



Communication readiness as a core capability for societal resilience to cognitive warfare

Sara Russo, Serena Tagliacozzo, Juan Camilo Urazan Chinchilla & Lina Maria Manrique-Villanueva

To cite this article: Sara Russo, Serena Tagliacozzo, Juan Camilo Urazan Chinchilla & Lina Maria Manrique-Villanueva (19 Aug 2026): Communication readiness as a core capability for societal resilience to cognitive warfare, Defense & Security Analysis, DOI: [10.1080/14751798.2026.2714711](https://doi.org/10.1080/14751798.2026.2714711)

To link to this article: <https://doi.org/10.1080/14751798.2026.2714711>



© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 19 Aug 2026.



Submit your article to this journal [↗](#)



View related articles [↗](#)



View Crossmark data [↗](#)

Communication readiness as a core capability for societal resilience to cognitive warfare

Sara Russo ^{a,b}, Serena Tagliacozzo^c, Juan Camilo Urazan Chinchilla^d and Lina Maria Manrique-Villanueva^d

^aUniversity of Turin, Turin, Italy; ^bDepartment of Engineering, Economics, Politics and Law, Centre for High Defence Studies (CASD), Rome, Italy; ^cDepartment of Electronics, Information and Bioengineering, Politecnico di Milano, Milan, Italy; ^dCentro Regional de Estudios Estratégicos en Seguridad (CREES), Vicedirección de Investigaciones, Escuela Superior de Guerra “General Rafael Reyes Prieto, Bogotá, Colombia

ABSTRACT

Cognitive warfare exploits not only hostile narratives and disinformation, but the communicative vulnerabilities of targeted societies, including low institutional trust, fragmented sensemaking, and co-ordination failures. Although communication is increasingly seen as central to resilience and preparedness, how communication environments contribute to societal resilience remains underexplored. This paper addresses this gap by conceptualising communication readiness as a socio-cognitive capability of individuals, institutions, and societies to manage uncertainty, sustain trust, and enable co-ordinated sensemaking across cognitive, community, institutional, and societal levels under informational disruption. Drawing on an integrative review of cognitive warfare, risk communication, and societal resilience scholarship, the paper proposes a mechanism-based framework explaining how communication environments shape preparedness outcomes through exposure, interpretation, affective activation, social amplification, and behavioural and organisational response. The framework identifies communication readiness as a core dimension of civil preparedness and societal resilience, with implications for defence policy, preparedness planning, and resilience assessment in cognitively contested environments.

KEYWORDS

Cognitive warfare; civil preparedness; risk communication; hybrid threats; societal resilience; communication infrastructure

Introduction

Cognitive warfare is increasingly recognised as a central dimension of contemporary conflict, yet its analytical boundaries and operational implications remain unsettled.¹ Whilst strategic debates have progressively shifted from information operations towards cognitive effects, the prevailing literature continues to approach cognition primarily through the lenses of influence, manipulation, and psychological targeting.² This has led to a growing body of work focused on adversarial capabilities, how actors shape

CONTACT Sara Russo  sa.russo@unito.it; sara.russo@unicasd.it

© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

perceptions, exploit biases, and generate behavioural outcomes, whilst comparatively less attention has been devoted to the systemic vulnerabilities in the targeted society that make such influence possible.³ Within defence policy and practice, Strategic Communication (STRATCOM) has significantly contributed to integrating communication into contemporary security thinking, but it has often prioritised messaging and influence dimensions rather than the communicative conditions that shape societal resilience under uncertainty.⁴ This creates an important conceptual gap between communication as an instrument of influence and communication as a resilience-enabling capability.

In parallel, a distinct and well-established body of risk communication scholarship has developed within the field of crisis management, addressing how individuals and societies seek information during crises, process information, and how public institutions frame risk messages.⁵ This literature has demonstrated that communication is not merely a vehicle for transmitting information, but a critical infrastructure that shapes trust, co-ordination, and collective action in high stakes environments.⁶ Despite these insights, the connection between risk/crisis communication and cognitive warfare remains largely underexplored.

This disconnection is analytically significant. Cognitive warfare does not operate solely through the injection of misleading or manipulative content; it exploits pre-existing fragilities within societal systems such as low trust, ambiguity intolerance, fragmented narratives, and co-ordination failures.⁷ These fragilities can be minimised or redressed by capitalising on the lessons learned and illustrated within the realm of risk and crisis communication research.

Comprehensive security and total defence approaches developed in Nordic countries such as Finland and Sweden have filled many of these gaps by introducing concepts such as psychological defence⁸ which refer to the ability of the population to resist disinformation and influence operations.⁹ This focus reframed defence policy in terms of protecting collective cognition and ensuring cognitive security, shifting the attention from the act of influence/manipulation to the factors that enable societal resilience. Although closely related, these three constructs are analytically distinct: psychological defence denotes the societal-level capacity, developed within Nordic total defence doctrine, to resist and recover from information influence operations; cognitive resilience denotes the individual and group level capacity to sustain accurate perception and sound judgement under cognitively contested conditions; and cognitive security refers to the protection of the cognitive domain itself, the integrity of cognitive processes and decision-making across individuals, groups, and society. This is distinct from the protection of physical infrastructure, which lies outside all three constructs discussed here, and from societal functioning more broadly, which instead falls within the societal resilience construct developed throughout this article. These concepts therefore operate at different analytical levels rather than describing the same phenomenon under different names: societal resilience denotes the broadest, macro-level capacity; cognitive security specifies the domain to be protected; and psychological defence, developed within Nordic total defence doctrine, and offered here as the clearest existing societal-level analogue, and cognitive resilience denote, respectively, the societal and individual/group-level capacities through which that domain is protected. Communication readiness is proposed here as the cross-cutting communicative capability that underpins all of them. In particular the concept of communication readiness shifts the focus from militarised frameworks

typical of the cognitive warfare domain to a framework that emphasises readiness and preparedness constructed at multiple levels: individual, group/community, institutional and societal.

