



Synthetic Crises: Defending Corporate Reputation Against Deepfakes and Disinformation

By

Mbah Maria Ukachukwu¹ Afolabi Kazeem Opeyemi²

¹National Research Institute for Chemical Technology, Zaria, Kaduna-State, Nigeria

²Ahmadu Bello University, Zaria, Kaduna State, Nigeria



Article History

Received: 05/02/2025

Accepted: 25/02/2025

Published: 27/02/2025

Vol – 2 Issue – 1

PP: -60-71

DOI:10.5281/zenodo.
21623001

Abstract

The convergence of generative artificial intelligence, platform algorithmics, and participatory disinformation has fundamentally restructured the temporal, evidentiary, and institutional boundaries that once governed organizational crisis response (Coombs, 2019; Fearn-Banks, 2017 updated in Coombs & Holladay, 2022). Where organizations once possessed measurable windows for strategic communication, synthetic media ecosystems now compress response timelines to sub-minute intervals while simultaneously undermining the heuristic processes through which stakeholders evaluate organizational authenticity (Paris & Donovan, 2019; Zheng et al., 2020; Wardle & Derakhshan, 2018). This article presents a theoretically grounded, conceptually comprehensive examination of how deepfake technologies, algorithmic amplification architectures, and coordinated inauthentic behavior collectively produce a new species of organizational crisis — one defined not by institutional failure but by externally fabricated epistemic contamination (Kietzmann et al., 2020; Tandoc et al., 2018). Drawing upon Situational Crisis Communication Theory (SCCT) and the Social-Mediated Crisis Communication (SMCC) model — both substantially revised to accommodate digital complexity — we identify three structural disruptions governing synthetic crisis ecology: velocity compression, verisimilitude erosion, and viral persistence (Cheng, 2019; Jin & Austin, 2019; Veil, 2018). We further argue that existing crisis communication frameworks are theoretically insufficient to address synthetic victimization scenarios, in which organizations are genuine targets of malicious fabrication rather than authors of institutional failure (Liu & Fraustino, 2018; Kim, 2021; Coombs & Holladay, 2022). In response, this article proposes the Prebunking-Verification-Response (PVR) model — a continuous, infrastructurally grounded framework for building reputation resilience capable of operating within algorithmically hostile information environments (Veil, 2018; Macnamara, 2018; Zeffass et al., 2020). These contributions advance the theoretical frontier of crisis communication scholarship by repositioning synthetic reality as a permanent structural variable within the strategic communication landscape.

Keywords: crisis, communication, synthetic, media, deepfakes, algorithmic.

1. Introduction

The foundational architecture of crisis communication scholarship rests upon a set of assumptions that, while empirically validated across decades of research, were constructed within media environments fundamentally different from those that define organizational life in the 2020s (Coombs, 2019; Heath & O'Hair, 2020). These assumptions — that crises originate in identifiable organizational events, that stakeholders receive and evaluate information through recognizable channels, that authenticity can be established through institutional authority, and that strategic response operates within a manageable temporal

window — have been systematically destabilized by the convergence of three transformative technological forces: generative artificial intelligence, algorithmic platform architecture, and coordinated inauthentic behavior (Paris & Donovan, 2019; Zheng et al., 2020; Yang, 2018; Wardle & Derakhshan, 2018). The cumulative effect of these forces is not merely an acceleration of existing crisis dynamics but a qualitative transformation of the epistemic environment within which organizational reputation is constructed and contested (Jin & Austin, 2019; Coombs & Holladay, 2022). Contemporary crises no longer require institutional failures to materialize (Coombs, 2019; Benoit, 2018). They can be entirely synthetic: fabricated by malicious actors through

generative adversarial networks, deepfake audio and video production, and large language models capable of mimicking executive communication styles with unsettling precision (Kietzmann et al., 2020; Hancock et al., 2020). When these synthetic artifacts are introduced into platform ecosystems designed to amplify emotionally provocative content, they can achieve global virality before organizational crisis teams complete initial threat detection protocols (Cheng, 2019; Veil, 2018). The consequences extend beyond reputational damage into ontological disruption: stakeholders are left unable to determine which representations of organizational reality are authentic, creating what this article terms "epistemic disorientation" — a sustained condition of communicative uncertainty that undermines the foundational premise of strategic public relations (Jin & Austin, 2019; Kim, 2021; Craft et al., 2020). The urgency of this problem is compounded by the inadequacy of existing theoretical frameworks (Liu & Fraustino, 2018; An & Gower, 2020). Situational Crisis Communication Theory (SCCT), despite significant post-2018 refinement, was developed to explain how organizations communicate during crises they have caused or been associated with (Coombs, 2019). It provides limited guidance for scenarios in which organizations are themselves victims of sophisticated fabrication campaigns (Liu & Fraustino, 2018; An & Gower, 2020). Similarly, the Social-Mediated Crisis Communication (SMCC) model offers valuable insights into peer-to-peer crisis information behavior but was formulated before algorithmic mediation became a dominant variable in crisis discourse construction (Austin et al., 2019; Jin & Austin, 2019). Neither framework adequately theorizes the role of synthetic content, platform recommendation architectures, or the forensic competencies required to distinguish authentic organizational communication from malicious replication (Yang, 2018; Veil, 2018; Zerfass et al., 2020).

This article addresses that theoretical deficit through four interconnected contributions. First, we conduct a comprehensive review of post-2018 crisis communication literature, identifying where established frameworks require extension to accommodate synthetic crisis ecologies (Liu & Fraustino, 2018; Heath & O'Hair, 2020). Second, we develop the concept of "synthetic victimization" as a distinct crisis cluster requiring specific theoretical and practical treatment within SCCT (Coombs, 2019; Kim, 2021; Benoit, 2018). Third, we analyze the architecture of synthetic crisis across three dimensions — velocity, verisimilitude, and viral persistence — demonstrating their interdependent effects on stakeholder attribution and organizational credibility (Zheng et al., 2020; Yang, 2018; Paris & Donovan, 2019; Tandoc et al., 2018). Fourth, we propose the Prebunking-Verification-Response (PVR) framework as a theoretically coherent and practically actionable model for building reputation resilience within algorithmically hostile environments (Veil, 2018; Cheng, 2019; Macnamara, 2018; Zerfass et al., 2020). These contributions are timely. The global economic losses attributable to corporate disinformation campaigns exceeded \$78 billion in 2022, with deepfake-related financial fraud alone increasing by 400% between 2019 and 2023 (European

Commission, 2023). The public relations profession is not merely engaging with an interesting theoretical puzzle; it confronts an existential threat to its institutional credibility as the discipline responsible for managing organizational truth in public discourse (Macnamara, 2018; Tambuscio et al., 2018; Nothhaft et al., 2018). Scholars and practitioners must respond with theoretical sophistication, ethical clarity, and infrastructural preparedness commensurate with the scale and complexity of the challenge (Veil, 2018; Austin et al., 2019; Gregory & Halff, 2020).

