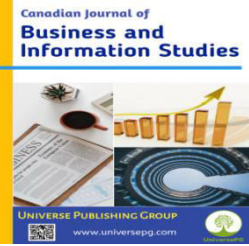




Publisher homepage: www.universepg.com, eISSN: 2663-7820

Canadian Journal of Business and Information Studies

Journal homepage: <http://www.universepg.com/journal/cjbis>



OPEN ACCESS | Research Article



Cognitive Warfare and the Limits of Classical Crisis Communication Models in an Environment of Manipulable Facts

Ali Hajizada Nizami* 

¹Sawol Communications Inc., Washington, USA

²Hajizade Group, Baku, Azerbaijan

*Correspondence: gd@hajizadegroup.com (Ali Hajizada Nizami, Sawol Communications Inc., Washington, USA and Hajizade Group, Baku, Azerbaijan).

Received Date: 10 July 2026

Accepted Date: 12 August 2026

Published Date: 19 August 2026

Abstract

The article examines why classical crisis communication models lose practical strength under conditions where evidence, attribution, and public judgment are exposed to synthetic manipulation. The study focuses on the transfer of cognitive influence practices from military and intelligence settings into corporate reputation management, executive protection, and stakeholder communication. Its novelty lies in treating deepfakes as an entry point into the wider field of cognitive warfare, where the attacker targets the audience's capacity to evaluate evidence, not a single message. The purpose is to explain why response-speed models become fragile when the factual basis of a crisis remains contested. The study draws on comparative source analysis, conceptual synthesis, and typological classification of ten recent academic sources. The analytical section identifies three shifts: from disinformation to cognitive manipulation, from speed to attribution logic, and from crisis reaction to cognitive resilience. The proposed framework supports corporate communication teams facing synthetic media, coordinated amplification, and trust erosion.

Keywords: Cognitive warfare, Crisis communication, Synthetic media, Corporate reputation, Disinformation.

1. Introduction

Crisis communication theory developed around situations where an organization faces reputational pressure after an operational failure, scandal, accusation, accident, data leak, leadership misconduct claim, organized information attack, or external disruption. The usual sequence presumes that the communicative task starts after the organization has established the relevant facts with enough confidence. Even under uncertainty, the working order remains recognizable: identify the incident, assess respon-

sibility, choose a response posture, address stakeholders, and correct false interpretations. Synthetic evidence and coordinated amplification disturb that order at the first step (Deppe & Schaal, 2024; Sabzevari *et al.*, 2024; van Diggelen *et al.*, 2025).

Deepfake video, cloned voice, AI-generated screenshots, fabricated documents, and automated narrative production have changed the evidentiary conditions of crisis work (Barrington *et al.*, 2025; van Diggelen *et al.*, 2025). Deepfakes remain the most

visible sign of that shift, although their practical danger extends beyond the fabrication of speech or behavior. They alter the setting in which journalists, investors, employees, regulators, and online audiences decide what counts as proof (Ahmed *et al.*, 2024; Schiff *et al.*, 2025). Once audio and video lose their former status as intuitive evidence, crisis communication teams cannot rely on rapid clarification as their main protective instrument (Barrington *et al.*, 2025; Deppe & Schaal, 2024).

The aim of this article is to explain why classical crisis communication models have limited explanatory and practical capacity in an environment of manipulable facts. Three research objectives guide the study. The first objective is to distinguish cognitive warfare from narrower categories of deepfake-based disinformation and reputational attack. The second objective is to identify why speed-centered crisis response becomes insufficient when the factual basis and source attribution of a crisis remain uncertain. The third objective is to develop corporate-oriented decision logic for communication professionals facing persistent cognitive attacks against brands, executives, and institutional trust.

The novelty of the article lies in shifting the analytical focus from deepfakes as isolated technological threats to cognitive warfare as a broader operational category. This shift allows crisis communication to be reconsidered as a system of attribution, verification, emotional stabilization, and stakeholder sense-making under adversarial pressure. The hypothesis states that crisis communication models built around rapid response to ascertainable facts lose practical effectiveness when adversaries manipulate the facts themselves, while attribution and cognitive resilience become more decisive than speed alone.