Building on this research stream, this paper conceptualises communication readiness as a core civil preparedness capability and communicative enabler of societal resilience to cognitive warfare. By integrating cognitive warfare, risk communication, and societal resilience scholarship, it develops an analytical framework that transfers established risk communication principles into the cognitive warfare domain and identifies implications for defence policy, resilience planning, and future research.

The paper proceeds in five steps. First, it reviews how communication is conceptualised across cognitive warfare, risk and crisis communication, and societal resilience (“what communication is”). Second, it maps these conceptualisations onto established communication theories to identify their primary communicative functions (“what communication does”). Third, it examines the levels at which communication operates (“where communication operates”). Fourth, it develops a mechanism-based framework explaining how communication shapes preparedness outcomes (“how communication produces outcomes”). Finally, it discusses implications for defence policy, civil preparedness, and future research.

Methodology

This article adopts an integrative conceptual review¹⁰ to develop the concept of communication readiness as a preparedness capability for cognitively contested environments. Unlike systematic reviews, which aim to synthesise empirical evidence addressing narrowly defined research questions, integrative reviews are designed to connect fragmented bodies of knowledge, reconcile different theoretical perspectives, and generate new conceptual frameworks. This approach is appropriate because communication readiness spans multiple disciplines that have largely evolved in parallel and lack a common analytical vocabulary.

The three literature streams were selected because they address complementary dimensions of communication under conditions of uncertainty and strategic competition. Cognitive warfare examines the strategic exploitation of communication, risk, and crisis communication focuses on uncertainty management and trust, and societal resilience considers communication as a condition for preparedness and adaptive capacity. Consistent with integrative review methodology, source selection was guided by theoretical relevance rather than exhaustive coverage. The cognitive warfare literature was informed by a recent bibliometric mapping of the field,¹¹ whilst the remaining literature was purposively selected from foundational academic contributions and authoritative institutional publications that explicitly addressed communication as a factor shaping preparedness, resilience, trust, co-ordination, or cognitive influence.

The analytical synthesis proceeded iteratively. First, the literature was examined to identify how communication is conceptualised within each research domain. Second, these conceptualisations were compared against established communication theories to identify common communicative functions. Third, communication was mapped across four interconnected levels of analysis (cognitive, community, institutional, and societal) to clarify where communicative vulnerabilities and preparedness capacities

emerge. Finally, recurring concepts and relationships were synthesised into five mechanisms, namely exposure, interpretation, affective activation, social amplification, and behavioural and organisational response, which together constitute the proposed communication readiness framework. The resulting framework is intended as a theory-building contribution that organises existing knowledge and provides a foundation for future empirical validation and operational application.

Conceptual analysis and integrative literature review

Cognitive warfare: communication as influence

The study of influence operations as an instrument of statecraft predates contemporary debates on cognitive warfare. Historical work on propaganda and psychological warfare shows that strategic actors shape beliefs and behaviour not through message truth or falsity alone, but by manipulating broader perceptual and communicative conditions, such as repetition, framing, selective emphasis, and informational saturation that narrow critical evaluation and deepen reliance on pre-structured narratives.¹² Cognitive warfare reformulates this logic as direct intervention on perception, attention, interpretation, and decision-making, treating influence operations as antecedent to what is now conceptualised more broadly as cognitive warfare.¹³ A convergent psychological strand shows why: prolonged exposure to threat and emotionally salient stimuli narrows attentional scope, heightens threat sensitivity, and reinforces in-group/out-group polarisation, leaving populations more vulnerable to simplified, emotionally charged narratives.¹⁴

The intersection between influence operations and the psychological ecology of conflict has been theorised most systematically through the concept of cognitive warfare. In this framework, the objective is not only to circulate information or even disinformation, but to shape the cognitive environment in which information is noticed, believed, remembered, and acted upon, thereby affecting the mental processes through which individuals and groups interpret reality.¹⁵ In other words, the process is much more systematic, long-lasting, and even far more subtle than the target audience can consciously perceive, to the extent that it no longer requires the use of language directly associated with violence. Studies of Russian disinformation and co-ordinated online manipulation have reinforced this interpretation by showing that strategic campaigns often seek less to persuade audiences of one coherent falsehood than to saturate, fragment, and destabilise the shared epistemic space on which collective judgment depends.¹⁶ In that sense, cognitive warfare names the strategic integration of influence operations with the psychological vulnerabilities intensified by conflict.

Empirically, the Russia-Ukraine conflict offers one of the clearest contemporary illustrations of this dynamic. Recent studies have documented biased information presentation, strategic framing, reflexive control, agenda influence, bot amplification, manipulated audiovisual content, and repeated narrative exposure across platforms and media ecosystems, all of which are consistent with attempts to shape perception, channel attention, and distort judgment.¹⁷ Survey and content-analysis research has also found reduced fact-checking accuracy, false-memory effects, attributional distortions, and the reinforcement of confirmation bias among exposed audiences, indicating that influence operations in this conflict are psychologically consequential rather than

merely informationally visible.¹⁸ Taken together, this evidence supports the argument that in contemporary war, influence operations, and psychological effects of conflict should be understood as mutually constitutive dimensions of cognitive warfare, by treating these as subordinate elements and framing the cognitive as a higher-order dimension, which constitutes a theoretical hypothesis put forward by the authors of this paper.