2. Literature Review: Crisis Communication Scholarship in the Post-2018 Landscape

2.1 The Evolution of Situational Crisis Communication Theory

Situational Crisis Communication Theory, most comprehensively articulated in its fifth edition formulation, remains the dominant theoretical framework for predicting stakeholder responses to organizational crises and prescribing effective communicative strategies (Coombs, 2019). The theory's explanatory power derives from its integration of attribution theory, which holds that stakeholders evaluate crisis events through cognitive assessments of causality, controllability, and prior organizational history (Coombs, 2019; Frandsen & Johansen, 2020). These assessments determine the degree of responsibility attributed to the organization and, consequently, the reputational threat the crisis poses (Kim, 2021; An & Gower, 2020). SCCT organizes crises into three clusters — victim, accidental, and preventable — each associated with a spectrum of recommended responses ranging from denial and minimization to apology and corrective action (Coombs, 2019; Benoit, 2018).

Post-2018 scholarship has substantially refined and extended this framework in important ways. Kim (2021) demonstrated through social media analytics that attribution processes in digital environments are mediated not only by cognitive evaluation but by emotional contagion — the rapid, network-mediated spread of anger, disgust, and moral outrage that can crystallize stakeholder attributions before organizations have issued any response (Kim, 2021; Brady et al., 2020). This finding is significant because it reveals that strategic communication operates not merely in a competitive information environment but within affectively charged network dynamics that amplify negative attribution independently of organizational action (Kim, 2021; Yang, 2018; Lee & Kwon, 2019). Cheng (2019) further demonstrated that cultural variability in attribution heuristics requires crisis practitioners operating in global environments to calibrate response strategies across distinct audience epistemologies, complicating the universalist prescriptions of classical SCCT (Cheng, 2019; Frandsen & Johansen, 2020). Most relevantly for the present analysis, Liu and Fraustino (2018) identified a critical theoretical gap in SCCT: its typologies presuppose that the triggering event of a crisis is causally connected to organizational conduct, whether

through active culpability or passive negligence (Liu & Fraustino, 2018). However, in scenarios where crises are externally manufactured through synthetic fabrication, this causal presumption fails entirely (Paris & Donovan, 2019; Hancock et al., 2020). The organization is not responsible for the crisis event because no such event occurred; it is responding to a manufactured representation designed to simulate institutional failure (Liu & Fraustino, 2018; Kim, 2021; Coombs & Holladay, 2022). This distinction demands a fourth crisis cluster within SCCT — "synthetic victimization" — characterized by external epistemic attack rather than internal operational failure (Liu & Fraustino, 2018; An & Gower, 2020).

2.2 The Social-Mediated Crisis Communication Model and Algorithmic Extension

The Social-Mediated Crisis Communication model has undergone substantial revision since 2018 to accommodate the growing complexity of social media ecosystems (Austin et al., 2019; Jin & Austin, 2019). The model's core architecture identifies three types of social media users in crisis contexts: influential social media creators who produce crisis content, social media followers who consume and share it, and social media inactives who access crisis information through traditional media (Jin & Austin, 2019; Eriksson & Olsson, 2020). The revised model emphasizes that these categories are not static but dynamically reconfigured by platform algorithms that determine content visibility, amplification, and cross-network migration (Austin et al., 2019; Yang, 2018; Lee & Kwon, 2019). Austin et al. (2019) demonstrated empirically that the source of crisis information — whether organizational, journalistic, or peer-generated — significantly moderates stakeholder risk perceptions and behavioral intentions (Austin et al., 2019). Their findings indicate that peer-generated crisis information carries higher perceived credibility in digitally native audiences than organizational statements, creating structural disadvantages for institutional voices competing with viral peer content (Austin et al., 2019; Eriksson & Olsson, 2020). This credibility asymmetry has profound implications for organizations managing synthetic crises: when fabricated peer testimonials or counterfeit organizational statements achieve viral status through peer-sharing networks, official organizational corrections must overcome both algorithmic suppression and peer-credibility disadvantage simultaneously (Jin & Austin, 2019; Zheng et al., 2020; Craft et al., 2020). Yang (2018) extended the SMCC model by quantitatively modeling the relationship between crisis information form — text, image, video — and stakeholder attribution intensity (Yang, 2018). His findings revealed that visual crisis information generates significantly stronger attribution responses than text-based equivalents, regardless of factual accuracy (Yang, 2018; Brady et al., 2020). This finding acquires heightened urgency in synthetic crisis environments, where deepfake video content — combining visual immediacy with fabricated substance — represents the most attribution-intensive crisis artifact currently available to malicious actors (Yang, 2018; Kietzmann et al., 2020; Hancock et al., 2020).

Jin and Austin (2019) further revised the SMCC model to incorporate what they term "algorithmic crisis actors": platform recommendation systems that function as non-human participants in crisis discourse by selectively amplifying content based on engagement metrics rather than informational accuracy (Jin & Austin, 2019). This conceptual move is theoretically significant because it expands the actor landscape of crisis communication beyond human stakeholders to include computational agents whose crisis behavior is neither intentional nor responsive to strategic communication (Jin & Austin, 2019; Zeffass et al., 2020). Organizations cannot persuade an algorithm; they can only understand its mechanics and structure their communications to operate within — or actively leverage — its amplification logics (Kietzmann et al., 2020; Gregory & Halff, 2020).

2.3 Disinformation, Synthetic Media, and Corporate Vulnerability

Paris and Donovan's (2019) foundational analysis of deepfakes and cheap fakes established a typological distinction essential for crisis communication research (Paris & Donovan, 2019). Deepfakes — synthetic media produced through machine learning techniques — require technical sophistication and computational resources to produce but are increasingly accessible to non-specialist actors (Paris & Donovan, 2019; Kietzmann et al., 2020). Cheap fakes — manipulated media produced through simple editing techniques such as speed alteration, decontextualization, or caption manipulation — require minimal technical skill but can generate equivalent reputational damage when distributed through high-velocity social networks (Paris & Donovan, 2019; Tandoc et al., 2018). Corporate vulnerability to both categories is substantial: deepfakes threaten executive credibility and brand authenticity, while cheap fakes threaten operational reputation and consumer trust (Kietzmann et al., 2020; Hancock et al., 2020). Zheng et al. (2020) provided the first systematic examination of deepfake exposure effects on organizational reputation, demonstrating that even brief exposure to synthetic executive misconduct simulations produced significant decreases in consumer trust that persisted after correction (Zheng et al., 2020). Critically, their study found that corrections were less effective when delivered by the victimized organization than when delivered by credible third-party sources — a finding with direct implications for PVR framework design (Zheng et al., 2020; Craft et al., 2020). Wardle and Derakhshan (2018) provided essential conceptual grounding by distinguishing between misinformation — false content shared without malicious intent — and disinformation — false content deliberately created to cause harm (Wardle & Derakhshan, 2018). This distinction is theoretically critical for crisis communication because organizational response strategies must differ fundamentally depending on whether synthetic content originates from malicious attack or inadvertent error (Wardle & Derakhshan, 2018; Tandoc et al., 2018; Liu & Fraustino, 2018). Tandoc et al. (2018) further elaborated this typological framework, identifying six distinct forms of online content falsity — satire, parody, fabrication, manipulation, advertising, and propaganda — each requiring distinct

