it demonstrated the potential for social signals to function as an anticipatory layer in multimodal early-warning infrastructures. This confirmatory evidence supports the broader argument of this paper: social media can accelerate hazard detection, but it also adds ambiguity that must be managed through structured verification and careful communication.

Importantly, the Thailand case revealed the operational limits of using social media for early detection. Linguistic ambiguity, uneven platform adoption, misinformation, and high-volume “chatter spikes” can all create false positives. These limitations highlight why smart-alert systems require multi-source validation (MSV), where social-data signals are examined alongside hydrological sensors, municipal reports, satellite imagery, or local community networks.

Context and Transferability

While the Thailand case grounds the framework empirically, this section clarifies the contextual limits of those insights and outlines how the underlying design principles can be adapted across different linguistic, institutional, and technological environments. Although this paper articulates its framework in broad terms, the operational realities of AI-enabled warning systems remain deeply context dependent. Factors such as platform adoption, linguistic diversity, institutional capacity, governance cultures, and public trust norms shape how dual-risk dynamics manifest in practice. As a result, the framework should be understood as a transferable analytic model, not a universal prescription. Its components require local calibration, cultural grounding, and institutional adaptation. Making these contextual limits explicit strengthens the framework by clarifying where its principles hold and where they must be modified.

While the Thailand case demonstrates the feasibility of social-media–based early warning systems, its implementation also reveals a series of procedural steps that can guide adaptation in other national or organizational contexts. At minimum, any deployment requires (1) access to platform data streams with sufficient volume and geographic relevance; (2) a mapping layer capable of translating user-generated content into approximate locations; and (3) a verification pathway that connects social signals to authoritative data sources (e.g., sensors, official monitoring agencies, or trusted community partners). The Thai system operationalized these components through hashtag- or keyword-based data collection, language-specific tokenization, multi-level geocoding using internal administrative boundaries, and rate-based thresholds calibrated to local tweeting behaviors.

In other countries or hazard settings, each of these steps would need to be contextualized rather than duplicated.

Practically, adaptation begins with establishing platform baselines. That includes understanding normal posting volumes, linguistic cues, dialects, and platform adoption rates within the population of interest. Because geocoding precision varies widely across languages and countries, implementers must assess which location cues are realistically extractable (e.g., street names, landmarks, neighborhood terms) and whether supplemental data sources (e.g., local place-name databases, crowd-curated gazetteers, or government-provided shapefiles) are available. Threshold-setting likewise must be recalibrated using local behavioral patterns, taking into account that a 0.05% spike in Thailand corresponds to very different absolute numbers in regions with lower social media activity.

Moreover, cross-context adoption requires embedding the system within existing institutional workflows. This includes identifying which agencies have authority to issue warnings, how AI-generated signals will enter decision protocols, and what verification steps are required before public communication. Even in lightweight implementations, smart-alert systems benefit from clear governance design: where data are stored, who validates alerts, how uncertainty is communicated, and what safeguards are in place to mitigate privacy, bias, and misclassification risks. These procedural considerations allow organizations to adapt the underlying model, even with very different languages, platforms, or hazards, while preserving the integrity and legitimacy of the alerts. Taken together, these contextual considerations point to the need for structured design approaches capable of guiding the operational deployment of AI-enabled alert systems.

Finally, thresholds, acceptable false-positive rates, and the prioritization of hazard types are not purely technical parameters; they are decisions made by institutions, communities, or cross-agency bodies that reflect local risk cultures, governance traditions, and social expectations. What counts as an “acceptable” error rate in one country or community may be unacceptable (or even harmful) in another. Recognizing these differences is essential for adapting smart-alert systems responsibly across diverse sociotechnical and institutional contexts.