From a neuropsychological standpoint, this relationship becomes even clearer. Emotionally salient conflict messaging modulates large-scale networks linking prefrontal control systems with limbic and memory-related regions, which affects how subsequent information is encoded, prioritised, and evaluated under stress.¹⁹ Accordingly, messages designed to activate fear, outrage, or existential threat do not simply persuade; they affect the conditions under which subsequent information is interpreted and evaluated, reinforcing patterns of cognitive vulnerability and increasing susceptibility to strategic influence. This is precisely the move that distinguishes cognitive warfare from older labels such as propaganda or psychological operations: the target is no longer only opinion or morale, but the broader cognitive architecture through which conflict is perceived, interpreted, and acted upon.²⁰

Whilst cognitive warfare scholarship has extensively examined how strategic actors shape perceptions, amplify emotional responses, and destabilise epistemic environments, comparatively less attention has been devoted to the communicative conditions that make such vulnerabilities manageable or resilient. This observation creates an important bridge towards risk communication and societal resilience literature, both of which have long examined how trust, uncertainty management, and communication coherence shape collective responses during crises.

Risk communication: communication as uncertainty management

In this article, risk communication and crisis communication are treated as closely related and complementary fields addressing communication before, during, and after disruptive events, risk communication with a stronger orientation towards the pre-event and ongoing management of uncertainty, and crisis communication towards the acute, in-event phase. Because both examine how communication supports preparedness, trust, uncertainty management, and co-ordinated response, we refer to them jointly as risk/crisis communication whenever the distinction between phases is not analytically relevant. Within the crisis governance scholarship, communication has increasingly been conceptualised as a strategic mechanism for uncertainty management, institutional legitimacy, and collective co-ordination under conditions of stress.²¹ Rather than treating communication as a simple information transmission mechanism, this body of research conceptualises it as a critical emergency support function²² through which institutions manage uncertainty, sustain legitimacy, and co-ordinate societal behaviour during crises.²³ Furthermore, modern disaster management highlights that risk and crisis communication constitutes a whole-of-society function through which adaptive capacities can be built, communicative vulnerabilities reduced, and the active participation of citizens enhanced.²⁴

These dynamics become particularly relevant in contemporary digital environments characterised by high informational velocity, emotional amplification, and fragmented communication ecosystems. Authority dissonance, namely exposure to contradictory

institutional messaging, can generate uncertainty and reduce trust in official actors.²⁵ At the same time, narrative capture and selective framing shape the interpretative frameworks through which individuals perceive risks and assign meaning to events.²⁶ The heuristic framework proposed by Hansson et al.²⁷ emphasises that communication-related vulnerability operates at individual (literacy, trust), social-structural (inequality, digital divides), and situational (crisis uncertainty) levels, influencing preparedness, and response behaviours. From this perspective, communication vulnerability is understood not solely as a problem of information access, but as a broader socio-cognitive vulnerability affecting the ability of individuals and communities to interpret, assess, and respond effectively to uncertainty.

Psychological and cognitive research help explain why such environments may increase societal vulnerability. Cognitive dissonance theory suggests that individuals confronted with contradictory, or threatening information may reinterpret evidence in ways that reduce psychological discomfort rather than improve risk assessment.²⁸ Similarly, Kahneman's²⁹ dual-process model indicates that high-speed and emotionally saturated information environments favour intuitive and heuristic reasoning over reflective analysis. Focusing on the effects of media and messages' exposure in times of crises, the Social Amplification of Risk Framework (SARF) posits that risk information is filtered and transformed through media, institutions, and interpersonal networks, amplifying or attenuating public perceptions and responses beyond the objective characteristics of the hazard.³⁰ These amplification processes can generate risk contagion, whereby fear, uncertainty, and behavioural responses spread across populations and stakeholder groups during crises, shaping collective risk perceptions and crisis outcomes.

Importantly, risk communication literature has also identified mechanisms capable of mitigating these dynamics. Research on health emergencies and disaster communication shows that transparent communication, acknowledgment of uncertainty, participatory engagement, and trust-centred messaging improve public compliance and resilience while mitigating the effects of misinformation during crises such as COVID-19, Ebola, and the Fukushima nuclear accident.³¹ Crisis communication literature places particularly emphasis on the source and medium of the crisis message to facilitate its elaboration.³² These findings suggest that crisis communication is mediated by social processes such as credibility and trust in the information source³³ and attribution of crises' responsibility in line with the situational crisis communication theory.³⁴

In this respect, risk and crisis communication can serve a co-ordination and stabilisation function within uncertain and conflict-laden environments³⁵ provided that the messages are tailored to the diverse audiences' capacities and needs, that information uncertainty is managed in a transparent manner and that messages delivered by institutional sources remain consistent³⁶ and guided by the core principles of the Crisis and Emergency Risk Communication (CERC) model namely: be first, be right, be credible, express empathy, promote action, and show respect.³⁷ Thus, risk communication offers not only a tool for crisis governance, but a potential operational logic for strengthening epistemic governance, namely the processes that shape collective perceptions and influence the understanding of a situation within cognitively contested environments.³⁸

Societal resilience: communication as social coordination

Over the past decade, and particularly since the COVID-19 pandemic and the war in Ukraine, societal resilience has emerged as a central organising principle in Euro-Atlantic security policy.³⁹ The concept captures the capacity of societies to withstand, adapt to, and recover from, shocks ranging from natural disasters and pandemics to hybrid warfare and large-scale military aggression.⁴⁰ In the Euro-Atlantic context, three frameworks are particularly influential: (1) the baseline requirements and conceptual framing of resilience by NATO; (2) the analytical definition developed by the European Commission, particularly through its Joint Research Centre (JRC); and (3) the Nordic countries' long-standing "total defence" and civil preparedness models. These approaches illustrate how societal resilience has evolved into a multidimensional governance paradigm integrating civilian preparedness, institutional continuity, social cohesion, and communication systems.