2. Methodology

The material base consists of ten academic sources published between 2022 and 2026. The search strategy covered Scopus-indexed and publisher-based databases, including SpringerLink, Frontiers, Cambridge Core, Taylor & Francis, Wiley Online Library, SAGE, and journal search platforms related to communication studies, information systems, security studies, psychology, and AI ethics. Search strings combined

“cognitive warfare,” “deepfakes,” “crisis communication,” “synthetic media,” “computational propaganda,” “cognitive bias,” “voice clones,” “liar’s dividend,” “strategic communication,” and “AI-enabled counter-measures.” Screening excluded works centered only on technical detection, general media literacy, electoral disinformation without crisis relevance, and normative commentary without conceptual or methodological value. A broader pool of recent publications was narrowed to ten sources covering four thematic groups: conceptual definitions of cognitive warfare, ethical and strategic criticism, cognitive bias in crisis information management, and synthetic media effects relevant to corporate and public communication (Ahmed *et al.*, 2024; Barrington *et al.*, 2025; Cosic *et al.*, 2026; Deppe & Schaal, 2024; Miller, 2023; Paulus *et al.*, 2024; Reczkowski & Adamski, 2025; Schiff *et al.*, 2025; van Diggelen *et al.*, 2025; Zilincik, 2026).

The study uses comparative analysis to separate deepfake incidents from cognitive warfare operations, source analysis to extract concepts relevant to crisis communication, conceptual synthesis to connect security studies with public relations theory, typologization to classify response limitations, and analytical generalization to formulate a corporate decision model. These methods correspond to the three objectives: definitional separation, critique of speed-centered response, and construction of an applied communication framework.

3. Results

Recent conceptual work describes cognitive warfare as influence directed at perception, judgment, belief, institutional trust, and decision-making. The NATO-oriented conceptual discussion treats the cognitive domain as a field where technology, behavioral science, information operations, and strategic communication intersect (Deppe & Schaal, 2024; Khan & Hossain, 2021). In crisis communication, this position shifts the object of crisis management. The organization deals with more than a harmful message, a false publication, or a hostile accusation. The attacker pressures the stakeholder’s ability to decide whether any denial, proof, expert statement, or executive message deserves confidence.

Ethical analysis of cognitive warfare connects computational propaganda, disinformation, institutional harm, and psychological manipulation within one conflict category (Miller, 2023). That connection matters for corporate communication because a reputational attack against an executive, brand, founder, or board does not need to convince every audience member that a fake video is true. It only needs to fragment confidence in the organization's communicative environment. Doubt becomes operationally useful. A company facing a synthetic scandal loses time while verifying the file and while explaining why verification itself deserves trust.

Deepfakes enter this structure as a practical trigger. Cross-national evidence on viral deepfakes reports that social media news use strengthens illusory truth effects, meaning that repeated exposure increases perceived credibility even when the material is false (Ahmed *et al.*, 2024). This finding changes the meaning of the first response window. In a classical crisis model, the opening phase usually turns into a race to frame the event. In a manipulable-fact environment, the opening phase turns into a race over evidentiary discipline. A premature denial without visible verification logic gives adversaries a second target: the organization's credibility as an evaluator of evidence.

Research on AI-powered voice clones sharpens the problem. Experimental evidence indicates that people are poorly equipped to detect cloned voices (Barrington *et al.*, 2025). For corporate and VIP protection, reputational exposure no longer belongs only to public video. Voice messages, phone calls, meeting audio, investor briefings, executive instructions, and internal recordings become plausible carriers of manipulation. The crisis team carries a double burden. It has to protect the public-facing reputation of the organization and the internal trust architecture through which employees decide whether instructions are genuine.

The "liar's dividend" adds another layer. Work on disinformation claims shows that public figures exploit the existence of manipulated media by dismissing authentic evidence as fake (Schiff *et al.*, 2025). This mechanism matters for crisis communication because

synthetic media changes both sides of the evidentiary problem. False content appears more credible, while genuine content becomes easier to deny. The crisis professional operates inside an evidentiary trap. If the organization confirms too slowly, the fake gains circulation. If it rejects too quickly, stakeholders suspect defensive evasion. If it provides technical proof, audiences with low trust in the institution distrust the proof provider.

Crisis information management research offers a bridge between classical uncertainty and cognitive warfare. An exploratory study of crisis information management reports that data bias and confirmation bias reinforce each other under urgency, producing path dependencies in decision-making (Paulus *et al.*, 2024). This finding matters because crisis teams under synthetic attack often inherit biased data streams from social platforms, media monitoring tools, screenshots, reposts, anonymous accounts, and emotionally saturated stakeholder reactions. Speed under these conditions does not always reduce reputational damage. It sometimes accelerates the organization's dependence on distorted inputs.

