

Crisis Communication and Cross-Border Legal Accountability: Protecting and Restoring Brand Image in the Age of Digital Misinformation

Md Mehedi Hasan^{1*}, Md Asif Ullah², Ritu Moni³

¹ Department of Advertising and Public Relations, Russian State University for the Humanities,
Moscow, Russia

² Department of International Law, Higher School of Economics, Moscow, Russia

³ Department of Law, Stamford University, Dhaka, Bangladesh

¹ORCID: 0009-0001-4237-6255

*Corresponding Author

DOI: <https://doi.org/10.47772/IJRISS.2026.100900509>

Received: 26 September 2026; Accepted: 03 October 2026; Published: 15 October 2026

ABSTRACT

Digital misinformation has altered the conditions under which organizations identify, communicate, and recover from reputational crises. False claims can circulate before an organization has established the underlying facts, while manipulated audio, video, and images can make false attribution appear credible. This article examines the communication and legal problems that arise when such narratives cross national borders. It combines crisis communication theory with an analytical review of literature on misinformation, deepfakes, social media, correction, corporate reputation, and digital influence, alongside a conceptual examination of cross-border jurisdiction and platform regulation. The analysis is qualitative and does not claim statistical generalization. Instead, it synthesizes published research and illustrative cases to develop an operational framework consisting of four connected stages: Detect, Assess, Respond, and Recover. The framework treats legal review as an integrated part of crisis management rather than as a step that begins only after public communication has occurred. The analysis indicates that monitoring technology can improve the speed with which emerging narratives are identified, but high-risk decisions still require human verification, contextual judgment, and a documented evidentiary basis. It also shows that cross-border crises cannot be managed through a single communication rule because jurisdiction, applicable law, platform obligations, and stakeholder expectations may differ across countries. The article contributes a practical link between communication theory and legal analysis by specifying where legal questions enter the crisis process and by identifying areas that require future empirical testing.

Keywords: crisis communication; brand image; corporate reputation; misinformation; deepfakes; social media; artificial intelligence; stakeholder trust; cross-border law; crisis response.

INTRODUCTION

The speed of digital communication has changed the practical problem of reputation management. A claim about an organization can move from a small online discussion to a widely visible narrative without passing through a formal editorial or institutional verification process. Research on online misinformation has shown that false news can spread rapidly and that novelty and emotional response can contribute to sharing [1]. Other work shows that exposure to misinformation can be concentrated within particular networks rather than distributed evenly across an entire population [2]. These findings do not, by themselves, establish how corporate crises unfold, but they describe an information environment in which corporate reputation is increasingly contested.

Manipulated media adds a distinct verification problem. Synthetic audio, video, and images can attribute words or actions to a person who never made the statement or performed the act. The resulting risk is not limited to the false content itself. It also concerns the credibility of digital evidence and the difficulty of persuading audiences that an apparently authentic recording is not genuine [3]. Corporate reputation research likewise treats crisis communication as an important part of how stakeholders form and revise judgments about an organization [4].

Correction is difficult because audiences do not assess every message through detailed source checking. Research on the illusory truth effect indicates that repetition can increase perceived familiarity and, under some conditions, perceived truth [5], [6]. Reviews of misinformation research identify familiarity, limited attention, and reasoning processes as relevant factors in how false information is evaluated [7]. For crisis communication, the implication is that publishing a correction is only one part of the problem. The organization must also decide how to present verified information without unnecessarily reinforcing the false narrative it is trying to correct.

Established crisis communication theories provide a useful starting point. Situational Crisis Communication Theory connects crisis characteristics and perceived responsibility with response strategies [8], [9], while Image Repair Theory focuses on rhetorical choices made when an organization's image is threatened [10]. Digital crises, however, introduce conditions that were less central to the original development of these frameworks, including algorithmic distribution, user-generated content, synthetic media, and fragmented publics. Recent crisis-communication research continues to develop these theoretical foundations in relation to digital media and changing communication environments [11].

Social media also changes who participates in a crisis narrative. Customers, employees, journalists, investors, activists, influencers, and loosely organized online communities may all contribute information or interpretation. Research on social-mediated crisis communication indicates that platform characteristics, network structures, and public participation affect how crisis information circulates [12], [13]. A crisis team therefore has to monitor several information environments at once and distinguish between the existence of online attention and the reliability of the underlying claim.

Timing is similarly important. Research on proactive disclosure, often described as “stealing thunder,” has examined whether organizations can protect credibility by disclosing negative information before another actor does so [14]-[16]. The evidence does not support a universal rule that earlier disclosure is always preferable. Rather, timing interacts with the quality of information available, subsequent organizational action, transparency, and the nature of the crisis [14]-[16].

This article develops these observations into a practical framework for digital misinformation crises that have a cross-border legal dimension. It asks four questions: (1) how does digital misinformation alter the risk profile of brand crises; (2) what communication capabilities are required for timely and credible response; (3) how can technological tools be combined with human verification and stakeholder communication; and (4) how do jurisdiction, applicable law, and platform regulation affect crisis decisions when the information and affected stakeholders cross national borders? The central contribution is not a new statistical estimate, but an analytical connection between crisis communication processes and the legal constraints that operate alongside them.

THEORETICAL AND CONCEPTUAL BACKGROUND

Crisis communication can be treated as a process of managing information, uncertainty, stakeholder relationships, and reputational consequences during a threatening event. No single theory provides a complete explanation for every crisis. Instead, several perspectives are useful when their respective limits are made explicit.