For NATO, resilience is both a civil and military imperative. Within NATO doctrine, resilience functions as a strategic condition of deterrence and operational continuity rather than solely as a civil emergency management concern. It is anchored in Article 3 of the North Atlantic Treaty, which obliges Allies to maintain and develop their individual and collective capacity to resist armed attacks.⁴¹ Since 2016, NATO has operationalised resilience through seven baseline requirements for national preparedness.⁴²

These baseline requirements function as a strategic checklist against three core functions, namely continuity of government, continuity of essential services to the population, and continuity of civil support to the military. Thus, they help to assess the extent to which the civilian systems can support military operations and maintain societal functioning under crisis conditions. Christie and Bērziņa⁴³ argue that, in current highly digitalised societies, three new functions should be added: payment systems, psychological defence, and continuity of data and infrastructure software. Even within this functional listing, psychological defence is not itself an infrastructure to be maintained, but a socio-cognitive capacity to be cultivated, precisely the kind of capacity that communication readiness; developed below, is intended to specify. Adopting a comprehensive approach, societal resilience is thus framed as a whole-of-government and whole-of-society effort and as a key deterrent especially in times of non-conventional attacks.⁴⁴ A NATO report on resilience⁴⁵ further highlights resilience as a systemic property, integrating cyber, infrastructure, and societal systems into a comprehensive preparedness framework.

Although communication systems appear among NATO's baseline resilience requirements, they are mainly conceptualised as an infrastructure rather than as a socio-cognitive capability. The EU approach moves beyond this infrastructural framing, treating resilience as a transnational and multi-level process, linking local, national, and supranational actors. Co-ordination and solidarity amongst Member States are considered essential to address cross-border crises.⁴⁶

The EU approach expands resilience beyond infrastructural continuity by embedding it within democratic legitimacy, participatory governance, and societal co-ordination. As expressed by Cataldo et al.⁴⁷ "*Active citizenship and participatory governance contribute to resilience by fostering trust, enhancing social cohesion, and enabling rapid, context-sensitive responses. Preparedness training, psychosocial support, and*

local risk assessments empower communities to act decisively and reduce the burden on higher-level actors and systems. Civil preparedness and individual resilience capacity are closely interlinked". Importantly, this perspective implicitly recognises communication as a central condition of societal resilience. Trust, participatory governance, and collective co-ordination all depend on communicative processes. In this sense, resilience is strictly linked to social and cognitive conditions. The JRC's CORE model further reinforces this systemic perspective by conceptualising resilience as an ecosystem linking governance, civic space, critical services, and societal co-ordination across multiple levels of society.⁴⁸

Whilst NATO and EU frameworks largely approach resilience through governance and institutional co-ordination, Nordic total defence models embed resilience more deeply within civic culture, public trust, and everyday preparedness practices.

Nordic total defence models are analytically significant because they institutionalise communication, trust, and civic preparedness as strategic security functions, rather than secondary civil-support activities. Total defence assumes that societies must be prepared for prolonged emergencies, that civilian infrastructure must support military operations, and that citizens play an active role in preparedness, crisis communication, and co-ordinated societal response.⁴⁹

In Finland, the model of *kokonaisturvallisuus* (comprehensive security) institutionalises co-ordination amongst ministries, municipalities, private companies, NGOs, and citizens. The national Security Strategy for Society explicitly defines resilience as a shared responsibility spanning all sectors.⁵⁰ Sweden revitalised its total defence framework after 2015, reintroducing civil-defence education, preparedness campaigns, and crisis communication through the Swedish Civil Contingencies Agency. Norway's civil preparedness system similarly emphasises distributed responsibility, continuity planning, and strong local preparedness as pillars of national security.⁵¹

Nordic societal resilience is socially embedded and emphasises public trust and social cohesion as strategic assets in national preparedness systems.⁵² Within these contexts, Sweden has developed the concept of psychological defence, understood as the ability of societies to detect, resist, and recover from information influence operations that target public trust, social cohesion, and democratic processes. This approach is particularly relevant for this paper as it operationalises communication readiness as part of civil preparedness to hybrid attacks and of societal resilience and as a strategic condition of preparedness and co-ordinated societal response.

What communication does: mapping concepts against communication theory

Across the three bodies of literature reviewed above, communication has often been approached through different and partially incompatible conceptual lenses, that is as an instrument of influence in cognitive warfare scholarship, as a governance function in risk communication research, and as a cultural and institutional practice in societal resilience frameworks. This section therefore clarifies how communication has been theorised across these traditions, tracing a progression from foundational transmission models through to socio-technical approaches, and identifying the shared socio-cognitive logic that underlies all three fields.

Early communication models conceptualised communication primarily as the transfer of information between sender and receiver. The classical transmission model developed by Shannon and Weaver⁵³ focused on signal fidelity, encoding, decoding, and the reduction of informational noise, remains foundational within emergency management and crisis communication, particularly in relation to alerts, warnings, and rapid dissemination protocols.