A comparison of the cognitive warfare literature with crisis information management produces a sharper conclusion. The conceptual account by Deppe and Schaal explains why cognitive warfare targets sense-making at individual and collective levels (Deppe & Schaal, 2024). The ethical account by Miller clarifies why institutional harm and freedom of communication create moral limits for countermeasures (Miller, 2023). The crisis information management study by Paulus and colleagues shows why urgency and bias damage information products inside crisis organizations (Paulus *et al.*, 2024). Together, these positions indicate that crisis response cannot be reduced to a communication output. It begins earlier, with disciplined production of a verified internal picture.

The skeptical perspective on cognitive warfare protects the argument from conceptual inflation. Strategic theory and affective-science criticism warn that the term "cognitive warfare" risks overuse, especially when analysts describe every form of non-violent information aggression as war (Zilincik, 2026). This critique has direct value for a corporate article

because business communication does not need weaponized language for every reputational disturbance. The concept has analytical value only where the attack shows persistence, adversarial coordination, manipulation of evidence, emotional targeting, and an intention to degrade judgment. A single fake post, even a harmful one, does not automatically constitute cognitive warfare.

The same skeptical work proposes that information aggression is often better understood through emotion-centered subversion (Zilincik, 2026). This observation aligns with recent work on emotionally based strategic communications, which describes defensive communication as a structured process for sensing emotional climates, designing legitimate messages, evaluating impact, and adapting under human supervision (Coscic *et al.*, 2026). For crisis communication, the implication is precise. A synthetic attack is rarely resolved through fact correction alone. Anger, humiliation, fear, distrust, and resentment shape whether factual correction receives acceptance.

Religious and anthropological discussion of cognitive warfare expands the focus from information exposure to the protection of human judgment, autonomy, and moral agency (Reczkowski & Adamski, 2025). Its disciplinary setting differs from corporate com-

munication, yet its treatment of cognitive warfare as an attack on perception, decision-making, and belief formation helps explain business risks. In a corporate setting, the same structure appears in less dramatic form. Investors hesitate, employees doubt internal instructions, partners suspend cooperation, journalists wait for forensic confirmation, and audiences reinterpret older evidence through the lens of the synthetic incident.

AI-enabled countermeasure research introduces the operational layer. The proposed idea of advanced persistent manipulators describes coordinated human-machine influence systems capable of extended multimedia attacks, while defensive counter-systems require human control, harm minimization, and value balancing (van Diggelen *et al.*, 2025).

This perspective is especially relevant for corporate communication because a firm cannot answer automated manipulation with improvised statements alone. It needs a governed system combining monitoring, forensic escalation, legal review, executive authentication, stakeholder mapping, and communication authority. **Table 1** arranges the resulting shift from classical crisis response to cognitive-warfare-oriented crisis communication.

Table 1: Shift from classical crisis communication to cognitive-warfare-oriented crisis response (adapted by the author based on Coscic *et al.*, 2026; Deppe & Schaal, 2024; Paulus *et al.*, 2024; van Diggelen *et al.*, 2025).

Classical crisis communication	Transitional pressure	Cognitive-warfare-oriented response
Incident is treated as an event with recoverable facts	Synthetic content distorts the evidentiary base	Facts are verified through forensic, procedural, and source-based attribution
Speed of response dominates early crisis logic	Fast denial risks strengthening distrust	Response timing follows verification thresholds and stakeholder risk
Message correction addresses false claims	Repetition, emotion, and platform dynamics sustain belief	Correction is paired with emotional stabilization and channel-specific containment
Communication team manages reputation	Attack targets judgment, trust, and decision capacity	Cross-functional cell integrates communication, security, legal, intelligence, and executive authentication
Trust restoration follows clarification	Authentic evidence remains vulnerable to denial	Trust depends on visible verification routines and pre-established credibility infrastructure

The model is adapted from recent conceptual and countermeasure work on cognitive warfare, AI-enabled manipulation, emotional targeting, and crisis information bias (Cosic *et al.*, 2026; Deppe & Schaal, 2024; Paulus *et al.*, 2024; van Diggelen *et al.*, 2025). The table clarifies why the classical model weakens in a synthetic-evidence environment. Its weak point is its treatment of speed as the first operational virtue before the evidentiary ground has been stabilized. Once adversaries manipulate the fact base, speed without attribution becomes a reputational hazard.