detection and correction approaches (Tandoc et al., 2018). For crisis communication practitioners, this typological complexity means that synthetic crisis management cannot rely upon uniform response protocols; it requires nuanced assessment of fabrication type, intent, and distribution mechanism before strategic response decisions can be made (Tandoc et al., 2018; Liu & Fraustino, 2018; Benoit, 2018). Kietzmann et al. (2020) examined deepfake technology through a business risk lens, identifying four corporate vulnerability categories: executive impersonation, product falsification, financial fraud, and competitive sabotage (Kietzmann et al., 2020). Their analysis concluded that existing risk management frameworks are inadequate for synthetic media threats because they presuppose adversarial actors who exploit organizational weaknesses rather than manufacture organizational realities (Kietzmann et al., 2020). Hancock et al. (2020) extended this analysis by examining the psychological mechanisms through which synthetic media achieves persuasive impact, demonstrating that deepfake content leverages "digital identity trust" — the automatic credibility extension audiences grant to familiar faces and voices — to achieve attribution effects disproportionate to its evidential quality (Hancock et al., 2020). Tambuscio et al. (2018) contributed essential network science perspectives by computationally modeling the diffusion dynamics of misinformation across platform structures, demonstrating that algorithmically connected networks amplify false information at rates disproportionate to factual merit (Tambuscio et al., 2018). Their modeling revealed that network segregation — the clustering of audiences within ideologically homogeneous information communities — substantially accelerates false content propagation by limiting exposure to corrective information from outgroup sources (Tambuscio et al., 2018; Brady et al., 2020). Nothhaft et al. (2018) approached corporate vulnerability from a strategic communication management perspective, arguing that contemporary organizations require "communication intelligence" capabilities — systematic environmental scanning and sense-making capacities — to detect emerging synthetic threats before they achieve crisis velocity (Nothhaft et al., 2018).

2.4 Reputation Management and Organizational Legitimacy in Synthetic Environments

Organizational reputation, conceptualized as the aggregate evaluation stakeholders form of an organization's past conduct and future prospects, constitutes a strategic asset whose value is fundamentally dependent upon information integrity (Zerfass et al., 2020; Gregory & Halff, 2020). When synthetic disinformation contaminates the information environment within which reputational evaluations are formed, it does not merely damage existing reputation; it undermines the epistemic foundations upon which any stable reputation can be constructed (Coombs & Holladay, 2022; Kim, 2021). Zerfass et al. (2020) conducted extensive survey research across European communication professionals, finding that artificial intelligence and algorithmic communication management were identified as the most significant emerging challenges to strategic communication practice — challenges for which fewer than 20% of surveyed organizations reported

adequate preparedness (Zerfass et al., 2020). Gregory and Halff (2020) examined the implications of AI-driven communication for the public relations profession's epistemic authority, arguing that as AI systems become capable of producing synthetic organizational communication, the profession's claim to represent authentic organizational voice becomes increasingly contested (Gregory & Halff, 2020). These findings collectively suggest that the reputation management implications of synthetic media extend well beyond individual crisis events to challenge the foundational legitimacy of the public relations function itself (Gregory & Halff, 2020; Nothhaft et al., 2018; Zerfass et al., 2020).

2.5 Ethical Dimensions of Crisis Communication in Synthetic Environments

The ethical landscape of crisis communication has been substantially complicated by synthetic media and the organizational systems deployed to detect it (Macnamara, 2018; Veil, 2018; Craft et al., 2020). Macnamara's (2018) comprehensive evaluation of organizational listening practices revealed that most public relations departments collect stakeholder sentiment data through monitoring systems that lack adequate transparency about collection methods, analytical assumptions, and interpretive frameworks (Macnamara, 2018). In synthetic crisis environments, this opacity becomes ethically untenable: organizations deploying AI systems to detect and characterize stakeholder responses must transparently disclose these systems' capabilities and limitations, or risk compounding epistemic distrust through surveillance opacity (Macnamara, 2018; Kietzmann et al., 2020). Craft et al. (2020) examined the ethical obligations of communication professionals in disinformation environments, arguing that professional responsibility now extends beyond representing clients truthfully to actively combating the false information ecosystems that threaten democratic communication infrastructure (Craft et al., 2020). Veil (2018) examined crisis communication ethics from the perspective of organizational listening, arguing that effective crisis management requires genuine responsiveness to stakeholder concern rather than strategic performance of attentiveness (Veil, 2018). In synthetic crisis contexts, this distinction acquires particular urgency: when organizations deploy AI monitoring systems to manage rather than genuinely respond to stakeholder sentiment, they replicate the epistemic manipulation they claim to resist (Veil, 2018; Craft et al., 2020; Macnamara, 2018).

3. The Architecture of Synthetic Crisis: Velocity, Verisimilitude, and Viral Persistence

3.1 Velocity: Strategic Time Compression and the Sub-Minute Crisis

Temporal strategy has always been central to crisis communication theory (Coombs, 2019; Frandsen & Johansen, 2020). The conventional understanding posited that organizational responses issued within the first hour of crisis emergence were significantly more effective than delayed responses at containing reputational damage and managing

stakeholder attribution (Coombs, 2019; Heath & O'Hair, 2020). This "golden hour" framework operated under the assumption that crises spread through journalistic channels with identifiable production cycles — news gathering, editorial review, publication, and audience reach — each introducing temporal delays that provided organizational response windows (Austin et al., 2019; Eriksson & Olsson, 2020). In algorithmically mediated synthetic crisis environments, this assumption is invalidated by the interaction of three velocity mechanisms: generation speed, distribution infrastructure, and engagement automation (Paris & Donovan, 2019; Tambuscio et al., 2018). Deepfake content can be generated in minutes to hours; distributed through social platforms in seconds; and amplified through bot networks and engagement pods within minutes of initial posting (Paris & Donovan, 2019; Hancock et al., 2020). The compound effect is that synthetic crises can achieve global visibility and stakeholder attribution formation before organizations detect the initial threat signal (Zheng et al., 2020; Nothhaft et al., 2018). Empirical documentation of this velocity effect is accumulating across multiple research contexts. Cheng (2019) conducted a temporal analysis of corporate social media crises across multiple industries and found that organizations responding after the sixty-minute threshold from viral content emergence suffered attribution penalties that corrective action could not fully neutralize (Cheng, 2019). Yang (2018) further demonstrated that visual content — the primary medium of deepfake attack — achieves peak amplification velocity significantly faster than text-based content, meaning that deepfake crises likely achieve irreversible attribution crystallization in shorter windows than conventional analysis suggests (Yang, 2018; Brady et al., 2020). Tambuscio et al. (2018) provided complementary network evidence, demonstrating through computational modeling that false information achieves network saturation at rates approximately three times faster than factual corrections across equivalent network structures — a finding that quantifies the asymmetric disadvantage organizations face in correcting synthetic crisis content (Tambuscio et al., 2018). Lee and Kwon (2019) further demonstrated that mobile-first content consumption patterns dramatically accelerate initial attribution formation, as smartphone users process crisis content through rapid, heuristic-dependent evaluation rather than deliberate analytical assessment (Lee & Kwon, 2019). The strategic implication of velocity compression is profound: traditional crisis response planning cycles — threat identification, stakeholder analysis, message development, channel selection, approval processes, and dissemination — are structurally incompatible with sub-minute crisis timelines (Jin & Austin, 2019; Eriksson & Olsson, 2020). Organizations must therefore develop pre-positioned response architectures: pre-authorized message templates, cryptographically authenticated distribution channels, automated threat detection systems, and crisis team protocols that eliminate approval hierarchies during the initial response window (Veil, 2018; Austin et al., 2019; Nothhaft et al., 2018). This architectural requirement moves crisis management from a communicative function to an infrastructural one — a shift with significant

organizational, financial, and ethical implications that scholarship has only begun to theorize (Macnamara, 2018; Gregory & Half, 2020; Zeff et al., 2020).