Subsequent theoretical traditions progressively expanded this understanding. Persuasion and influence models conceptualised communication as a mechanism for shaping attitudes and behaviour through framing, source credibility, emotional salience, and cognitive processing.⁵⁴ These mechanisms are particularly relevant within cognitive warfare, where communication operates as a tool for narrative targeting, behavioural influence, attentional capture, and emotional amplification, but have also been used in the context of risk and crisis communication.⁵⁵

Speech act theory further extended the communicative dimension of action by emphasising that language does not merely describe reality, but actively performs actions within it.⁵⁶ Strategic declarations, institutional announcements, emergency alerts, and official directives shape behavioural expectations, authorise responses, and structure collective interpretation. This performative dimension is visible across all three literature streams, from coercive signalling and destabilising narratives in cognitive warfare to evacuation orders and crisis directives in emergency management and preparedness systems.⁵⁷

Other traditions foreground the constitutive rather than purely instrumental dimensions of communication. Ritual and symbolic models conceptualise communication as the process through which societies reproduce shared identities, social cohesion, and collective values over time.⁵⁸ This perspective is particularly relevant to societal resilience, where preparedness campaigns, commemorative practices, and recurring institutional messaging contribute to embedding readiness within civic culture.⁵⁹ Similarly, social constructionist models emphasise that communication actively participates in the production of social reality itself through shared meanings, institutionalised narratives, and collectively accepted interpretations of risk, legitimacy, and normality.⁶⁰ These dynamics are central across the three fields: cognitive warfare exploits competing constructions of truth and legitimacy; risk communication shapes how publics recognise and interpret threats; and resilience frameworks rely on the gradual institutionalisation of preparedness norms and collective expectations.⁶¹

Communication also possesses an important relational and political dimension. Dialogic and participatory approaches emphasise reciprocity, responsiveness, and co-creation of meaning between institutions and publics, highlighting the importance of participation and deliberation in sustaining legitimacy and social trust. Habermas's theory of communicative action similarly positions communication as oriented towards mutual understanding through transparency, sincerity, truthfulness, and rational deliberation.⁶² These principles strongly underpin risk communication and societal resilience scholarship, where institutional legitimacy and behavioural compliance depend heavily on public trust and credible communication practices during crises.⁶³ At the same time, critical discourse approaches stress that communication environments are also structured by relations of power, authority, and exclusion, which shape which narratives become dominant, legitimate, or marginalised within

society.⁶⁴ From this perspective, cognitive warfare can be understood not only as informational manipulation, but also as a struggle over interpretative authority and the production of socially accepted reality. The same can apply to the development of narratives about risk, a process that is often referred to as “riskification”.⁶⁵ More recent socio-technical and networked approaches further demonstrate that communication increasingly emerges through interactions amongst institutions, digital platforms, algorithms, media systems, and distributed social actors, producing communication environments that are recursive, networked, and dynamically amplified through digital infrastructures. The social amplification mechanism developed later in this article returns to this dynamic, specifying how these socio-technical properties function as an active lever of both cognitive vulnerability and communication readiness, rather than merely a background condition.⁶⁶

Table 1 Summarises how these theoretical traditions map onto the three fields, identifying the primary analytical function each model performs within cognitive warfare, risk, and crisis communication, and societal resilience literature respectively.

Taken together, these theoretical traditions show that communication performs multiple analytical functions: it transmits information, shapes attention and interpretation, constitutes shared meanings, establishes or contests authority, and co-ordinates relations across institutional and socio-technical networks. The next section identifies the levels at which these communicative functions generate vulnerability or support preparedness.

Table 1. Primary analytical functions of communication models across cognitive warfare, risk communication, and societal resilience literature (what the communication does).

Communication Model	Cognitive Warfare	Risk & Crisis Communication	Societal Resilience & Civil Preparedness
Transmission	—	Rapid alert dissemination; signal fidelity under crisis conditions	Continuity of communication systems during shocks
Influence & persuasion	Narrative targeting; behavioural manipulation; attentional capture	Message framing; protective behaviour compliance	Preparedness behaviour promotion; norm adoption
Speech acts	Destabilising declarations; coercive signalling	Operational directives; evacuation and shelter orders	Institutional emergency announcements; policy authorisation
Ritual & symbolic	Identity exploitation; symbolic manipulation	Symbolic trust-building and institutional continuity	Civic identity reinforcement; preparedness culture embedding
Social construction	Competing truth regimes; legitimacy contestation	Risk framing; public interpretation of evolving threats	Shared risk norms; institutionalisation of preparedness expectations
Dialogic & participatory	Disruption of deliberative conditions	Two-way communication; public engagement during crises	Participatory governance; community-based preparedness
Communicative action	Erosion of deliberative and legitimacy conditions	Transparency; institutional credibility; public deliberation	Democratic resilience; trust in governance institutions
Discourse & power	Struggle over interpretative authority; narrative dominance	Authority and framing structures in crisis messaging	Inclusion and exclusion in preparedness narratives
Networked & socio-technical	Platform exploitation; algorithmic amplification	Digital coordination; multi-channel dissemination	Cross-sector network co-ordination under distributed stress

Where communication operates: levels of analysis

The communication functions identified above operate at different, but interconnected levels of analysis. We distinguish four levels: cognitive or individual, group or community, institutional, and societal. This distinction clarifies where communicative vulnerabilities arise, where preparedness capacities can be built, and how processes at one level may affect outcomes at another.

Figure 1 synthesises these relationships by positioning communication readiness as a capability spanning all four analytical levels.

Communication readiness, therefore, emerges from the alignment of capacities across all four levels rather than residing within any single one. Having established where communication operates, the following section examines the mechanisms through which it produces vulnerability and preparedness outcomes.