The comparison across sources leads to three findings. First, deepfakes are best treated as instruments within a broader cognitive operation when they are combined with amplification, ambiguity, emotional targeting, and institutional distrust. Second, attack attribution becomes a strategic variable because the organization's response depends on whether the incident is a hoax, fraud, parody, insider leak, coordinated smear, geopolitical influence operation, or adversarial business attack. Third, corporate crisis communication requires a resilience layer that precedes the crisis: verified executive channels, media-forensic partnerships, authentication protocols, scenario training, and stakeholder education.

Classical models still retain utility for structuring responsibility, apology, corrective action, stakeholder segmentation, and message consistency. Their limits appear when they presume that the organization and audience are debating the interpretation of a shared reality. Cognitive warfare removes that shared ground. The practical communication problem then precedes persuasion. The organization first has to help stakeholders understand how reality is being tested, verified, and protected.

4. Discussion

The findings support a revision of crisis communication practice. A company exposed to synthetic media or coordinated narrative manipulation needs a decision architecture that separates four questions before selecting a public message: what happened, whether the evidence is authentic, who benefits from circulation, and which stakeholder group is most vulnerable at the current stage. Classical crisis

manuals usually answer the first question and move quickly toward response posture. In cognitive attack conditions, the second and third questions determine whether any posture will remain credible.

The proposed implementation model begins before the crisis. Organizations with high public visibility need an evidence-readiness layer. This layer contains verified executive communication channels, pre-agreed authentication procedures for voice and video, a registry of official accounts, media-forensic contacts, and escalation rules for suspected synthetic content, and internal drills that train teams to pause without appearing evasive. The practical aim is to prevent the first public statement from turning into an uncontrolled experiment in trust.

During the first response window, the communication team needs to avoid two failures. The first failure is emotional silence, where the organization waits for perfect technical certainty while stakeholders experience fear, anger, or suspicion. The second failure is evidentiary over claiming, where the organization declares content fake before it has a defensible basis. A stronger response separates emotional acknowledgment from factual determination. The organization states what is known, what remains under verification, which channels carry authority, and when the next update will follow. This preserves pace without pretending that all facts have already been secured. **Table 2** compares the operational limits of classical crisis communication with the requirements of a cognitive-warfare-oriented model. The comparison clarifies what changes inside the crisis team's decision process.

The table indicates that crisis communication under cognitive attack turns into evidentiary governance. The communication department remains central, but it cannot operate as the sole decision unit. Security teams, legal advisers, digital forensics specialists, executive offices, investor relations, and HR communication require a shared escalation protocol. Fragmentation creates the main managerial risk: one unit verifies the media file, another prepares a public statement, a third briefs employees, and a fourth contacts regulators. Contradictions between these tracks give adversaries usable material.

Table 2: Limits of classical crisis communication models under manipulable-fact conditions (compiled by the author based on Deppe and Schaal, 2024; Miller, 2023; Paulus *et al.*, 2024; van Diggelen *et al.*, 2025; Zilincik, 2026).

Crisis communication element	Classical model logic	Limit under manipulable facts	Required modification
Initial diagnosis	Identify incident and reputational exposure	Incident evidence itself is unstable	Establish verification status before message posture
Response speed	Early response protects credibility	Fast denial without attribution increases suspicion	Use staged response with time-bound updates
Stakeholder mapping	Segment audiences by relationship to organization	Audiences differ by susceptibility to manipulation and emotional activation	Add cognitive vulnerability and channel exposure mapping
Message correction	Refute false claims with facts	Facts are contested, fabricated, or dismissed	Combine correction with proof-chain explanation
Spokesperson authority	Senior figure reassures stakeholders	Executive image and voice are targets of imitation	Use authenticated channels and identity confirmation
Monitoring	Track media and social reaction	Coordinated amplification distorts perceived salience	Separate organic concern from adversarial amplification
Reputation repair	Restore trust after clarification	Clarification does not end doubt when proof is manipulable	Build repeated verification routines and external validation
Ethical control	Avoid deceptive communication	Defensive AI tools risk overreach	Preserve human authorization and proportionality

Workable decision logic has five stages. The first stage is signal capture, where the organization records the earliest version of the content, the first visible accounts, reposting patterns, and initial stakeholder reactions. The second stage is verification triage, where the team classifies the case as confirmed authentic, likely manipulated, unclear, or non-assessable with available evidence. The third stage is attribution assessment, where intent, origin, coordination, and beneficiary logic are examined. The fourth stage is stakeholder containment, where internal and external groups receive calibrated updates through authenticated channels. The fifth stage is resilience review, where the organization evaluates which trust mechanisms failed or held.