3.2 Verisimilitude: The Systematic Erosion of Credibility Heuristics

Cognitive psychology has long established that human information processing under uncertainty relies upon heuristic shortcuts — mental rules of thumb that reduce evaluative complexity by substituting proxies of truth for evidential evaluation (Kim, 2021; Brady et al., 2020). In communication contexts, these heuristics include source credibility assessments, message coherence evaluations, and social proof monitoring (Kim, 2021; Lee & Kwon, 2019). These heuristics function adaptively in information environments where synthetic deception requires substantial skill and resources — conditions that no longer obtain in the generative AI era (Zheng et al., 2020; Kietzmann et al., 2020; Hancock et al., 2020).

Synthetic media technologies are specifically engineered to exploit credibility heuristics in ways that create significant organizational vulnerability (Paris & Donovan, 2019; Hancock et al., 2020). Deepfake video content replicates the visual and kinetic signatures of authentic footage, satisfying the perceptual fluency heuristic that equates technical quality with authenticity (Kietzmann et al., 2020; Hancock et al., 2020). Generative language models replicate the linguistic patterns, stylistic idiosyncrasies, and institutional vocabularies of specific organizational actors, satisfying source familiarity heuristics (Kietzmann et al., 2020; Zheng et al., 2020). Coordinated inauthentic behavior — networks of fake accounts that simulate organic stakeholder consensus — exploits social proof heuristics by manufacturing the appearance of widespread credibility endorsement (Paris & Donovan, 2019; Tambuscio et al., 2018; Wardle & Derakhshan, 2018). When these heuristic exploits are combined — as they frequently are in sophisticated synthetic crisis campaigns — stakeholders experience "epistemic disorientation": a condition in which previously reliable cognitive verification tools produce systematically unreliable outputs (Jin & Austin, 2019; Kim, 2021; Craft et al., 2020). This disorientation has measurable consequences for crisis communication effectiveness. Zheng et al. (2020) demonstrated that stakeholders exposed to high-quality synthetic crisis content applied identical credibility heuristics to authentic organizational corrections as to the fabricated content — meaning that organizational corrections were evaluated with the same epistemic suspicion as the original attack (Zheng et al., 2020). Brady et al. (2020) provided complementary evidence that moral-emotional language in synthetic crisis content — language emphasizing harm, betrayal, and injustice — generates disproportionate sharing behavior independent of content veracity, creating viral amplification dynamics that organizational corrections' typically neutral, factual tone cannot match (Brady et al., 2020). This analysis reveals a fundamental limitation of conventional crisis response strategies within synthetic environments. SCCT's recommendation of corrective action

as an appropriate response to preventable crises presupposes that audiences can recognize corrective action as genuinely organizational (Coombs, 2019; Benoit, 2018). When synthetic replicas of organizational corrections — "deepfake apologies" designed to further confuse stakeholder attribution — are technically feasible, the entire corrective action strategy may be subverted by adversarial actors (Liu & Fraustino, 2018; Kim, 2021). Crisis communication theory must therefore grapple with the possibility that conventional response strategies can be weaponized against the organizations that deploy them (Liu & Fraustino, 2018; Coombs & Holladay, 2022).

3.3 Viral Persistence: Platform Architecture and the Longevity of Manufactured Reality

The "continued influence effect" — the empirically documented finding that corrective information fails to eliminate the cognitive impact of misinformation even after successful debunking — has been well established in cognitive and communication psychology (Yang, 2018; Wardle & Derakhshan, 2018). In algorithmically mediated platform environments, this psychological phenomenon is structurally amplified by recommendation architectures that continue surfacing high-engagement content long after corrections are issued (Kietzmann et al., 2020; Tandoc et al., 2018). Platform algorithms optimize for user engagement, operationalized through metrics such as watch time, comment generation, and share behavior (Jin & Austin, 2019; Lee & Kwon, 2019). Synthetic crisis content — designed to provoke emotional responses — consistently generates higher engagement signals than organizational corrections, which typically prioritize factual accuracy over emotional intensity (Austin et al., 2019; Brady et al., 2020; Yang, 2018). The structural consequence is what we term "algorithmic persistence bias": the tendency of platform recommendation systems to systematically favor synthetic crisis artifacts over organizational corrections within recommendation feeds, search results, and discovery mechanisms (Jin & Austin, 2019; Tandoc et al., 2018). This bias operates independently of content veracity and requires direct engagement with platform governance structures, algorithmic optimization of corrective content, and sustained counter-narrative presence within crisis-related information flows (Veil, 2018; Macnamara, 2018; Gregory & Halff, 2020). Further complicating viral persistence is the cross-platform migration of synthetic content (Paris & Donovan, 2019; Wardle & Derakhshan, 2018). Fabricated crisis artifacts migrate across ecosystems — from X to TikTok to Reddit to YouTube — adapting to each platform's format norms, content policies, and audience characteristics through re-editing, decontextualization, and re-annotation (Paris & Donovan, 2019; Tandoc et al., 2018). Tambuscio et al. (2018) demonstrated computationally that cross-network migration substantially extends the active life of false content by introducing it to network communities where corrections have not yet penetrated (Tambuscio et al., 2018). Organizations monitoring a crisis on a single platform may therefore dramatically underestimate total synthetic contamination

within the stakeholder information environment (Macnamara, 2018; Cheng, 2019; Nothhaft et al., 2018).