How does communication generate outcomes: identifying key mechanisms

The socio-cognitive infrastructure outlined in the preceding section is continuously activated, disrupted, amplified, and potentially stabilised through recurrent mechanisms that permit communication to generate its outcomes.

We propose a framework based on five interconnected socio-cognitive mechanisms: exposure, interpretation, affective activation, social amplification, and behavioural and organisational response. These mechanisms elucidate how communication environments shape the ways individuals and groups perceive reality, interpret threats, regulate emotional responses, co-ordinate behaviour, and maintain institutional legitimacy under conditions of stress and contestation.

Importantly, the model illuminates where communication readiness capacity can intervene to reduce communicative fragility, stabilise collective sense-making, and strengthen societal preparedness. This perspective aligns with research showing that information ecosystems are both vulnerability surfaces and resilience infrastructures.⁶⁷

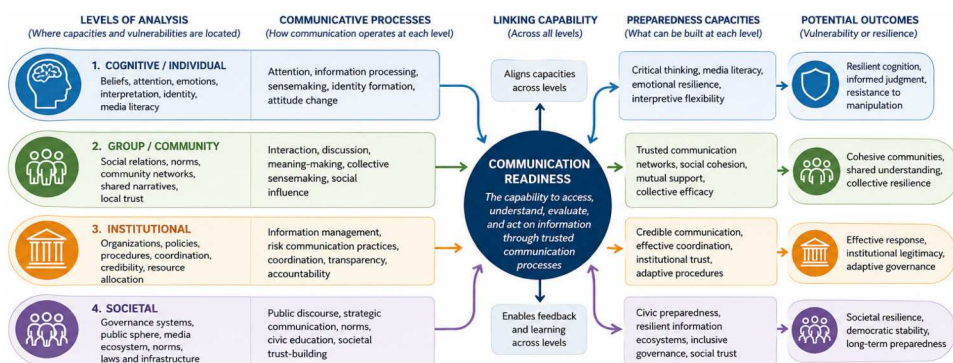


Figure 1. Communication readiness linking levels of analysis. Communication readiness is a core capability that aligns communicative processes, preparedness capacities, and outcomes across the cognitive/individual, group/community, institutional, and societal levels, shaping whether these levels produce vulnerability or resilience.

The very mechanisms through which cognitive disruption spreads, such as uncertainty amplification, narrative contestation, and trust erosion, therefore also constitute key leverage points for preparedness and resilience-building interventions.⁶⁸ In this framework, communication readiness is conceptualised as the socio-cognitive capability, introduced above, enacted through recursive communicative practices that sustain stable societal structures and thereby support their resilience.

Although analytically separated for clarity, the mechanisms described below are mutually reinforcing rather than strictly linear: exposure shapes interpretation; interpretation conditions trigger emotional activation; emotional responses intensify risk amplification dynamics; and behavioural responses reshape future communication environments and trust conditions over time. The mechanisms are linked through a common communicative logic: disruption affecting one mechanism alters the conditions under which subsequent communication is interpreted, trusted, amplified, and acted upon. Conversely, communication readiness can intervene at each mechanism to preserve interpretive coherence, trust, and co-ordinated response, thereby reducing the likelihood that local communicative disruption escalates into broader societal vulnerability. Accordingly, the framework is intended for contexts characterised by sustained informational contestation in which communication influences preparedness, trust, and collective co-ordination. It is not intended to explain all communication crises; rather, it proposes that communicative disruption is more likely to escalate when communication readiness is weak, whereas higher levels of communication readiness can moderate or interrupt escalation across the five mechanisms. [Figure 2](#) summarises the proposed framework and illustrates how communication readiness capacities may intervene across the socio-cognitive chain through which vulnerability and resilience co-evolve within contested communication environments.

Exposure refers to the patterned contact of individuals and groups with narratives, frames, symbols, and informational cues distributed through media systems, institutional messaging, digital platforms, and interpersonal networks. In contemporary conflict environments, such exposure is rarely neutral: visibility, repetition, salience, and informational prioritisation are increasingly shaped by algorithmic amplification, agenda-

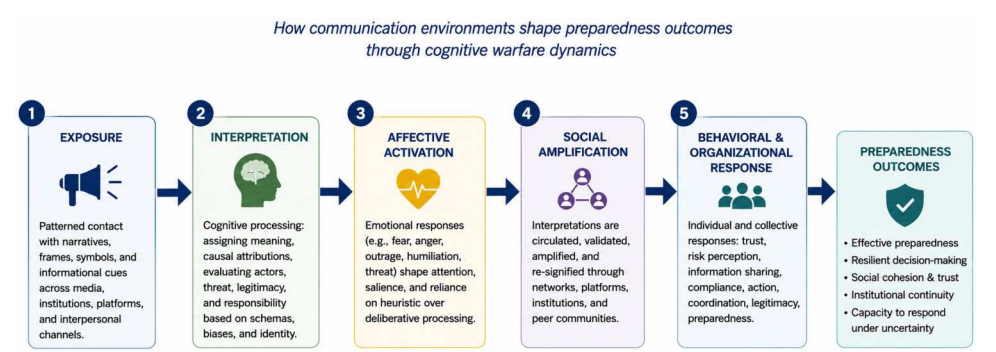


Figure 2. Communication-readiness mechanisms. The figure depicts exposure, interpretation, affective activation, social amplification, and behavioural and organisational response as interacting mechanisms that jointly and recursively shape preparedness outcomes in cognitively contested environments.