Situational Crisis Communication Theory (SCCT) links crisis type, responsibility attribution, and response strategy [8], [9]. Image Repair Theory addresses the rhetorical strategies available when an organization's image is threatened [10]. These theories help explain why the same message may be appropriate in one crisis and inappropriate in another. Digital misinformation requires an additional operational layer because organizations must establish what is true before they can determine how responsibility should be communicated.

Research on communication channels shows that the medium used for a crisis response can influence audience perceptions and secondary reactions [17], while meta-analytic work suggests that social and traditional media can produce different outcomes depending on context [18]. Social media should therefore not be treated simply as another publicity outlet. It is also a distribution environment in which users can reinterpret, reproduce, and challenge organizational statements [19].

Misinformation research adds a behavioral dimension. Repeated exposure can make information feel familiar, and familiarity can influence judgments of truth [5], [20], [21]. At the same time, systematic reviews identify methodological limitations in the literature, including reliance on particular samples and experimental designs [22]. Correction research likewise shows that corrections can reduce belief in false information, but that the quality and accuracy of the correction matter [23], [24]. These qualifications are important because they prevent the communication framework from treating psychological findings as universal rules.

Influencers create another layer of complexity. Their participation can increase the reach of crisis information, but audiences may interpret a brand-linked influencer as commercially motivated. Research has identified both risks and conditions under which similarity, identification, and perceived authenticity affect responses [25], [26]. For that reason, influencer participation should be treated as a stakeholder-specific option rather than as an automatic substitute for an organization's own factual communication.

The conceptual model developed here therefore links five elements: the digital threat, detection and verification, communication response, audience and stakeholder conditions, and legal exposure. The intended outcome is not simply removal of a false post. It is a more complete process of restoring credible information, managing stakeholder relationships, documenting decisions, and learning from the event.

2.1 Legal and Regulatory Dimensions of Digital Crisis Communication

Communication decisions in a cross-border misinformation crisis can create legal consequences at the same time that they create reputational consequences. Communication teams are concerned with what should be said and how quickly it should be communicated. Legal analysis asks additional questions: where can a dispute be brought, which law may apply, what evidence supports a statement, and what legal obligations govern the platform through which the content is distributed? These questions become harder when the same content is accessible in several countries.

Private international law is relevant because jurisdiction and applicable-law rules may determine where claims relating to online defamation or personality rights can be pursued and which substantive rules a court will apply. Scholarship on cross-border personality-rights disputes has highlighted the difficulty of adapting territorial connecting factors to online content that can be accessed in multiple jurisdictions [41]. Research on social-media defamation similarly identifies unresolved conflict-of-law problems created by borderless publication [42]. The practical point for crisis management is that a communication statement should not be assessed only against the law of the organization's home country.

Platform regulation creates a further layer. The European Union's Digital Services Act establishes obligations for online intermediaries and, in particular, additional duties for very large online platforms in relation to systemic risks, including risks associated with the dissemination of disinformation [43]. At the same time, the regulatory framework does not create a single substantive law of defamation or personality rights across Europe. Research on the evolving European platform-liability framework therefore needs to be read alongside national rules and private international law [44].

These legal considerations do not replace crisis communication theory. They qualify the range of available communication choices. SCCT can assist with responsibility assessment, while Image Repair Theory can assist with message strategy. Legal review then addresses jurisdiction, evidence, applicable standards, and exposure in the jurisdictions relevant to the crisis. The framework proposed in this article consequently embeds legal review within each phase rather than treating law as a post-crisis litigation issue.

RESEARCH METHODOLOGY

This study uses an analytical qualitative design. It does not report a probability sample, controlled experiment, or independently collected quantitative dataset. The purpose is to synthesize established research and illustrative case material and to develop a practical framework that connects crisis communication with cross-border legal considerations.

The literature review covers crisis communication, corporate reputation, misinformation, deepfakes, social media, correction, digital influence, and crisis timing. The publication periods of the cited literature are summarized in Figure 1. The revised manuscript uses the cited literature to support specific propositions rather than presenting the literature as evidence for claims that it does not directly test.

Figures 1 and 2 are descriptive summaries of the reference base used in this manuscript; they are included to document the evidence base and should not be interpreted as empirical findings.