Strategic Frameworks for Implementation

Building on the conceptual and empirical foundations developed in earlier sections, this part of the paper consolidates the operational design principles necessary for implementing AI-enabled smart-alert systems. These principles (i.e., Graduated Confidence Communication/GCC and operational Multi-Source Verification/MSV) translate the dual-risk framework into concrete mechanisms that guide how emerging signals are interpreted, validated, and communicated under conditions of uncertainty. Design patterns map directly to specific classes of secondary risk. In operational terms, GCC (messages scaled to model confidence) primarily mitigates verification and accuracy risks and secondarily supports ethical fit by tempering language, while MSV (cross-validation across social, sensor, and administrative data) mitigates verification/accuracy and bias/equity risks. The institutional role of adaptive governance architectures, such as addressing privacy–surveillance risks and sustaining legitimacy, is developed in the subsequent section.

Graduated Confidence Communication (GCC)

GCC serves as an operational mechanism to manage uncertainty and prevent premature escalation in early-warning contexts. Rather than issuing binary warnings, GCC communicates *graded levels of confidence* that reflect the evolving strength of the underlying signals. This structure provides institutional actors and publics with clearer expectations about how early indicators should be interpreted, and it helps prevent the overconfidence, misinterpretation, or alarm fatigue that often result from premature or overly definitive alerts.

GCC functions by translating probabilistic outputs in AI systems into structured tiers of communication (e.g., “signal of interest,” “signal strengthening,” “high-confidence alert”). This approach aligns directly with the dual-risk framework: it reduces secondary risks related to legitimacy loss, miscommunication, and trust erosion, while enabling earlier and more nuanced communication that mitigates primary risk (i.e., hazard impact). In addition to calibrating message timing and intensity, GCC also mitigates interpretive errors by reducing the risk of overconfidence in early or ambiguous signals. By presenting confidence bands rather than binary alerts, GCC helps prevent premature escalation and protects against the legitimacy losses associated with false alarms, especially in communities with past experiences of alert fatigue.

Multi-Source Verification

Operational MSV focuses on *how* detection systems cross-check and validate early-warning signals during the initial stages of hazard emergence. Because early signals extracted from social media often suffer from noise, demographic imbalance, linguistic ambiguity, or platform-specific biases, MSV strengthens detection pipelines by integrating information from diverse, independent, transparent, and heterogeneous data sources.

Operational examples include:

- cross-analyzing keyword surges with sensor readings
- validating geocoded posts with rainfall or hydrological data
- checking unexpected spikes against historical baselines
- using cross-platform confirmation (e.g., Twitter + local forums)
- evaluate and cross-validate prediction outputs across different models

In the dual-risk framework, MSV reduces secondary risks such as inaccurate classification, false positives, and representational bias while supporting faster detection of primary risks. MSV not only strengthens accuracy by cross-checking heterogeneous data sources but also reduces representational and equity-related risks. By incorporating multiple sources, including institutional datasets, community signals, environmental sensors, and geospatial information, MSV ensures that no single demographic group or platform artifact disproportionately shapes the alert output. While GCC and MSV provide essential operational mechanisms for early detection and communication, these design principles alone cannot guarantee equitable, accountable, or culturally legitimate alert outcomes. These broader concerns require institutional governance structures, addressed in the next section.

Adaptive Governance Architectures for Smart-Alert Systems

This section extends the framework from operational design into the institutional domain. Adaptive governance architectures (AGA) establish the oversight structures, decision protocols, and normative commitments that determine how smart-alert systems function in practice, ensuring that they are legitimate, accountable, and aligned with community expectations. AGA integrates institutional MSV, oversight, ethical safeguards, and the explicit management of value-laden choices such as acceptable false-positive rates and error burdens.

AGA defines the institutional actors responsible for validating alerts, escalating signals, approving public communication, and managing uncertainty. Even robust detection algorithms require human-centered review processes to determine when preliminary signals merit action. Institutions must therefore designate:

- validation authorities
- escalation thresholds
- interagency coordination pathways
- documentation standards
- transparency and audit requirements

These structures address the secondary risks of legitimacy, authority confusion, and inconsistent decision-making. AGA also supports public trust by creating clear, accountable lines of responsibility. Because thresholds inevitably encode normative decisions about what constitutes “acceptable risk,” GCC and MSV offer ways to surface and communicate these value-laden judgments rather than hiding them within technical parameters.