4. Synthetic Victimization as a Distinct Crisis Cluster

Building upon Liu and Fraustino's (2018) identification of the theoretical gap in SCCT's crisis typology, we formally propose "synthetic victimization" as a fourth crisis cluster requiring dedicated theoretical treatment and distinct strategic protocols (Liu & Fraustino, 2018; Coombs & Holladay, 2022). Synthetic victimization describes crisis scenarios in which organizational reputational threat originates entirely from external fabrication — malicious actors producing and distributing false representations of organizational conduct, capability, or communication — rather than from internal operational or ethical failure (Liu & Fraustino, 2018; Paris & Donovan, 2019; Kietzmann et al., 2020). The distinction between synthetic victimization and conventional victim-cluster crises within SCCT is critical and consequential (Coombs, 2019; An & Gower, 2020). In conventional victim crises — natural disasters, workplace violence, external economic shocks — the organization experiences genuine adverse events but bears minimal causal responsibility (Coombs, 2019; Frandsen & Johansen, 2020). Stakeholder attribution in victim crises tends toward sympathy, and strategic communication appropriately emphasizes organizational suffering and resilience (Coombs, 2019; Kim, 2021; Eriksson & Olsson, 2020). In synthetic victimization scenarios, by contrast, the adverse "event" itself is fabricated: no product recall occurred, no executive misconduct transpired (Paris & Donovan, 2019; Kietzmann et al., 2020). The organization is defending not against the communicative consequences of a real event but against the evidential fabrication of a non-existent one (Liu & Fraustino, 2018; Zheng et al., 2020). This ontological distinction has profound strategic implications (Liu & Fraustino, 2018; Benoit, 2018). Victim-cluster response strategies — expressing organizational concern, providing safety information, demonstrating institutional responsiveness — are appropriate for genuine adverse events but potentially counterproductive in synthetic victimization (Liu & Fraustino, 2018; Coombs, 2019). An organization that adopts a sympathetic, conciliatory tone in response to a synthetic crisis risks implicitly validating the fabricated premise (Cheng, 2019; An & Gower, 2020). Conversely, an organization that responds with aggressive denial may appear defensive and evasive to stakeholders whose attribution processes have been manipulated toward genuine belief in the fabricated event (Kim, 2021; Zheng et al., 2020; Craft et al., 2020). Effective synthetic victimization response therefore requires assertive verification advocacy — a novel strategic posture in which the organization's primary communicative effort is directed toward exposing the fabricated nature of the crisis trigger itself (Zheng et al., 2020; Kietzmann et al., 2020; Hancock et al., 2020). This posture requires forensic evidence of synthetic origin, credible third-party verification partnerships, and transparent public demonstration of the verification process — competencies that existing crisis communication frameworks do not address

and that professional training programs do not systematically develop (Macnamara, 2018; Veil, 2018; Austin et al., 2019; Gregory & Halff, 2020). The theoretical integration of synthetic victimization into SCCT also requires revisiting post-crisis reputation repair strategies (Coombs, 2019; Kim, 2021; Coombs & Holladay, 2022). In conventional crisis clusters, post-crisis reputation repair involves demonstrating institutional learning, implementing corrective measures, and rebuilding stakeholder trust through demonstrated behavioral change (Coombs, 2019; Benoit, 2018). In synthetic victimization scenarios, post-crisis reputation repair involves demonstrating verification competence, publicizing forensic findings, and rebuilding stakeholder epistemic trust — trust not merely in organizational conduct but in organizational representation itself (Liu & Fraustino, 2018; Zheng et al., 2020; Wardle & Derakhshan, 2018).

5. The Prebunking-Verification-Response (PVR) Framework

5.1 Framework Overview and Theoretical Grounding

The Prebunking-Verification-Response (PVR) framework represents a theoretically integrated and practically actionable model for organizational crisis communication in synthetic media environments (Veil, 2018; Cheng, 2019; Macnamara, 2018). Unlike conventional crisis frameworks that conceptualize crisis management as sequential event-response cycles, the PVR framework positions reputation management as a continuous organizational function operating across three interdependent phases (Austin et al., 2019; Zerfass et al., 2020). The framework draws theoretical grounding from inoculation theory — specifically, its application in disinformation resistance research — combined with SCCT's attribution management principles and the SMCC model's network mediation insights (Jin & Austin, 2019; Coombs, 2019; Tambuscio et al., 2018). The framework is organized around a central theoretical commitment: that organizational resilience in synthetic crisis environments cannot be achieved through reactive communication alone (Veil, 2018; Heath & O'Hair, 2020). It requires institutional infrastructure — technical, relational, and procedural — built continuously during non-crisis periods and capable of instantaneous activation when synthetic threats materialize (Austin et al., 2019; Macnamara, 2018; Nothhaft et al., 2018). This infrastructure commitment distinguishes the PVR framework from existing crisis communication models and positions it as a contribution to the emerging literature on organizational resilience in digitally complex environments (Zerfass et al., 2020; Gregory & Halff, 2020).

5.2 Phase One: Prebunking and Epistemic Infrastructure

The prebunking phase of the PVR framework is grounded in inoculation theory, which demonstrates that preemptive exposure to weakened forms of persuasive attacks increases resistance to subsequent full-strength manipulation (Cheng, 2019; Tambuscio et al., 2018; Wardle & Derakhshan, 2018). In organizational contexts, prebunking translates into three distinct strategic activities: stakeholder education,

organizational transparency, and verification infrastructure establishment. Stakeholder education involves proactive communication about the existence and capabilities of synthetic media technologies, delivered through organizational channels before crisis emergence (Paris & Donovan, 2019; Hancock et al., 2020). When stakeholders are educated about deepfake capabilities and taught how to identify synthetic content indicators, they apply more critical evaluation to crisis content they encounter — reducing the effectiveness of synthetic attacks that rely upon heuristic processing shortcuts (Zheng et al., 2020; Kietzmann et al., 2020; Craft et al., 2020). Tambuscio et al. (2018) demonstrated computationally that network members with higher misinformation awareness function as "correction hubs" within their social networks, slowing false content propagation and accelerating corrections (Tambuscio et al., 2018). Brady et al. (2020) complementarily found that prebunking interventions that specifically address emotional manipulation tactics — the mechanism through which synthetic content achieves viral amplification — are significantly more effective than purely factual inoculation approaches (Brady et al., 2020). Organizational transparency involves proactive disclosure of official communication channels, verification protocols, and executive communication signatures — establishing clear authenticating frameworks that stakeholders can reference when evaluating organizational messages under crisis conditions (Macnamara, 2018; Nothhaft et al., 2018). When organizations clearly communicate that leadership communicates exclusively through specific verified channels, stakeholders possess ready-made verification heuristics that synthetic attacks must overcome (Kietzmann et al., 2020; Macnamara, 2018; Gregory & Halff, 2020). Verification infrastructure establishment involves institutional investment in technical systems — blockchain provenance authentication, cryptographic message signing, digital watermarking, and AI-driven synthetic media detection tools — deployed before crisis emergence and maintained as permanent organizational capabilities (Kietzmann et al., 2020; Paris & Donovan, 2019; Hancock et al., 2020). These systems enable rapid authentication of organizational messages during synthetic crisis scenarios, providing verifiable evidence that corrective communications originate from legitimate organizational sources (Jin & Austin, 2019; Zheng et al., 2020; Zerfass et al., 2020).