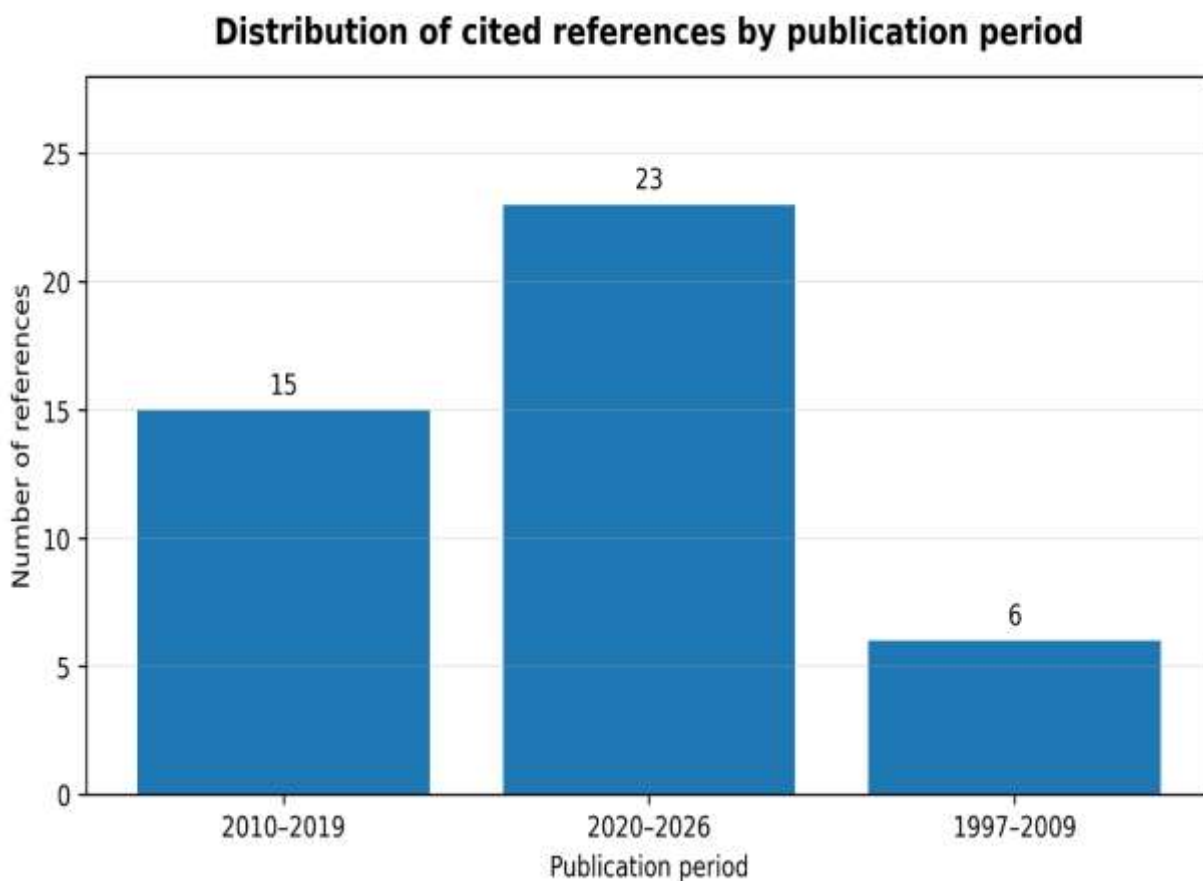


Figure 1. Distribution of the 44 cited references by publication period. The figure describes this manuscript's reference base and is not an empirical result.

Case-based analysis is used illustratively. The cases discussed in the source manuscript include PepsiCo, United Airlines, Starbucks, and examples involving manipulated media. They are not treated as a representative sample, and no causal effect is attributed to a particular communication strategy on the basis of these cases alone. Their purpose is to show how timing, narrative amplification, stakeholder reaction, and response coordination can interact during reputational crises.

The analysis also retains the source manuscript's discussion of social listening, sentiment analysis, fact checking, and communication-coordination tools. These are treated as functional categories rather than as evidence that a particular software product is superior. The analytical comparison focuses on detection and verification, timing, message quality, stakeholder coordination, legal exposure, and recovery.

A key methodological decision is to separate synthesis from empirical measurement. The composition of the reference base is shown in Figure 2. The illustrative percentages and numerical claims that appeared in the earlier version are not presented here as statistical findings because the underlying manuscript does not document an original dataset capable of supporting such inference. Future empirical work can test the framework through experiments, surveys, social-media data, or longitudinal designs.

Composition of the manuscript's reference base

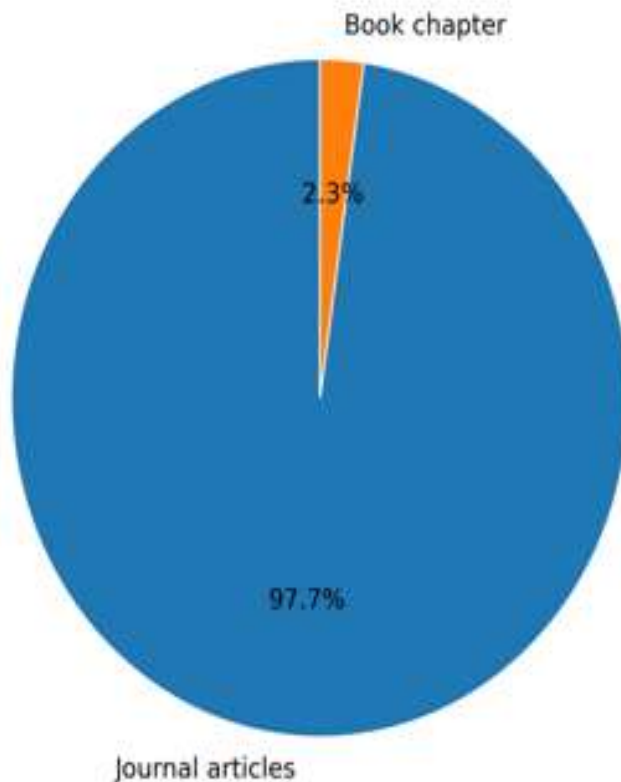


Figure 2. Composition of the manuscript's reference base by source type. The chart describes the cited sources and does not represent the composition of empirical observations.

RESULTS AND DISCUSSION

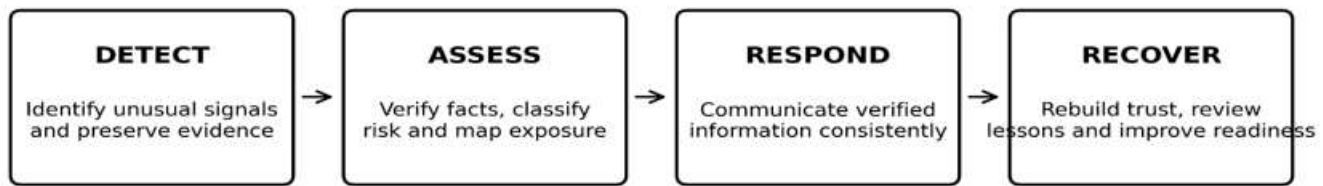
The synthesis indicates that digital misinformation compresses the time available for organizational decision-making. A false or misleading claim can become visible to a large audience before an organization has completed verification. Evidence on misinformation diffusion and repetition helps explain why the delay matters [1], [5], [6]. The analytical implication is that crisis readiness should be measured partly by the organization's ability to move from detection to verification without sacrificing accuracy.