Normative Choices in Smart-Alert System Design and the Distribution of Uncertainty

Although AI-enabled alert systems are often framed as technical tools, their configuration depends on a series of explicit normative choices about what levels of error, delay, and uncertainty are socially acceptable. Decisions such as setting allowable false-positive or false-negative rates are not merely statistical thresholds; they reflect underlying judgments about whose safety is prioritized, who bears the burden of unnecessary alerts, and how institutions balance precaution against public fatigue.

For instance, a lower false-positive tolerance may reduce public annoyance but increases the likelihood that emerging risks go undetected, disproportionately affecting communities with less access to alternative information sources. Conversely, a higher tolerance for false positives may improve early detection but impose uneven costs on groups who cannot easily absorb disruptions caused by frequent alerts. Making these normative dimensions explicit is essential for designing equitable, transparent, and democratically legitimate smart-alert systems. These choices are not technical; they are ethical and political.

Examples include deciding:

- whether false positives are more harmful than false negatives
- whether alerts should prioritize vulnerable communities
- how cultural expectations shape acceptable levels of uncertainty
- how to avoid disproportionate burden on marginalized groups

Governance clarifies the normative choices embedded in early-warning systems by establishing criteria for equitable error distribution, culturally grounded review mechanisms, privacy safeguards, and limits on institutional overreach.

Privacy, Cultural Fit, and Sociotechnical Safeguards

Governance must ensure that alert systems adhere to societal expectations around privacy, data protection, cultural appropriateness, and community legitimacy. This includes:

- data minimization policies
- appropriate use of location data
- community consultation
- culturally appropriate messaging standards
- institutional transparency

These safeguards reduce secondary risks associated with surveillance, cultural mismatch, and trust erosion.

Multi-Source Verification as Governance Practice

Whereas the earlier section on Multi-Source Verification focused on MSV as a detection mechanism, here MSV serves as an institutional review process that determines who validates alerts, how validation decisions are justified, and how cross-agency verification prevents institutional bias or procedural opacity.
Governance-oriented MSV includes:

- cross-institutional validation committees
- human-in-the-loop review
- documentation of verification pathways
- accountability tracking

This version of MSV maps directly onto the governance layer of the figure and table, linking accuracy and equity concerns to institutional practices. Together, the operational mechanisms and the governance structures complete the system-level framework for AI-enabled smart-alert systems, positioning the paper to reflect more broadly on future research and practical implications in the next section.

Discussion and Future Directions

The preceding sections form the basis for a broader reflection on how AI-enabled warning systems reshape crisis communication, highlighting implications for research, emergency management practice, public trust, and long-term societal resilience. Our framework underscores that alert-system performance cannot be evaluated solely in accuracy terms; it must also be assessed in relation to the underlying normative choices that determine which errors are minimized, for whom, and at what social cost.

Implications for Strategic Communication

The integration of AI technologies into crisis communication challenges fundamental assumptions in strategic communication about message control, audience targeting, and communication effectiveness. The speed and scale of AI analytics create possibilities for real-time message optimization and audience analysis that exceed traditional communication planning capabilities while introducing new uncertainties about message interpretation and response. The shift from reactive to predictive communication fundamentally alters the temporal dynamics of strategic communication, extending it into speculative territory where communicators must address uncertain futures rather than known present conditions.

The democratization of information production through social media platforms combined with AI analytical capabilities creates new power dynamics in crisis communication that strategic communication theory has not adequately addressed. Traditional models assume institutional control over authoritative information sources, but AI systems can potentially identify and amplify non-institutional voices that provide valuable insights about developing situations. This distributed intelligence model challenges institutional gatekeeping roles while potentially improving information quality and response speed.