Monitoring metrics need to move beyond reach, sentiment, and share of voice. Cognitive warfare conditions require indicators that reflect evidentiary instability and stakeholder judgment. Suitable metrics include time to verification status, number of authoritative-channel visits, employee compliance with authentication protocols, proportion of media reports using verified language, recurrence of debunked claims, platform migration of the narrative, stakeholder confusion in inbound inquiries, and executive impersonation attempts. These indicators do not replace reputational metrics. They explain whether the organization is regaining control over the conditions under which reputation is judged. **Table 3** presents an applied response matrix for corporate communication teams. It links the type of synthetic or

cognitive attack with the response priority, organizational owner, and communication output.

Table 3: Corporate response matrix for cognitive attacks against reputation and trust (compiled by the author based on Ahmed *et al.*, 2024; Barrington *et al.*, 2025; Cosic *et al.*, 2026; Reczkowski and Adamski, 2025; Schiff *et al.*, 2025).

Attack type	Primary risk	Response priority	Lead function	Communication output
Authentic evidence dismissed as fake	Accountability erosion, distrust spiral	Protect proof chain	Legal, compliance, communications	Evidence statement with independent validation
Coordinated narrative amplification	Manufactured consensus, stakeholder pressure	Identify the amplification pattern	Intelligence, communications, legal	Stakeholder briefing separating verified facts from circulation claims
Cross-platform impersonation	Channel confusion, loss of authority	Reassert official communication map	Digital, communications, security	Authenticated channel notice and account registry
Emotionally targeted rumor	Fear, anger, employee instability	Stabilize audience emotion	HR communication and corporate affairs	Empathic update with practical guidance
Executive voice clone	False instruction, fraud, internal panic	Confirm identity and freeze unauthenticated requests	Security and executive office	Internal alert through verified channels
Persistent cognitive attack	Trust fatigue, long-term reputational erosion	Build a resilience cell	Executive leadership	Periodic verified briefings and post-incident learning report
Synthetic video scandal	Reputation damage, media acceleration	Preserve evidence and verify authenticity	Communications and digital forensics	Public holding statement with verification timeline

The response matrix indicates that the central practical decision concerns the type of uncertainty the organization faces. A voice-clone fraud requires internal containment before public explanation. A synthetic video scandal requires forensic preservation before reputational framing. A coordinated amplification campaign requires pattern diagnosis before broad denial. A liar's-dividend situation requires proof-chain protection because the threat comes from the denial of authentic evidence.

The author's position is that crisis communication in this environment needs a restrained but firmer epis-

temic function. Communication professionals are not forensic engineers, intelligence officers, or legal investigators. They still carry responsibility for translating verification procedures into language that stakeholders understand. This translation task has ethical weight. Over technical statements alienate audiences.

Emotional messaging without proof weakens credibility. Excessive secrecy generates suspicion. The most defensible position combines limited claims, visible process, authenticated channels, and repeated updates.

Training requires revision as well. Crisis simulations need to contain ambiguous synthetic evidence, competing expert opinions, emotionally charged stakeholder groups, and coordinated amplification by accounts with unclear origins. Teams need practice in saying “verification is underway” without sounding passive. They need templates for evidence-status language, not only apology, denial, correction, and reassurance. Executive media training has to cover authentication routines, live verification practices, and protocols for compromised voice or video.

The corporate migration of cognitive operations creates another managerial implication. Reputation protection no longer belongs only to external communication. It intersects with cybersecurity, fraud prevention, executive protection, investor relations, and employee trust. A fake CEO video aimed at the market, a cloned voice aimed at finance staff, and a false leak aimed at journalists differ in channel and target, but share one operational structure: they exploit trust routines designed for a pre-synthetic media environment.

The proposed framework has an analytical limitation. It does not test the model through corporate cases, controlled experiments, or practitioner interviews. Its value lies in conceptual integration and decision design. Future empirical work would need to examine how communication teams perform under simulated cognitive attack, which verification phrases reduce stakeholder confusion, and how external validation affects trust recovery after synthetic incidents.