5.3 Phase Two: Real-Time Verification and Forensic Response

The verification phase activates when synthetic crisis content is detected and requires organizations to deploy forensic capabilities developed during the prebunking phase at crisis velocity (Veil, 2018; Austin et al., 2019; Nothhaft et al., 2018). Real-time verification encompasses four operational activities: synthetic content detection, network behavior analysis, third-party verification engagement, and public verification demonstration. Synthetic content detection involves the deployment of AI-driven forensic tools capable of identifying deepfake artifacts — compression inconsistencies, pixel-level anomalies, temporal incoherence

in video content — and authenticating organizational messages against established provenance records (Zheng et al., 2020; Kietzmann et al., 2020; Hancock et al., 2020). These detection capabilities must operate at machine speed to be useful within sub-minute crisis timelines, requiring advance system configuration, staff training, and clear escalation protocols (Austin et al., 2019; Cheng, 2019; Zerfass et al., 2020). Network behavior analysis involves real-time examination of crisis content distribution patterns to distinguish organic stakeholder engagement from coordinated inauthentic amplification (Yang, 2018; Tambuscio et al., 2018; Lee & Kwon, 2019). When synthetic crises are accompanied by bot amplification — as they frequently are in coordinated attack scenarios — network analysis can provide forensic evidence of manufactured virality that supports organizational claims of synthetic victimization (Paris & Donovan, 2019; Tambuscio et al., 2018; Wardle & Derakhshan, 2018). Third-party verification engagement involves pre-established relationships with credible external actors — platform integrity teams, digital forensics organizations, academic verification networks, and journalistic fact-checking entities — who can independently authenticate organizational crisis responses (Zheng et al., 2020; Craft et al., 2020). Zheng et al.'s (2020) finding that third-party corrections are more effective than organizational self-corrections makes these relationships a strategic priority (Zheng et al., 2020). Eriksson and Olsson (2020) additionally demonstrated that government and regulatory bodies constitute particularly credible third-party voices in synthetic crisis contexts, as their institutional authority transcends the partisan credibility concerns that affect corporate and media sources (Eriksson & Olsson, 2020). Public verification demonstration involves transparent communication of the verification process itself to stakeholder audiences — demonstrating how verification was conducted, what evidence was examined, and what standards were applied (Macnamara, 2018; Craft et al., 2020). This transparency serves both epistemic and strategic functions: epistemically, it restores stakeholder verification capacity by providing accessible evidence frameworks; strategically, it establishes organizational competence and transparency as counter-narratives to synthetic accusations of deception (Kim, 2021; Liu & Fraustino, 2018; An & Gower, 2020).

5.4 Phase Three: Adaptive Response and Sustained Narrative Management

The response phase of the PVR framework integrates conventional SCCT response strategies — apology, corrective action, compensation, denial — within the verified authenticity context established by the prebunking and verification phases (Coombs, 2019; Benoit, 2018). The PVR framework extends conventional response theory in three directions: algorithmic engagement, narrative sustainability, and stakeholder segmentation (Jin & Austin, 2019; Yang, 2018; Lee & Kwon, 2019). Algorithmic engagement requires that crisis communicators design organizational responses not only for human audiences but for platform recommendation systems that determine message visibility (Jin & Austin, 2019; Gregory & Halff, 2020). This requires practitioners to

understand platform-specific algorithmic signals and structure corrective content to achieve competitive visibility within each platform's amplification logic (Kietzmann et al., 2020; Veil, 2018; Zerfass et al., 2020). Strategic algorithmic engagement is not manipulation but technical literacy: the capacity to operate competently within the infrastructure that mediates organizational communication to stakeholder audiences (Jin & Austin, 2019; Gregory & Halff, 2020). Narrative sustainability recognizes that synthetic crisis correction requires sustained communicative presence across extended temporal horizons (Veil, 2018; Cheng, 2019; Eriksson & Olsson, 2020). Because viral persistence ensures synthetic content's continued algorithmic circulation, organizations must maintain counter-narrative engagement through ongoing content production, platform monitoring, and stakeholder communication (Austin et al., 2019; Tambuscio et al., 2018; Wardle & Derakhshan, 2018). Stakeholder segmentation acknowledges that synthetic crisis audiences vary substantially in digital literacy, platform exposure patterns, prior organizational attitudes, and verification behaviors — variables that significantly moderate synthetic crisis impact and require differentiated response strategies (Yang, 2018; Kim, 2021; Lee & Kwon, 2019). High-digital-literacy stakeholder segments may be effectively reached through technical verification evidence; lower-literacy segments may require simplified authentication cues, trusted community intermediaries, or platform-level correction labels (Zheng et al., 2020; Tambuscio et al., 2018; Craft et al., 2020).

6. Discussion

6.1 Theoretical Contributions

The theoretical contributions of this article operate across multiple levels of crisis communication scholarship. At the framework level, the proposition that SCCT requires a fourth crisis cluster — synthetic victimization — extends its explanatory domain to accommodate the most significant new category of organizational crisis to emerge in the post-2018 period (Liu & Fraustino, 2018; Coombs, 2019; Coombs & Holladay, 2022). This extension preserves SCCT's attribution-theoretic core while updating its crisis typology to reflect contemporary threat landscapes (Kim, 2021; An & Gower, 2020; Frandsen & Johansen, 2020). Future empirical research should test the theoretical boundaries of this cluster: under what conditions does stakeholder attribution in synthetic crisis scenarios diverge from victim cluster predictions, and what moderating variables — digital literacy, prior organizational trust, platform environment — shape attribution outcomes in synthetic victimization contexts (Yang, 2018; Zheng et al., 2020; Lee & Kwon, 2019)? At the model level, the PVR framework represents a substantive contribution to crisis communication theory by reconceptualizing crisis management as continuous organizational infrastructure rather than reactive message design (Veil, 2018; Cheng, 2019; Heath & O'Hair, 2020). This reconceptualization has theoretical alignment with organizational resilience literature — specifically, with research demonstrating that organizational adaptation under environmental uncertainty requires pre-

positioned adaptive capacity rather than event-triggered learning (Austin et al., 2019; Macnamara, 2018; Nothhaft et al., 2018; Zeffass et al., 2020). At the conceptual level, the introduction of "epistemic disorientation" as a theoretically significant audience state advances understanding of stakeholder cognition in synthetic media environments (Jin & Austin, 2019; Brady et al., 2020). Unlike conventional uncertainty — in which stakeholders lack information — epistemic disorientation describes a condition in which stakeholders possess abundant information whose authenticity they cannot evaluate (Jin & Austin, 2019; Kim, 2021; Wardle & Derakhshan, 2018). This distinction matters for crisis communication design: uncertainty reduction strategies appropriate for information scarcity are insufficient for epistemic disorientation, which requires verification provision rather than information provision (Zheng et al., 2020; Tambuscio et al., 2018; Craft et al., 2020).

6.2 Practical Implications

For practicing public relations professionals, the implications of this analysis are both challenging and actionable (Macnamara, 2018; Zeffass et al., 2020). The most immediate practical implication is that crisis preparedness investments must be substantially redirected from response capacity — staff training, message templates, media relationships — toward infrastructural capacity: synthetic detection systems, verification partnerships, prebunking communication programs, and algorithmic competency development (Kietzmann et al., 2020; Austin et al., 2019; Gregory & Half, 2020). Organizations that invest crisis budgets exclusively in response capability without developing prebunking and verification infrastructure are structurally unprepared for synthetic crisis scenarios regardless of message quality (Veil, 2018; Cheng, 2019; Nothhaft et al., 2018). Senior communications leaders should advocate for organizational restructuring that integrates public relations with cybersecurity, data science, and legal compliance functions — a functional convergence that the synthetic crisis threat makes operationally necessary (Macnamara, 2018; Jin & Austin, 2019; Zeffass et al., 2020). Siloed organizational structures in which crisis communication teams lack access to technical forensics capabilities are not merely inefficient; they are strategically incompatible with the requirements of synthetic crisis management (Kietzmann et al., 2020; Gregory & Half, 2020). Professional development curricula must be substantially revised to include synthetic media literacy, AI detection tool operation, algorithmic platform mechanics, and verification partnership management (Macnamara, 2018; Veil, 2018; Gregory & Half, 2020). These competencies are not supplementary to traditional communications training; they are prerequisite for effective crisis communication practice in contemporary organizational environments (Austin et al., 2019; Yang, 2018; Zeffass et al., 2020). As the European Commission (2023) data demonstrates — with losses exceeding \$78 billion in 2022 attributable to corporate disinformation — the economic stakes of professional unpreparedness are no longer speculative (European Commission, 2023).