Resilience-Focused Approaches

The speculative framework advanced in this paper aligns with resilience-focused approaches to crisis communication. Research has shown that communicating mental health resources during COVID-19, particularly for vulnerable groups, can enhance community resilience (Akhther & Islam, 2022). Analysis of Historically Black Colleges and Universities' (HBCUs) website-based communication showed that mental health received minimal importance in pandemic response, with larger and advanced degree-granting institutions providing relatively greater mental health resources than smaller institutions.

Organizational memory, through after-action reports, plays a critical role in shaping resilience and renewal after crises. Research analyzing multiple reports created after the 2017 Las Vegas shooting found that reports from different professional fields commemorate crises in disparate ways that select and deflect memories of trauma, with these reports playing important emotional roles in making sense of organizational trauma (Rice & Bloomfield, 2022). Ultimately, AI-enabled systems must be embedded within collaborative emergency management structures that emphasize coordination, trust, and technological integration. Research investigating collaborative strategies to enhance emergency management identifies the importance of interagency cooperation, community engagement, technological integration, and policy development (Alkhouzaie et al., 2024).

Testable Implications

To translate the framework into evaluable claims, we derive testable propositions that link each design pattern—Graduated Confidence Communication (GCC), Multi-Source Verification (MSV), and adaptive governance architectures (AGA)—to measurable outcomes under real operational constraints. This step shifts the paper from theoretical contribution to empirical program design by specifying what success would look like (e.g., compliance, false-positive control, equitable coverage, legitimacy) and how to compare alternatives. The propositions below are therefore written to be fielded in drills, simulations, or quasi-experiments with agencies and platforms.

We propose four testable propositions:

- P1 (GCC efficacy). Confidence-matched alerts (vs. single-tone alerts) will yield higher compliance and lower alert fatigue under equal model accuracy.
- P2 (MSV accuracy). Multi-source verification will reduce false positives without lengthening time-to-alert beyond operational thresholds.
- P3 (Equity). Language-aware pipelines will increase detection/alert coverage in linguistic-minority areas relative to baseline models.
- P4 (AGA/trust). Transparent audit and role-clarity protocols will increase perceived legitimacy and willingness to comply with AI-mediated alerts.

Operationalization: P1 can be tested via A/B trials of alert templates in agency drills or controlled, IRB-approved online experiments measuring comprehension, intended compliance, and fatigue. P2 can use retrospective event logs to compare MSV vs. single-source pipelines on false-positive rate and time-to-alert. P3 requires stratified analyses by language/locale (coverage rate, precision/recall by subgroup). P4 can be evaluated with pre/post or difference-in-differences designs around policy rollouts (audit transparency, role charters), measuring perceived legitimacy and compliance intention.

Conclusion

The convergence of artificial intelligence, social media analytics, and crisis communication represents both unprecedented opportunity and substantial risk for emergency management systems. AI-enabled technologies offer the potential to detect disasters faster, communicate warnings more effectively, and tailor emergency responses to specific community needs and individual circumstances. The Thailand flood detection case study demonstrates that these capabilities are technically feasible and can provide valuable supplements to traditional emergency monitoring systems.

However, the implementation of AI-enabled crisis communication also introduces new categories of risk that require careful management and ongoing attention. The speed—accuracy dilemma inherent in emergency response becomes more complex when AI systems can process information faster than human verification systems can confirm its reliability. Privacy and surveillance concerns arise from the comprehensive data collection required for effective AI disaster detection. Algorithmic bias and equity issues may systematically exclude certain communities from AI-enabled early warning benefits.

The speculative framework presented here emphasizes the dual risk structure of AI-enabled crisis communication, recognizing that technologies designed to manage uncertainty may themselves become sources of uncertainty. Effective implementation requires explicit acknowledgment and management of both primary risks (the disasters we seek to detect and communicate about) and secondary risks (embedded within our technological communication systems). This dual risk structure creates complex interdependencies that traditional crisis communication models have not adequately addressed.

The framework's emphasis on graduated confidence communication, multi-source verification systems, and adaptive governance mechanisms provides practical approaches for managing these complexities while leveraging AI capabilities for improved emergency response. However, successful implementation requires sustained attention to ethical considerations, ongoing public education about AI system capabilities and limitations, and continuous adaptation to rapidly evolving technological capabilities.