5. Conclusion

Cognitive warfare differs from isolated deepfake disinformation because it targets the audience’s capacity to judge evidence, assess institutions, and maintain coherent decision-making under pressure. Deepfakes operate as visible instruments inside a broader pattern built from synthetic media, amplification, emotional activation, attribution ambiguity, and erosion of trust. This distinction clarifies why a corporate crisis caused by manipulated content cannot be treated as a conventional reputational incident with a faster technical add-on. Classical crisis communication models retain value for organizing responsibility, stakeholder contact, message discipline, UniversePG | www.universepg.com

and reputational repair. Their limits appear when the crisis begins with unstable evidence. In such cases, response speed loses its privileged position. Attribution, verification status, proof-chain integrity, and emotional stabilization become decisive conditions for communication credibility. The hypothesis is confirmed: when facts themselves are manipulable, crisis communication based only on rapid response to established facts lose explanatory and practical force. The proposed corporate model replaces improvised denial with staged decision logic: signal capture, verification triage, attribution assessment, stakeholder containment, and resilience review. Its practical contribution lies in connecting communication work with evidentiary governance. Organizations that prepare authenticated channels, verification language, cross-functional escalation, and cognitive-resilience metrics are better positioned to withstand persistent attacks against executives, brands, and stakeholder trust.

6. Acknowledgment

The author has no acknowledgments to declare.

7. Conflicts of Interest

The author declares no conflicts of interest.

8. References

- Ahmed, S., Bee, A. W. T., Ng, S. W. T., & Masood, M. (2024). Social media news use amplifies the illusory truth effects of viral deepfakes: A cross-national study of eight countries. *J. of Broadcasting & Electronic Media*, 68(5), 778–805.
<https://doi.org/10.1080/08838151.2024.2410783>
- Barrington, S., Cooper, E. A., & Farid, H. (2025). People are poorly equipped to detect AI-powered voice clones. *Scientific Reports*, 15(1), 11004.
<https://doi.org/10.1038/s41598-025-94170-3>
- Ćosić, K., Popović, S., & Wiederhold, B. (2026). Emotionally based strategic communications as a new tool in defensive cognitive warfare. *Frontiers in Psychology*, 17, 1751406.
<https://doi.org/10.3389/fpsyg.2026.1751406>
- Deppe, C., & Schaal, G. S. (2024). Cognitive warfare: A conceptual analysis of the NATO ACT

- cognitive warfare exploratory concept. *Frontiers in Big Data*, 7, 1452129.
<https://doi.org/10.3389/fdata.2024.1452129>
- Khan MF., and Hossain MA. (2021). Cooperative spectrum sensing with selection diversity reception in cognitive radio, *Int. J. Mat. Math. Sci.*, 3(1), 1-7.
<https://doi.org/10.34104/ijmms.021.0107>
- Miller, S. (2023). Cognitive warfare: An ethical analysis. *Ethics and Information Technology*, 25(3), 46.
<https://doi.org/10.1007/s10676-023-09717-7>
- Paulus, D., Fathi, R., & Comes, T. (2024). On the interplay of data and cognitive bias in crisis information management: An exploratory study on epidemic response. *Information Systems Frontiers*, 26(2), 391–415.
<https://doi.org/10.1007/s10796-022-10241-0>
- Reczkowski, R., & Adamski, B. (2025). Cognitive warfare and religion: Weaponization of the human cognitive dimension. *Pastoral Psychology*.
<https://doi.org/10.1007/s11089-025-01290-8>
- Sabzevari P, Omidvar F, Nilab Z, and Azandaryani M. (2024). The influence of cognitive behavioral therapy on self-control, mental health, and mindfulness in women affected by intimate partner violence. *Eur. J. Med. Health Sci.*, 6(6), 189-200.
<https://doi.org/10.34104/ejmhs.024.01890200>
- Schiff, K. J., Schiff, D. S., & Bueno, N. S. (2025). The liar's dividend: Can politicians claim misinformation to evade accountability? *American Political Science Review*, 119(1), 71–90.
<https://doi.org/10.1017/S0003055423001454>
- van Diggelen, J., Aidman, E., Rowa, J., & Vince, J. (2025). Designing AI-enabled counter-measures to cognitive warfare.
<https://doi.org/10.48550/arXiv.2504.11486>
- Zilincik, S. (2026). Cognitive warfare: Some sceptical observations from general strategic theory and affective science. *European Journal of International Security*: 1–22.
<https://doi.org/10.1017/eis.2026.10057>

Citation: Nizami AH. (2026). Cognitive warfare and the limits of classical crisis communication models in an environment of manipulable facts, *Can. J. Bus. Inf. Stud.*, 8(4), 702-710.
<https://doi.org/10.34104/cjbis.026.07020710>

Copyright: © The Author(s), 2026. Published by the UniversePG. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution 4.0 License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution and reproduction in any medium, and provided the original work is properly cited. 