Detection should therefore be understood as an early-warning function rather than as a conclusion that a crisis has already been established. Increases in brand mentions, repeated customer questions, unusual concentrations of negative discussion, or the appearance of an apparently authentic executive recording may justify escalation. Each signal still requires human assessment. The distinction matters because automated systems can identify anomalies but cannot reliably determine the legal or reputational significance of every anomaly.

Attribution is another point at which digital crises differ from conventional communication problems. A crisis narrative may contain a real event, a misleading interpretation of a real event, altered material, or a wholly fabricated claim. Before selecting a response strategy, the organization must separate the underlying event from the narrative built around it. This is consistent with the logic of SCCT, in which crisis type and responsibility attribution influence response choices [8], [9].

4.1 Four-Phase Response Framework: Detect, Assess, Respond, Recover

The analysis supports a four-phase operational model: Detect, Assess, Respond, and Recover. Figure 3 presents the framework, while Table 1 summarizes the main questions, actions, and outputs for each phase. The model is deliberately practical. It does not replace SCCT or Image Repair Theory; instead, it specifies where those theories can be applied during an actual digital crisis and where legal review should enter the decision process.



Legal review and human verification operate across all four phases.

Figure 3. Four-phase operational framework for digital misinformation crises. The phases run from Detect to Recover, and legal review and human verification operate across all four.

Table 1. Four-phase operational framework for digital misinformation crises. Each phase is defined by a core question, main actions, and a key output.

Phase	Core question	Main actions	Key output
Detect	What is changing?	Monitor narratives, media, stakeholder reports, and unusual activity; preserve relevant evidence.	Verified alert
Assess	How serious is it?	Classify the crisis, identify stakeholders, verify facts, and map jurisdictional and operational exposure.	Severity and response plan
Respond	What should stakeholders hear now?	Acknowledge the situation, provide verified guidance, correct material inaccuracies, and coordinate internal and external messages.	Consistent public and internal communication
Recover	What must be rebuilt?	Re-engage stakeholders, assess reputational effects, document lessons, and implement corrective action.	Trust repair and improved readiness

The first analytical point is that detection and verification should not be collapsed into a single activity. Monitoring systems can identify unusual patterns, but a signal becomes actionable only after a human reviewer establishes what is known, what is uncertain, and what evidence remains to be collected.

The second point is that legal review should begin during assessment. Once the organization knows what the claim concerns and where it is circulating, counsel can help identify relevant jurisdictions, potential claims, evidence requirements, and platform procedures. This reduces the risk that a hurried correction creates a new legal problem.

The third point is that response quality depends on consistency rather than message volume. A company may need different messages for employees, customers, regulators, journalists, investors, and online communities, but the factual foundation should remain the same. A single verified record can support audience-specific communication without creating contradictory versions of events.

Finally, recovery should not be treated as the moment when public attention declines. A crisis can leave unresolved questions about trust, internal governance, and stakeholder relationships. Post-crisis review should therefore record what was known at each decision point, which assumptions proved wrong, how the narrative changed, and which controls should be revised.

4.2 Internal Communication and Reputation Management

Internal communication is part of the reputation process because employees and managers can become information sources during a crisis. When internal audiences receive no reliable information, informal channels may fill the gap. Inconsistent internal messages can then become part of the external narrative.

A practical internal cascade should begin with the crisis-management team and senior leadership and then provide role-appropriate information to managers and employees. The factual record should remain consistent across levels. A dated internal briefing or other single source of truth can help prevent contradictions. The objective is not continuous messaging; it is to reduce uncertainty and ensure that employees know what has been verified and what remains uncertain.

4.3 Digital Tools and Human Verification

The source study identifies four broad tool functions: social listening, AI-assisted monitoring, fact checking, and coordination. Table 2 summarizes the role of these tools and the human controls required for high-risk decisions. These functions should remain distinct. Social listening identifies patterns, automated systems can help prioritize large volumes of material, fact checking evaluates claims against evidence, and coordination systems assign responsibility and maintain an agreed record.

Table 2. Digital tools and the human controls required for high-risk crisis decisions. The table pairs each tool function with its contribution, the human control it requires, and a governance question.

Tool function	What it contributes	Human control	Governance question
Social listening	Identifies unusual volume, topics and emerging narratives.	Interpret context and significance.	What threshold should trigger escalation?
AI-assisted monitoring	Prioritizes large volumes of content and detects patterns.	Validate high-risk classifications and possible false positives.	How are errors and bias handled?
Fact checking	Tests claims, images and videos against available evidence.	Assess source quality and uncertainty.	What evidence standard is required before publication?
Coordination system	Assigns tasks and keeps the response record consistent.	Approve sensitive actions and factual updates.	Who owns the final factual record?

Technology is useful for scale, but it should not become the final authority for high-risk factual claims. Automated systems can generate false positives, miss context, and misinterpret sarcasm or emerging narratives. Human review is particularly important before an organization publishes a statement that could affect reputation, legal exposure, or the rights of another person. Research on automated misinformation correction likewise supports treating correction as a socio-technical process rather than a purely technical task [23].

4.4 Repetition, Emotion, and Audience Trust

Audience response is not uniform. Stakeholders encounter crisis information through different channels and bring different levels of prior trust, knowledge, and involvement. The literature on misinformation indicates that familiarity and repeated exposure can influence judgments of truth [5], [6], [20], while broader reviews caution against treating these effects as context-free [22].