Closing the loop, we argue that, framed as a dual-risk problem, smart-alert systems must show how GCC, MSV, and AGA jointly lower hazard harm while containing system-embedded risks. By naming the trade-offs, mapping mitigations to risk classes, and specifying testable propositions, we provide a path from speculative design to auditable, equitable practice in AI-enabled emergency messaging.

The stakes for getting this right are substantial. Climate change and technological advancement are creating new categories of risk that exceed the capabilities of traditional emergency management systems. AI-enabled crisis communication offers tools for addressing these challenges, but only if implemented thoughtfully with appropriate attention to both opportunities and risks. The framework presented here provides a foundation for that implementation, but its ultimate value will depend on continued research, development, and refinement through practical application.

Biographical Notes

Kulsawasd "Bo" Jitkajornwanich (Ph.D. in Computer Science, University of Texas at Arlington) is an Assistant Professor in the College of Media & Communication at Texas Tech University. His research focuses on computational communication, artificial intelligence, natural language processing (NLP), social media analytics, spatio-temporal database systems, and big spatial data, among other topics. His work has appeared in communication journals such as *Journal of Communication* (Oxford University Press), computer science journals such as *Applied Artificial Intelligence* (Taylor & Francis), and interdisciplinary journals such as *JMIR Formative Research* (JMIR Publications). His work has also been featured in key research handbooks, such as the *Handbook of Innovations in Strategic Communication*, and the *Routledge Handbook of Employee Communication and Organizational Processes*. He is the 2019 recipient of the National Dissertation Award in the "Information Technology and Communication Arts" category from the National Research Council of Thailand.

Kerk F. Kee (Ph.D. in Communication Studies, University of Texas at Austin), is the Virginia & Choc Hutcheson Professor in Mass Communication in the College of Media & Communication at Texas Tech University. His scholarship centers on information diffusion and technology adoption in organizational, health, science, environmental, risk, and crisis communication contexts. He has published research in communication journals such as *New Media & Society*, and *Communication Research*; computer science journals including *ACM Computer Surveys*, and *IEEE Transactions on Human-Machine Systems*; as well as interdisciplinary journals like *AI & Society*, and *International Journal of Information*

Management. He received a prestigious CAREER award from the US National Science Foundation's Computer & Information Science & Engineering (CISE) Directorate in 2015.

References

Akhther, N., & Islam, K. (2022). Communicating mental health coping resources among college students of color: A resilience approach to COVID-19 response. *Journal of International Crisis and Risk Communication Research, 5*(2). https://doi.org/10.63278/jicrcr.v5i2.122

Alam, F., Ofli, F., & Imran, M. (2018). CrisisMMD: Multimodal Twitter datasets from natural disasters. *Proceedings of the International AAAI Conference on Web and Social Media, 12*(1), 465–473. https://doi.org/10.48550/arXiv.1805.00713

Alexander, D. E. (2014). Social media in disaster risk reduction and crisis management. *Science and Engineering Ethics, 20*(3), 717–733. https://doi.org/10.1007/s11948-013-9502-z

Alkhouzaie, H., Mutawam, M., Dallak, H., Alahmari, S., Alsawat, A., Ogdi, A., & Ogdi, Q. (2024). Strengthening emergency management: Collaborative strategies for effective crisis response. *Journal of International Crisis and Risk Communication Research, 7*(1). https://doi.org/10.63278/jicrcr.v7i1.89

Ansah, P. O. (2022). COVID-19 dialogue on Facebook: Crisis communication relationship between Ghanaian authorities and citizens. *Journal of International Crisis and Risk Communication Research, 5*(1). https://doi.org/10.63278/jicrcr.v5i1.101

Beck, U. (1992). *Risk society: Towards a new modernity*. Sage Publications.

Beck, U. (2009). *World at risk*. Polity Press.