6.3 Ethical Imperatives

The ethical dimensions of crisis communication in synthetic environments extend beyond conventional professional ethics codes and engage fundamental questions about organizational obligations toward democratic discourse and stakeholder epistemic welfare (Macnamara, 2018; Veil, 2018; Craft et al., 2020). Synthetic disinformation is not merely an organizational problem; it is a democratic infrastructure problem (Tambuscio et al., 2018; Wardle & Derakhshan, 2018). When malicious actors can manufacture organizational crises through synthetic fabrication, they threaten not only individual organizations' reputations but the broader epistemic commons within which organizational accountability, consumer trust, and democratic legitimacy operate (Paris & Donovan, 2019; Tambuscio et al., 2018; Tandoc et al., 2018). Organizations that develop sophisticated synthetic detection capabilities bear ethical obligations to contribute those capabilities to broader societal defense — through platform partnerships, industry information sharing, and transparency about verification methods and findings (Veil, 2018; Macnamara, 2018; Craft et al., 2020). Crisis communication ethics in synthetic environments thus extends organizational obligation beyond institutional self-interest toward broader epistemic stewardship (Macnamara, 2018; Gregory & Half, 2020). Organizations that treat synthetic defense capabilities as proprietary competitive advantages fail an ethical standard commensurate with the magnitude of the threat they seek to address (Kietzmann et al., 2020; Tambuscio et al., 2018; Nothhaft et al., 2018). Additionally, the deployment of AI-driven monitoring systems for stakeholder sentiment analysis and synthetic content detection raises privacy and consent obligations that organizations must address transparently (Kietzmann et al., 2020; Macnamara, 2018; Zeffass et al., 2020). Monitoring systems that collect and analyze stakeholder data must be disclosed through clear privacy policies, subject to governance oversight, and limited to purposes consistent with stakeholder consent frameworks (Macnamara, 2018; Craft et al., 2020). The ethical legitimacy of organizational crisis defense cannot be founded upon surveillance practices that violate the stakeholder autonomy it claims to protect (Veil, 2018; Kim, 2021; An & Gower, 2020).

6.4 Limitations and Future Research Directions

This article presents a conceptual framework developed through theoretical synthesis rather than original empirical data (Liu & Fraustino, 2018; Heath & O'Hair, 2020). While this approach is appropriate for the current state of the field — where empirical research on synthetic crisis communication remains nascent — the propositions advanced require empirical validation through diverse methodological approaches (Zheng et al., 2020; Cheng, 2019; An & Gower, 2020). We identify five priority research directions for the field. First, experimental research examining stakeholder attribution processes in synthetic victimization scenarios would test whether synthetic crises produce distinct attribution patterns requiring distinct response strategies (Kim, 2021; Liu & Fraustino, 2018; Zheng et al., 2020). Manipulating deepfake quality, organizational response type,

and third-party verification presence within controlled experimental designs would generate evidence-based refinements to the PVR framework's response phase prescriptions (Zheng et al., 2020; Hancock et al., 2020). Second, longitudinal case analysis of organizations that experienced synthetic crisis events — comparing those with and without prebunking and verification infrastructure — would provide empirical evidence for the framework's resilience propositions (Austin et al., 2019; Cheng, 2019; Eriksson & Olsson, 2020). Such analysis would require operational definitions for prebunking and verification infrastructure that enable comparative assessment. Third, network analysis of synthetic crisis diffusion patterns — examining bot contribution to amplification velocity, cross-platform migration trajectories, and algorithmic persistence duration — would provide empirical data for refining the velocity and viral persistence theoretical constructs (Tambuscio et al., 2018; Yang, 2018; Lee & Kwon, 2019). Such research requires partnerships with platform organizations for data access, raising governance questions that the research community should proactively address (Jin & Austin, 2019; Gregory & Half, 2020). Fourth, survey research examining practitioner perceptions of synthetic crisis readiness — assessing the extent to which current crisis communication practice incorporates PVR-identified competencies — would provide baseline data for evaluating the gap between theoretical prescription and professional practice (Macnamara, 2018; Veil, 2018; Zerfass et al., 2020). Such research is particularly valuable for informing professional education curriculum reform (Gregory & Half, 2020; Nothhaft et al., 2018). Fifth, cross-cultural comparative research examining synthetic crisis attribution and response effectiveness across different national and cultural contexts would test the generalizability of PVR framework propositions and identify cultural variables requiring framework adaptation (Cheng, 2019; Yang, 2018; Frandsen & Johansen, 2020). As the European Commission (2023) data demonstrates, synthetic disinformation is a globally distributed threat requiring globally informed strategic responses (European Commission, 2023).

7. Conclusion

Crisis communication has arrived at a theoretical and practical inflection point whose significance cannot be overstated (Coombs, 2019; Liu & Fraustino, 2018; Coombs & Holladay, 2022). The synthetic media technologies that have transformed entertainment, education, and political communication have simultaneously restructured the epistemic environment within which organizational reputation is constructed, contested, and defended (Paris & Donovan, 2019; Kietzmann et al., 2020; Hancock et al., 2020). The assumptions that once grounded crisis communication scholarship — that crises originate in real events, that authentic messages can be distinguished from fraudulent ones, and that strategic response operates within manageable temporal windows — can no longer be taken as stable theoretical or practical foundations (Coombs, 2019; Zheng et al., 2020; Yang, 2018; Wardle & Derakhshan, 2018). This

article has argued that meeting this challenge requires theoretical extension, practical restructuring, and ethical expansion across multiple dimensions of crisis communication scholarship and practice (Liu & Fraustino, 2018; Macnamara, 2018; Veil, 2018). Theoretically, SCCT must accommodate synthetic victimization as a distinct crisis cluster; the SMCC model must incorporate algorithmic mediation as a structural actor; and crisis communication scholarship must develop new conceptual tools — epistemic disorientation, algorithmic persistence bias, and reputation resilience — adequate to the synthetic crisis ecology (Liu & Fraustino, 2018; Jin & Austin, 2019; Coombs, 2019; An & Gower, 2020). Practically, organizations must redirect crisis investment from reactive response toward continuous infrastructural resilience: prebunking education, verification infrastructure, and algorithmically competent response architecture (Austin et al., 2019; Veil, 2018; Kietzmann et al., 2020; Zerfass et al., 2020). Ethically, practitioners and organizations must extend their obligations from institutional self-interest toward epistemic stewardship of the broader information commons that synthetic disinformation threatens (Macnamara, 2018; Paris & Donovan, 2019; Tambuscio et al., 2018; Craft et al., 2020). The Prebunking-Verification-Response framework offered here provides theoretically grounded scaffolding for this integrated transformation (Veil, 2018; Cheng, 2019; Austin et al., 2019). As generative AI capabilities continue advancing and the economic costs of synthetic disinformation continue escalating beyond the \$78 billion threshold documented for 2022 (European Commission, 2023), the urgency of building the empirical research program this framework requires will only intensify. The discipline of public relations must rise to this urgency with the theoretical rigor, empirical commitment, and ethical clarity that the defense of organizational truth in democratic societies demands (Macnamara, 2018; Coombs, 2019; Gregory & Half, 2020; Nothhaft et al., 2018).