A correction should therefore lead with verified information and provide an evidence path for readers who require more detail. Repeating a false allegation unnecessarily may give it additional visibility. At the same time, a purely technical correction may fail to address the uncertainty or concern experienced by affected stakeholders. A credible response should combine factual precision with an acknowledgment of legitimate stakeholder concerns.

Correction research also shows why accuracy matters on both sides of the exchange. Social corrections can reduce the perceived accuracy of false content, but inaccurate corrections may also reduce confidence in true information [24]. The practical rule that follows from this evidence is straightforward: organizations should publish only what they can substantiate and should state uncertainty openly where the evidence is incomplete.

4.5 Influencers and Decentralized Communication

Influencers and other high-visibility users may become part of a crisis even when the organization did not plan for their involvement. They can extend accurate information, but their participation can also create questions about commercial motives and authenticity [25], [26].

The organization should distinguish among independent information actors, paid brand partners, and subject-matter experts. These roles have different credibility structures and disclosure expectations. The organization's own channels should remain the primary source for facts about the organization. External voices can support reach and dialogue when their role is transparent, but they should not be used to conceal responsibility or substitute for evidence.

4.6 Case-Based Synthesis

The cases in the source manuscript illustrate different routes into reputational crisis. Table 3 compares the illustrative cases and the communication mechanisms highlighted by the analysis. The PepsiCo example concerns public interpretation of a communication artifact; the United Airlines case demonstrates how a real incident can be intensified by rapid online circulation and perceptions of the early response; and the Starbucks example concerns rumor and stakeholder trust. These cases are illustrative, not controlled comparisons.

Table 3. Illustrative cases and the mechanisms used in the analytical synthesis. The cases are illustrative and are not a controlled comparison.

Illustrative case	Crisis feature	Communication issue highlighted	Use in this study
PepsiCo	Public interpretation of a communication artifact.	How an intended message can be reinterpreted and amplified online.	Illustrates narrative formation and reputational pressure.
United Airlines	A real incident amplified through rapid online circulation.	Timing, perceived adequacy of the initial response and stakeholder reaction.	Illustrates the compressed digital crisis timeline.
Starbucks	Rumor and stakeholder-trust dynamics.	Need to distinguish circulating claims from verified organizational facts.	Illustrates the importance of verification and trust.

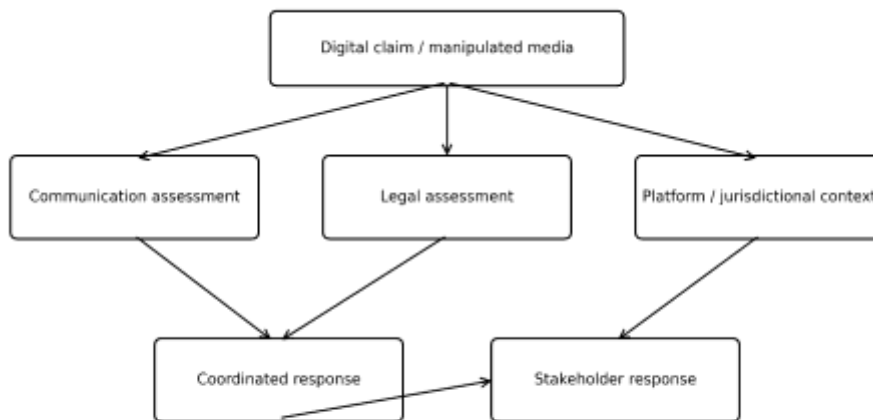
Their value for the present framework lies in the recurring mechanisms rather than in the identity of the companies. Across the cases, the relevant questions concern what happened, how quickly the narrative spread, when the organization responded, whether the response addressed the concern raised by stakeholders, and what remained unresolved afterward. The literature on crisis timing, channel choice, responsibility, and proactive disclosure supports this process-oriented interpretation [14]-[18], [27], [28].

The resulting crisis lifecycle can be described as trigger, amplification, public reaction, organizational response, and resolution or escalation. Early stages require detection and verification. The middle stage requires coordinated communication and stakeholder management. Recovery requires evidence-based corrective action and organizational learning.

4.7 Legal and Cross-Border Regulatory Considerations

Each stage of the framework has a legal dimension. Figure 4 shows how communication and legal decision points interact across the crisis process, while Table 4 maps the principal legal questions onto each stage. During

detection, the organization should preserve relevant material and identify whether the content may implicate rights such as reputation, privacy, personality, or intellectual property. During assessment, the organization should map where the content was created, hosted, and viewed and where relevant stakeholders and operations are located. These facts can affect the jurisdictional analysis of a dispute [41], [42].



The model links communication choices with verification, jurisdiction, applicable law, and platform context.

Figure 4. Communication and legal decision points in a cross-border crisis. A digital claim or manipulated media item prompts communication, legal, and platform or jurisdictional assessments, which feed a coordinated response and the stakeholder response.

Table 4. Legal issues integrated into the crisis-response process. Each stage links a communication question to a legal question and the practical record to be kept.

Crisis stage	Communication question	Legal question	Practical record
Detect	What information is circulating?	Could the content implicate reputation, personality, privacy or other rights?	Preserved copies, links and timestamps
Assess	What is verified and who is affected?	Which jurisdictions and legal interests may be relevant?	Fact sheet and jurisdiction map
Respond	What should be communicated now?	Is the statement supported and appropriate across relevant jurisdictions?	Approved message and evidence trail
Recover	What remains unresolved?	Are there continuing claims, regulatory issues or corrective duties?	Post-crisis review and legal record

During response, legal review should examine the evidentiary basis for factual assertions and the consequences of publishing an apology, denial, accusation, or correction in multiple jurisdictions. The point is not that every statement requires lengthy legal clearance. Rather, high-risk statements should be assessed against the jurisdictions and legal interests actually implicated by the crisis.