Bozdag, A. A. (2023). AIsmosis and the pas de deux of human-AI interaction: Exploring the communicative dance between society and artificial intelligence. *Online Journal of Communication and Media Technologies, 13*(4). https://doi.org/10.30935/ojcmt/13414

Coombs, W. T. (2014). *Ongoing crisis communication: Planning, managing, and responding*. Sage Publications.

Diers-Lawson, A., & Meißner, F. (2021). Editor's essay: Moving beyond Western corporate perspectives: On the need to increase the diversity of risk and crisis communication research. *Journal of International Crisis and Risk Communication Research, 4*(1). https://doi.org/10.63278/jicrcr.v4i1.31

Fire Safety Research Institute. (2024, April 17). *Phase One: Lahaina Fire Comprehensive Timeline Report*. UL Research Institutes & State of Hawai'i Office of the Attorney General. https://fsri.org/resource/phase-one-lahaina-fire-comprehensive-timeline-report

Gu, M., Guo, H., Zhuang, J., Du, Y., & Qian, L. (2022). Social media user behavior and emotions during crisis events. *International Journal of Environmental Research and Public Health, 19*(9), 5197. https://doi.org/10.3390/ijerph19095197

Jitkajornwanich, K., Kongthong, C., Khongsoontornjaroen, N., Kaiyasuan, J., Lawawirojwong, S., Srestasathiern, P., Srisonphan, S., & Vateekul, P. (2018). Utilizing Twitter data for early flood warning in Thailand. *2018 IEEE International Conference on Big Data*, 5165–5169. https://doi.org/10.1109/bigdata.2018.8621961

Johansson, S. (2024). The anxiety threshold: Exploring the relationship between discrete emotions and information-seeking repertoires during a societal crisis. *Journal of International Crisis and Risk Communication Research, 7*(1). https://doi.org/10.63278/jicrcr.v7i1.135

Jong, W., & Brataas, K. (2021). Victims as stakeholders: Insights from the intersection of psychosocial, ethical, and crisis communication paths. *Journal of International Crisis and Risk Communication Research, 4*(1). https://doi.org/10.63278/jicrcr.v4i1.28

Klinga, M., & Lundgren, M. (2024). Making sense of disinformation in the Swedish heterogeneous society: Understandings, experiences, and vulnerabilities. *Journal of International Crisis and Risk Communication Research, 7*(1). https://doi.org/10.63278/jicrcr.v7i1.138

Kryvasheyeu, Y., Chen, H., Obradovich, N., Moro, E., Van Hentenryck, P., Fowler, J., & Cebrian, M. (2016). Rapid assessment of disaster damage using social media activity. *Science Advances, 2*(3), e1500779. https://doi.org/10.1126/sciadv.1500779

LaCour, M., Serra, M. J., Duvall, M., & Hislop, C. (2023). Getting lost in the “realm of possibility”: Common phrases used to communicate rare events have substantially different effects on decision-making. *Journal of International Crisis and Risk Communication Research, 6*(2). https://doi.org/10.63278/jicrcr.v6i2.132

Lee, Y.-I., Lu, X., Voges, T., & Jin, Y. (2023). Fending off unverified accusation with narratives: The role of primary and secondary narratives in organization’s response effectiveness in an ongoing crisis. *Journal of International Crisis and Risk Communication Research, 6*(1). https://doi.org/10.63278/jicrcr.v6i1.126

Madden, S., Eng, N., & Myrick, J. G. (2023). Emotional responses to wireless emergency alerts for COVID-19 and predictors of public health compliance. *Journal of International Crisis and Risk Communication Research, 6*(1). https://doi.org/10.63278/jicrcr.v6i1.128

Maui Emergency Management Agency. (2025). *Maui Wildfires 2023 After-Action Report*. County of Maui. https://www.mauicounty.gov/DocumentCenter/View/151355/MEMA-2023-Wildfire-After-Action-Report

Meißner, F., & Diers-Lawson, A. (2022). Editorial essay: Innovation in risk and crisis communication: Toward new topics, theories, and methods. *Journal of International Crisis and Risk Communication Research, 5*(2). https://doi.org/10.63278/jicrcr.v5i2.118