setting dynamics, selective dissemination, and attentional competition.⁶⁹ Exposure therefore represents more than informational contact: it constitutes the initial structuring of the communicative environment within which collective sensemaking emerges, privileging some interpretations while excluding others.⁷⁰ Communication readiness at this stage rests on trusted communication channels, information clarity, and institutional consistency, including multiple, redundant channels and local crisis information centres, to reduce informational saturation and selective exposure effects during crises.⁷¹

Exposure alone does not determine behavioural outcomes. Individuals and groups must interpret the information to which they are exposed by assigning meaning, evaluating credibility, identifying causal responsibility, assessing legitimacy, and determining threat relevance. Interpretation is shaped by pre-existing schemas, identity commitments, selective attention, framing effects, and cognitive biases, influencing not only what audiences know, but how they make sense of what they know.⁷² Strategic actors may exploit these vulnerabilities through narrative narrowing, selective contextualisation, and ambiguity injection designed to increase interpretive divergence and weaken shared understandings of reality, an effect compounded when fragmented institutional communication and contradictory authority structures erode confidence in official interpretive frameworks.⁷³ Communication readiness at this stage therefore depends less on informational volume than on interpretive coherence: transparency, contextualisation, critical thinking capacities, verification practices, and trusted institutional communication that caters to audiences' informational needs.⁷⁴

Communication environments shape not only cognition, but also emotions, which serve a communicative function in directing behaviour.⁷⁵ Affective activation refers to the emotional processes through which certain cognitive and behavioural responses are prioritised over others. Fear, anger, humiliation, moral outrage, and perceived existential threat influence attentional scope, salience attribution, working memory, and evaluative judgment, favouring heuristic over deliberative processing under stress and uncertainty.⁷⁶ Narratives become influential not only through their informational content, but because they activate affective states that make certain interpretations feel urgent, credible, and normatively compelling.⁷⁷ Left unmanaged, emotional escalation may intensify polarisation, reduce ambiguity tolerance, and reinforce in-group and out-group dynamics, increasing susceptibility to manipulative narratives. Communication readiness may partially mitigate these dynamics through coherent communication, institutional credibility, empathetic messaging, and transparent acknowledgement of uncertainty, which reduces panic and supports more stable collective interpretation during crises.⁷⁸ Emotional stabilisation is thus a central component of preparedness within cognitively contested environments.

The fourth mechanism, social amplification, operationalises the recursive, platform-mediated communication environments through which information frames spread and become established, so that this socio-technical structure becomes an active driver of outcomes rather than a background condition. Communication effects do not remain confined to individual reception; they are amplified, normalised, contested, and re-signified through repeated sharing, commentary, algorithmic boosting, elite signalling, and community validation. This mechanism resonates with the social amplification of risk framework,⁷⁹ which shows how communication processes, media systems, and social interactions may amplify or attenuate societal perceptions of risk beyond

the original triggering event. Within cognitively contested environments, amplification dynamics may intensify uncertainty, accelerate emotional contagion, reinforce polarisation, and destabilise shared interpretive frameworks, as adversarial actors exploit platform algorithms, co-ordinated networks, and emotionally resonant content to sustain prolonged cycles of visibility and engagement. Communication readiness here depends on the resilience of communication environments themselves: trusted institutional mediation, participatory communication practices, cross-sector co-ordination, and resilient local communication networks help slow destabilising amplification by reinforcing verification practices and sustaining shared interpretive reference points.

Table 2. Communication-readiness mechanisms and their contribution to societal resilience in cognitively contested environments.

Mechanism	What it describes	How vulnerability emerges	Communication-readiness interventions	Preparedness outcomes
1. Exposure	Patterned contact with narratives, frames and information across media, institutions, platforms and interpersonal networks. Shapes the informational environment where sensemaking begins.	Selective exposure, information overload, fragmented institutional messaging and algorithmic amplification of manipulative or emotionally charged content.	Trusted communication channels; exposure to coherent and credible information; message clarity and consistency; whole communication-environment approach.	Greater exposure to trusted information; reduced susceptibility to manipulative narratives; improved preparedness awareness.
2. Interpretation	Processes through which individuals assign meaning, assess credibility, evaluate responsibility and determine threat relevance.	Cognitive biases, identity filters, ambiguity, contradictory authorities, narrative contestation and interpretive fragmentation.	Transparency, contextualisation, critical thinking support, verification practices, coherent institutional messaging tailored to audience needs.	Stabilised collective sensemaking; reduced interpretive fragmentation; improved legitimacy of official information.
3. Affective activation	Emotional processes that give communication cognitive and behavioural force (fear, anger, outrage, threat perception).	Emotional escalation, polarisation, reduced ambiguity tolerance, heuristic decision-making under stress.	Empathetic and transparent communication; acknowledgement of uncertainty; emotionally intelligent messaging; trust-based engagement.	Emotional stabilisation; reduced panic and polarisation; improved public receptivity to guidance.
4. Social amplification	Circulation and reinforcement of narratives through social networks, institutions and digital platforms.	Emotional contagion, algorithmic boosting, echo chambers, polarisation, recursive amplification of uncertainty.	Trusted institutional mediation; participatory communication; cross-sector coordination; resilient local communication networks.	Slower misinformation cascades; stronger shared reference points; sustained collective trust.
5. Behavioural and organisational response	Individual and collective outcomes shaped by the previous mechanisms (trust, compliance, coordination, preparedness behaviour).	Declining institutional legitimacy, reduced coordination capacity, maladaptive behaviours, weakened crisis response.	Continuous communication readiness; coordination across institutions and society; trust-building communication ecosystems.	Strengthened institutional legitimacy; sustained trust and compliance; coordinated, adaptive response capacity under uncertainty.