Platform regulation can affect the practical options available to the organization. The Digital Services Act establishes duties for covered platforms, including risk-management obligations for very large online platforms, but it does not harmonize all substantive national rules governing defamation, personality rights, or unfair commercial practices [43], [44]. Platform escalation should therefore be treated as one part of a broader response rather than as a substitute for legal analysis.

PRACTICAL IMPLICATIONS

1. Establish a standing crisis team that includes communication, legal, operations, customer support, technology, and senior decision-making functions.

2. Set explicit escalation thresholds that combine social listening, media monitoring, customer complaints, and internal reports.
3. Maintain a dated, evidence-based crisis fact sheet that records the source and status of important facts.
4. Prepare response templates for acknowledgment, guidance, correction, and updates, but require human approval before publication.
5. Use AI and automated analytics for scale and prioritization, not as the final authority for high-risk factual claims.
6. Segment stakeholders because employees, customers, regulators, investors, journalists, and online communities may require different information and channels.
7. Consider proactive disclosure when the facts are sufficiently established and when early communication is likely to reduce uncertainty; evaluate timing together with responsibility, legal exposure, and follow-up action.
8. Plan recovery before the immediate crisis ends by incorporating stakeholder listening, reputation assessment, corrective action, and organizational learning.
9. Include international legal counsel in crisis planning so that jurisdiction, applicable law, evidence, and platform-regulation issues can be assessed before publication when the situation warrants it.
10. Document major decisions and post-crisis lessons so that monitoring thresholds, verification procedures, and governance rules can be improved.

LIMITATIONS AND FUTURE RESEARCH

The study has important limitations. First, it is an analytical qualitative synthesis rather than a controlled empirical test. The source manuscript does not provide a probability sample or a reproducible original social-media dataset. Second, the cases are illustrative and cannot establish the average effect of a particular crisis response strategy across industries. Third, digital platforms and AI systems change rapidly, so the proposed framework requires periodic empirical validation. Fourth, the legal discussion is conceptual and doctrinal rather than a comprehensive comparison of every national legal system that could affect a multinational organization.

These limitations define a clear research agenda. Experiments could manipulate crisis type, response timing, transparency, and verification cues. Longitudinal social-media studies could examine the development of false narratives and corrections over time. Surveys and structural equation modeling could test relationships among perceived response speed, transparency, trust, brand credibility, and behavioral intentions. Comparative research could also examine whether institutional trust, media systems, legal traditions, and platform use alter the relationship between crisis communication and reputation.

CONCLUSION

Digital misinformation has changed the practical conditions of crisis communication. Organizations must now manage not only the content of a public response but also the speed of narrative formation, the reliability of digital evidence, the participation of decentralized actors, and the legal consequences of communicating across borders.

The Detect, Assess, Respond, Recover model offers an operational structure for these conditions. Detection identifies emerging signals; assessment separates verified facts from claims and maps stakeholder and legal exposure; response coordinates accurate information across relevant channels; and recovery addresses trust, corrective action, and institutional learning. The framework is intended as a practical synthesis of established crisis communication theory rather than as a replacement for empirical testing.

The analysis also places a clear limit on technological solutions. AI and automated monitoring can increase the amount of information that a crisis team can process, but they cannot remove the need for human verification

and accountability. Cross-border legal questions similarly cannot be reduced to a single platform rule because jurisdiction, applicable law, and substantive rights vary across legal systems. The practical implication is that communication and legal functions should be connected before a crisis occurs.

For organizations concerned with brand and reputation, the central issue is therefore not simply how quickly a statement can be published. It is whether the organization can move quickly while preserving factual accuracy, stakeholder clarity, documented evidence, and legal awareness. That combination provides a more defensible basis for managing misinformation and supporting reputation recovery.

Author Contributions

Conceptualization, M.M.H.; literature review and communication-theory methodology, M.M.H.; legal and regulatory analysis (international and private international law), M.A.U. and R.M.; case-based synthesis, M.M.H. and R.M.; validation, M.M.H. and M.A.U.; writing, original draft preparation, M.M.H.; writing, review and editing, M.M.H. and M.A.U.; supervision, M.M.H. All authors have read and agreed to the submitted version of the manuscript.

Funding

This research received no external funding.

Institutional Review Board Statement

Not applicable. This study did not involve human or animal subjects, primary data collection, or any procedure requiring ethical approval; it is based on published literature, publicly available case material, and legal-regulatory sources.

Informed Consent Statement

Not applicable, as this study did not involve human subjects.

Data Availability Statement

No new data were created or analyzed in this study. Data sharing is not applicable to this article. The literature, case material, and legal-regulatory sources discussed are publicly available and cited in the References section.

Conflicts of Interest

The authors declare no conflict of interest.