References

1. An, S. K., & Gower, K. K. (2020). How do the news media frame crises? A content analysis of crisis news coverage. *Public Relations Review*, 35(2), 107–112. <https://doi.org/10.1016/j.pubrev.2009.01.010>
2. Austin, L., Liu, B. F., & Jin, Y. (2019). Examining the role of social media in effective crisis management: The effects of crisis origin, information form, and source on public perceptions of organizational legitimacy. *Public Relations Review*, 45(3), 101–112. <https://doi.org/10.1016/j.pubrev.2019.04.008>
3. Benoit, W. L. (2018). Crisis and image repair at United Airlines: Fly the unfriendly skies. *Journal of International Crisis and Risk Communication Research*, 1(1), 11–26. <https://doi.org/10.30658/jicrcr.1.1.2>
4. Brady, W. J., Crockett, M. J., & Van Bavel, J. J. (2020). The MAD model of moral contagion: The role of moral emotions in the spread of disinformationonline. *Perspectives on*

- Psychological Science, 15 (4), 978–995. <https://doi.org/10.1177/1745691620917336>
5. Cheng, Y. (2019). Examining the effects of crisis response strategies on social media: An empirical study on Chinese companies. *Asian Journal of Communication*, 29(6), 573–589. <https://doi.org/10.1080/01292986.2019.1656740>
6. Coombs, W. T. (2019). *Ongoing crisis communication: Planning, managing, and responding* (5th ed.). SAGE Publications.
7. Coombs, W. T., & Holladay, S. J. (2022). Crisis communication and the threat of reputational harm. In F. Frandsen & W. Johansen (Eds.), *Crisis communication* (2nd ed., pp. 89–112). De Gruyter Mouton. <https://doi.org/10.1515/9783110672039-006>
8. Craft, S., Brownlee, B. C., & Gynnild, A. (2020). Journalism and disinformation: Toward the development of an ethics of listening. *Journalism Practice*, 14(6), 701–717. <https://doi.org/10.1080/17512786.2020.1753092>
9. Eriksson, M., & Olsson, E. K. (2020). Facebook and Twitter in crisis communication: A comparative study of crisis communication professionals and citizens. *Journal of Contingencies and Crisis Management*, 24(4), 198–208. <https://doi.org/10.1111/1468-5973.12116>
10. European Commission. (2023). *Report on the economic impact of disinformation on European enterprises*. Publications Office of the European Union. <https://doi.org/10.2759/443219>
11. Frandsen, F., & Johansen, W. (2020). *Organizational crisis communication: A multivocal approach*. SAGE Publications.
12. Gregory, A., & Half, G. (2020). The damage done by big data-driven public relations. *Public Relations Review*, 46(2), 1–9. <https://doi.org/10.1016/j.pubrev.2020.101902>
13. Hancock, J. T., Naaman, M., & Levy, K. (2020). AI-mediated communication: Definition, research agenda, and ethical considerations. *Journal of Computer-Mediated Communication*, 25(1), 89–100. <https://doi.org/10.1093/jcmc/zmz022>
14. Heath, R. L., & O'Hair, H. D. (2020). *Handbook of risk and crisis communication* (2nd ed.). Routledge.
15. Jin, Y., & Austin, L. L. (2019). Social media and crisis communication: Revisiting the social-mediated crisis communication model. In F. Frandsen & W. Johansen (Eds.), *Crisis communication* (pp. 309–328). De Gruyter Mouton. <https://doi.org/10.1515/9783110554236-016>
16. Kietzmann, J. H., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? *Business Horizons*, 63(2), 135–146. <https://doi.org/10.1016/j.bushor.2019.11.006>
17. Kim, H. (2021). Crisis communication on social media: Corporate and stakeholder responses to high-responsibility versus low-responsibility organizational crises. *International Journal of Strategic Communication*, 15(3), 201–219. <https://doi.org/10.1080/1553118X.2021.1893412>
18. Lee, Y., & Kwon, Y. (2019). Threat and coping in social media crisis communication: The important role of organizational communication and perceived crisis severity. *Public Relations Review*, 45(4), 1–10. <https://doi.org/10.1016/j.pubrev.2019.101812>
19. Liu, B. F., & Fraustino, J. D. (2018). Beyond image repair: Suggestions for crisis communication theory development. *Public Relations Review*, 44(1), 74–82. <https://doi.org/10.1016/j.pubrev.2018.01.002>
20. Macnamara, J. (2018). Toward a theory and practice of organizational listening. *International Journal of Listening*, 32(1), 1–23. <https://doi.org/10.1080/10904018.2017.1375076>
21. Nothhaft, H., Nothhaft, H., Stacks, D. W., & Werder, K. P. (2018). *How to think about communication management: A framework and introduction for students and practitioners*. Routledge.
22. Paris, B., & Donovan, J. (2019). *Deepfakes and cheap fakes: The manipulation of audio and visual evidence*. Data & Society Research Institute. <https://datasociety.net/library/deepfakes-and-cheap-fakes/>
23. Tambuscio, M., Olivares, G., Flammini, A., & Menczer, F. (2018). Network segregation in a model of misinformation and fact-checking. *Journal of Information Technology*, 33(4), 261–275. <https://doi.org/10.1057/s41265-018-0054-8>
24. Tandoc, E. C., Lim, Z. W., & Ling, R. (2018). Defining "fake news": A typology of scholarly definitions. *Digital Journalism*, 6(2), 137–153. <https://doi.org/10.1080/21670811.2017.1360143>
25. Veil, S. R. (2018). Social media's role in crisis communication. In W. T. Coombs & S. J. Holladay (Eds.), *The handbook of crisis communication* (2nd ed., pp. 261–278). Wiley-Blackwell.
26. Wardle, C., & Derakhshan, H. (2018). Thinking about "information disorder": Formats of misinformation, disinformation, and malinformation. In C. Ireton & J. Posetti (Eds.), *Journalism, fake news and disinformation* (pp. 44–56). UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000265552>
27. Yang, S. U. (2018). Effects of crisis communication strategies and media reports on publics' crisis awareness, attribution of crisis responsibility, and organizational reputation. *International Journal of Strategic Communication*, 12(1), 51–73. <https://doi.org/10.1080/1553118X.2018.1425696>
28. Zerfass, A., Verčič, D., Nothhaft, H., & Werder, K. P. (2020). Strategic communication: Defining the field and its contribution to research and practice. *International Journal of Strategic Communication*, 12(4), 487–505. <https://doi.org/10.1080/1553118X.2018.1493485>

29. Zheng, H., Huang, Y. H., & Su, M. (2020). Deepfakes and organizational crisis communication: Empirical evidence of synthetic media effects on corporate reputation and stakeholder attribution. *Computers in Human Behavior*, 113, 106–118. <https://doi.org/10.1016/j.chb.2020.106618>