Miller, A. N., Collins, C., Neuberger, L., Todd, A., Sellnow, T. L., & Boutemen, L. (2021). Being first, being right, and being credible since 2002: A systematic review of crisis and emergency risk communication (CERC) research. *Journal of International Crisis and Risk Communication Research, 4*(1). https://doi.org/10.63278/jicrcr.v4i1.26

Mirbabaie, M., Bunker, D., Stieglitz, S., Marx, J., & Ehnis, C. (2020). Social media in times of crisis: Learning from Hurricane Harvey for the coronavirus disease 2019 pandemic response. *Journal of Information Technology, 35*(3), 195–213. https://doi.org/10.1177/0268396220929258

Page, T. G., & Clementson, D. E. (2023). The power of style: Sincerity's influence on reputation. *Journal of International Crisis and Risk Communication Research, 6*(2). https://doi.org/10.63278/jicrcr.v6i2.131

Prasad, M. (2022). Templated crisis communication for people with disabilities, access and functional needs. *Journal of International Crisis and Risk Communication Research, 5*(2). https://doi.org/10.63278/jicrcr.v5i2.123

Reuter, C., & Kaufhold, M. A. (2018). Fifteen years of social media in emergencies: A retrospective review and future directions for crisis informatics. *Journal of Contingencies and Crisis Management, 26*(1), 41–57. https://doi.org/10.1111/1468-5973.12196

Reuter, C., Hughes, A. L., & Kaufhold, M.-A. (2023). Social media in crises: A systematic literature review and future agenda. *Computers in Human Behavior, 140*, 107568.

Rice, R. M., & Bloomfield, E. F. (2022). Commemorating disorder in after-action reports: Rhetorics of organizational trauma after the Las Vegas shooting. *Journal of International Crisis and Risk Communication Research, 5*(1). https://doi.org/10.63278/jicrcr.v5i1.102

Rodríguez-Díaz, C. E. (2018). Maria in Puerto Rico: Natural disaster in a colonial archipelago. *American Journal of Public Health, 108*(1), 30–32. https://doi.org/10.2105/AJPH.2017.304198

Rogers, D., & Tsirkunov, V. (2011). *Costs and benefits of early warning systems*. World Bank Publications.

Schwarz, A., Sellnow, D. D., Sellnow, T. D., & Taylor, L. E. (2024). Instructional risk and crisis communication at higher education institutions during COVID-19: Insights from practitioners in the Global South and North. *Journal of International Crisis and Risk Communication Research, 7*(1). https://doi.org/10.63278/jicrcr.v7i1.134

Starbird, K., Maddock, J., Orand, M., Achterman, P., & Mason, R. M. (2014). Rumors, false flags, and digital vigilantes: Misinformation on Twitter after the 2013 Boston Marathon bombing. *iConference 2014 Proceedings*, 654–662. https://doi.org/10.9776/14308

Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media + Society, 6*(1). https://doi.org/10.1177/2056305120903408

Vogler, D., & Meißner, F. (2024). The mediated construction of crises—Combining automated and qualitative content analysis to investigate the use of crisis labels in headlines of Swiss news media between 1998 and 2020. *Journal of International Crisis and Risk Communication Research, 7*(1). https://doi.org/10.63278/jicrcr.v7i1.136

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

Wang, Y., & Chen, J. (2022). What motivates information seeking and sharing during a public health crisis? A combined perspective from the uses and gratifications theory and the social-mediated crisis communication model. *Journal of International Crisis and Risk Communication Research, 5*(2). https://doi.org/10.63278/jicrcr.v5i2.120

Wu, Y., Cong, Y., Zhang, H., Wang, H., & Hu, P. (2024, September 5). *Emotional Contagion and Public Risk Perception in Crisis Events on Social Media: Insights from the Chinese Context during COVID-19*. https://doi.org/10.31234/osf.io/s3utx