REFERENCES

1. S. Vosoughi, D. Roy, and S. Aral, "The spread of true and false news online," *Science*, vol. 359, no. 6380, pp. 1146-1151, 2018, doi: 10.1126/science.aap9559.
2. N. Grinberg, K. Joseph, L. Friedland, B. Swire-Thompson, and D. Lazer, "Fake news on Twitter during the 2016 U.S. presidential election," *Science*, vol. 363, no. 6425, pp. 374-378, 2019, doi: 10.1126/science.aau2706.
3. M. Mustak, J. Salminen, M. Mäntymäki, A. Rahman, and Y. K. Dwivedi, "Deepfakes: Deceptions, mitigations, and opportunities," *Journal of Business Research*, vol. 154, p. 113368, 2023, doi: 10.1016/j.jbusres.2022.113368.
4. K. Nuortimo, J. Harkonen, and K. Breznik, "Exploring corporate reputation and crisis communication," *Journal of Marketing Analytics*, vol. 14, pp. 4-25, 2026, doi: 10.1057/s41270-024-00353-8.
5. J. Udry and S. J. Barber, "The illusory truth effect: A review of how repetition increases belief in misinformation," *Current Opinion in Psychology*, vol. 56, p. 101736, 2024, doi: 10.1016/j.copsyc.2023.101736.
6. V. Vellani, S. Zheng, D. Ercelik, and T. Sharot, "The illusory truth effect leads to the spread of misinformation," *Cognition*, vol. 236, p. 105421, 2023, doi: 10.1016/j.cognition.2023.105421.

7. G. Pennycook and D. G. Rand, "The psychology of fake news," *Trends in Cognitive Sciences*, vol. 25, no. 5, pp. 388-402, 2021, doi: 10.1016/j.tics.2021.02.007.
8. W. T. Coombs, "Protecting organization reputations during a crisis: The development and application of Situational Crisis Communication Theory," *Corporate Reputation Review*, vol. 10, pp. 163-176, 2007, doi: 10.1057/palgrave.crr.1550049.
9. W. T. Coombs and S. J. Holladay, "Helping crisis managers protect reputational assets: Initial tests of the Situational Crisis Communication Theory," *Management Communication Quarterly*, vol. 16, no. 2, pp. 165-186, 2002, doi: 10.1177/089331802237233.
10. W. L. Benoit, "Image repair discourse and crisis communication," *Public Relations Review*, vol. 23, no. 2, pp. 177-186, 1997, doi: 10.1016/S0363-8111(97)90023-0.
11. A. Elgueta-Ruiz, G. Sadi, G. Gonçalves, and J. Martínez-Ortiz, "Meta-research on crisis communication: 24 years of research in *Public Relations Review* (2000-2023)," *Public Relations Review*, vol. 52, no. 2, p. 102685, 2026, doi: 10.1016/j.pubrev.2026.102685.
12. Y. Cheng, "How social media is changing crisis communication strategies: Evidence from the updated literature," *Journal of Contingencies and Crisis Management*, vol. 26, no. 1, pp. 58-68, 2018, doi: 10.1111/1468-5973.12130.
13. K. D. Sweetser and colleagues, "Social media dialogues in a crisis: A mixed-methods approach to identifying publics on social media," *Public Relations Review*, vol. 44, no. 4, pp. 562-573, 2018, doi: 10.1016/j.pubrev.2018.07.005.
14. L. M. Arpan and D. Pompper, "Stormy weather: Testing 'stealing thunder' as a crisis communication strategy to improve communication flow between organizations and journalists," *Public Relations Review*, vol. 29, no. 3, pp. 291-308, 2003, doi: 10.1016/S0363-8111(03)00043-2.
15. S. Lee, "Stealing thunder as a crisis communication strategy in the digital age," *Business Horizons*, vol. 63, no. 6, pp. 801-810, 2020, doi: 10.1016/j.bushor.2020.07.006.
16. A.-S. Claeys and V. Cauberghe, "Crisis response and crisis timing strategies, two sides of the same coin," *Public Relations Review*, vol. 38, no. 1, pp. 83-88, 2012, doi: 10.1016/j.pubrev.2011.09.001.
17. F. Schultz, S. Utz, and A. Göritz, "Is the medium the message? Perceptions of and reactions to crisis communication via Twitter, blogs and traditional media," *Public Relations Review*, vol. 37, no. 1, pp. 20-27, 2011, doi: 10.1016/j.pubrev.2010.12.001.
18. J. Xu, "Does the medium matter? A meta-analysis on using social media vs. traditional media in crisis communication," *Public Relations Review*, vol. 46, no. 4, p. 101947, 2020, doi: 10.1016/j.pubrev.2020.101947.
19. S. R. Veil, T. Buehner, and M. J. Palenchar, "A work-in-process literature review: Incorporating social media in risk and crisis communication," *Journal of Contingencies and Crisis Management*, vol. 19, no. 2, pp. 110-122, 2011, doi: 10.1111/j.1468-5973.2011.00639.x.
20. A. Hassan and S. J. Barber, "The effects of repetition frequency on the illusory truth effect," *Cognitive Research: Principles and Implications*, vol. 6, p. 38, 2021, doi: 10.1186/s41235-021-00301-5.
21. J. Udry, S. K. White, and S. J. Barber, "The effects of repetition spacing on the illusory truth effect," *Cognition*, vol. 225, p. 105157, 2022, doi: 10.1016/j.cognition.2022.105157.
22. E. L. Henderson, S. J. Westwood, and D. J. Simons, "A reproducible systematic map of research on the illusory truth effect," *Psychonomic Bulletin & Review*, vol. 29, pp. 1065-1088, 2022, doi: 10.3758/s13423-021-01995-w.
23. E. K. Vraga, L. Bode, and M. Tully, "Creating news literacy messages to enhance expert corrections of misinformation on Twitter," *Communication Research*, vol. 49, no. 2, pp. 229-251, 2022, doi: 10.1177/0093650219898094.
24. F. Stoeckel, S. Stöckli, B. Ceka, C. Ricchi, B. Lyons, and J. Reifler, "Social corrections act as a double-edged sword by reducing the perceived accuracy of false and real news in the UK, Germany, and Italy," *Communications Psychology*, vol. 2, p. 10, 2024, doi: 10.1038/s44271-024-00057-w.
25. J. Singh, B. Crisafulli, L. T. Quamina, and M. T. Xue, "'To trust or not to trust': The impact of social media influencers on the reputation of corporate brands in crisis," *Journal of Business Research*, vol. 119, pp. 464-480, 2020, doi: 10.1016/j.jbusres.2020.03.039.
26. Z. Olbermann and H. Schramm, "Brand-related social media influencers as spokespersons after a corporate greenwashing crisis: Implications of parasocial interactions and wishful identification on the perception of the brand image," *Public Relations Review*, vol. 51, no. 4, p. 102612, 2025, doi: 10.1016/j.pubrev.2025.102612.

27. L. Hagen, T. Keller, S. Neely, N. DePaula, and C. Robert-Cooperman, "Crisis communications in the age of social media: A network analysis of Zika-related tweets," *Social Science Computer Review*, vol. 36, no. 5, pp. 523-541, 2018, doi: 10.1177/0894439317721985.
28. S.-Y. Kim and J.-H. Lee, "How to maximize the effectiveness of stealing thunder in crisis communication: The significance of follow-up actions and transparent communication," *Corporate Communications: An International Journal*, vol. 27, no. 3, pp. 425-440, 2022, doi: 10.1108/CCIJ-04-2021-0047.
29. J. Tække, "Crisis communication and social media: A systems- and medium-theoretical perspective," *Systems Research and Behavioral Science*, vol. 34, no. 2, pp. 182-194, 2017, doi: 10.1002/sres.2451.
30. Y. Li and N. Kapucu, "Determinants of the use of social media in crisis communication: An analysis of microblogging by Chinese local government," *International Journal of Public Administration*, vol. 48, no. 2, pp. 100-114, 2025, doi: 10.1080/01900692.2024.2316130.
31. S. Hong and B. Kim, "Exploring social media use in university crisis communication: An experiment to measure impact on perceived crisis severity and attitudes of key publics," *Journal of Contingencies and Crisis Management*, vol. 27, pp. 61-71, 2019, doi: 10.1111/1468-5973.12242.
32. S. Hong, B. Kim, and S. Y. Lee, "A public health crisis in the university: Impact of crisis response strategies on universities' transparency and post-crisis relationships during COVID-19 pandemic," *Public Relations Review*, vol. 49, no. 1, p. 102287, 2023, doi: 10.1016/j.pubrev.2023.102287.
33. J. W. M. Verhoeven, J. J. Van Hoof, H. Ter Keurs, and M. Van Vuuren, "Effects of apologies and crisis responsibility on corporate and spokesperson reputation," *Public Relations Review*, vol. 38, no. 3, pp. 501-504, 2012, doi: 10.1016/j.pubrev.2012.02.002.
34. A.-S. Claey's, V. Cauberghe, and P. Vyncke, "Restoring reputations in times of crisis: An experimental study of the Situational Crisis Communication Theory and the moderating effects of locus of control," *Public Relations Review*, vol. 36, no. 3, pp. 256-262, 2010, doi: 10.1016/j.pubrev.2010.05.004.
35. S. Kim, E. J. Avery, and R. W. Lariscy, "Are crisis communicators practicing what we preach? An evaluation of crisis response strategy analyzed in public relations research from 1991 to 2009," *Public Relations Review*, vol. 35, no. 4, pp. 446-448, 2009, doi: 10.1016/j.pubrev.2009.08.002.
36. L. Zhou and J.-H. Shin, "Does stealing thunder always work? A content analysis of crisis communication practice under different cultural settings," *Public Relations Review*, vol. 43, no. 5, pp. 1036-1047, 2017, doi: 10.1016/j.pubrev.2017.08.004.
37. A.-S. Claey's, V. Cauberghe, and J. Leysen, "Implications of stealing thunder for the impact of expressing emotions in organizational crisis communication," *Journal of Applied Communication Research*, vol. 41, no. 3, pp. 293-308, 2013, doi: 10.1080/00909882.2013.806991.
38. G. Burel, "Exploring the impact of automated correction of misinformation in social media," *AI Magazine*, vol. 45, no. 2, pp. 227-245, 2024, doi: 10.1002/aaai.12180.
39. W. T. Coombs, "Situational Crisis Communication Theory: Refining and clarifying a cognitive-based theory of crisis communication," in *The Handbook of Crisis Communication*, 2022, doi: 10.1002/9781119678953.ch14.
40. W. T. Coombs, "Attribution Theory as a guide for post-crisis communication research," *Public Relations Review*, vol. 33, no. 2, pp. 135-139, 2007, doi: 10.1016/j.pubrev.2006.11.016.
41. J.-J. Kuipers, "Towards a European approach in the cross-border infringement of personality rights," *German Law Journal*, vol. 12, no. 8, pp. 1681-1706, 2011, doi: 10.1017/S2071832200017491.
42. S. Sakolciová, "Defamation on social media: Challenges of private international law," *Bratislava Law Review*, vol. 5, no. 1, 2021, doi: 10.46282/blr.2021.5.1.226.
43. R. Ó Fathaigh, D. Buijs, and J. van Hoboken, "The regulation of disinformation under the Digital Services Act," *Media and Communication*, vol. 13, Art. 9615, 2025, doi: 10.17645/mac.9615.
44. Z. Hajnal, "The new liability forms of online platforms in the new European digital legal framework from the consumers' perspective," *Acta Universitatis Sapientiae, Legal Studies*, vol. 12, no. 2, pp. 19-35, 2023, doi: 10.47745/AUSLEG.2023.12.2.02.