Finally, behavioural and organisational response refers to the individual and collective consequences that emerge when repeated exposure, interpretation, affective activation, and social amplification interact over time. These responses may include shifts in trust, risk perception, verification practices, information sharing, and compliance with strategic narratives, as well as institutional legitimacy, co-ordination capacity, and the ability of organisations and communities to respond effectively under contested informational conditions.⁸⁰ This stage is particularly significant because it connects cognitive warfare dynamics to societal resilience outcomes, showing how communication environments may either undermine or strengthen the practical capacity of societies and institutions to orient, decide, co-ordinate, and act under pressure.⁸¹ Preparedness outcomes therefore depend, not solely on the presence or absence of hostile narratives, but on the broader communicative conditions through which societies sustain co-ordinated collective action during crises. Communication readiness, in this sense, becomes a core preparedness capability operating across cognitive, group/community, institutional and societal levels simultaneously. Table 2 synthesises the five communication-readiness mechanisms, showing how each may generate vulnerabilities under conditions of cognitive warfare and how corresponding communication-readiness capacities may contribute to societal resilience.

Reading across the table shows that the same communicative mechanisms through which cognitive disruption may propagate can also constitute points of intervention for preparedness and resilience. Exposure, interpretation, affective activation, social amplification, and behavioural and organisational response may each generate specific vulnerabilities when exploited or destabilised, while corresponding communication-readiness capacities can help sustain trust, interpretive coherence, emotional stability, co-ordination, and collective action under uncertainty. Levels and mechanisms serve different analytical purposes. Levels identify where communication-related vulnerabilities and capacities are located, whereas mechanisms explain how communication generates vulnerability or preparedness across those levels. A single mechanism may therefore operate simultaneously at multiple levels. Table 3 synthesises how each of the five mechanisms manifests across these four levels, mapping where vulnerability emerges and where communication readiness can intervene.

Practical implications for defence against cognitive warfare and for societal resilience

The framework presented in this article should be understood as a conceptual lens rather than a prescriptive operational model. Its primary contribution is to organise fragmented insights from the literature into an integrated understanding of how communication infrastructures shape societal resilience under cognitive warfare. As argued throughout this paper, communication readiness shifts attention from militarised approaches focused primarily on countering adversarial manipulation towards preparedness frameworks that strengthen resilience across multiple levels of society.

Here we illustrate some practical implications for societal resilience to cognitive warfare:

- (1) Communication readiness is a socio-cognitive capability operating across civilian, institutional, informational, and military domains. As such, it arises from sustaining

Table 3. Communication readiness mechanisms across levels of analysis.

Mechanism	Cognitive level	Group/Community level	Institutional level	Societal level
1. Exposure	Attention, salience, selective exposure, information processing	Shared communication environment; interpersonal and local information networks	Trusted channels, message consistency, multichannel communication, information centres	Inclusive information environment and equitable access to reliable information
2. Interpretation	Meaning-making, credibility assessment, framing, cognitive biases	Collective sensemaking, shared narratives, identity-based interpretation	Transparency, contextualisation, coherent messaging, audience-oriented communication	Stable interpretive frameworks and reduced narrative fragmentation
3. Affective activation	Fear, anger, uncertainty, heuristic processing, emotional regulation	Emotional contagion, polarisation, in-group/out-group dynamics	Empathy, acknowledgement of uncertainty, trust-building, emotional stabilisation	Reduced collective anxiety and greater social cohesion during crises
4. Social amplification	Reinforcement of perceptions through repeated exposure and cognitive biases	Sharing, validation, contestation, social diffusion of narratives	Cross-sector co-ordination, trusted mediation, verification practices	Resilient communication ecosystem limiting misinformation, polarisation and cascading risk perceptions
5. Behavioural & organisational response	Trust, risk perception, compliance, verification and information-sharing behaviours	Collective preparedness, co-ordination, mutual support	Organisational legitimacy, crisis response capacity, co-ordinated decision-making	Societal resilience, co-ordinated collective action, institutional legitimacy and adaptive preparedness

the communicative conditions through which societies maintain shared meaning, legitimacy, and co-ordinated collective action under uncertainty.

- (2) Following on the above point, we contend that communication readiness is the backbone of the societal resilience architecture, not merely an instrument of influence management, a matter of infrastructural continuity as in NATO's baseline requirements, or a question of media literacy. Preparedness against cognitive disruption instead requires strengthening the communicative infrastructures through which uncertainty is interpreted, trust is maintained, emotional escalation is managed, and collective responses are co-ordinated across cognitive, community, institutional, and societal levels. Vulnerability arises not only from exposure to hostile content or disruption of physical networks, but from fragmentation, incoherence, recursive amplification dynamics, and the erosion of shared interpretive reference points.
- (3) Existing societal resilience frameworks should be reformed to include communication-readiness indicators, not only technical communication capacity, but also trust stability, communication coherence, uncertainty management, institutional credibility, amplification dynamics, and emotional escalation patterns. This aligns with recent discussions on psychological defence, cognitive resilience, and democratic governance within Nordic total defence models, where public trust, preparedness education, and co-ordinated crisis communication are increasingly treated as

strategic security assets. The five mechanisms proposed in this framework provide a conceptual basis for such assessment instruments: rather than prescribing standardised metrics, they point to what should be examined, namely institutional trust under informational stress, consistency of communication across authoritative actors, and the resilience of local communication networks. These vulnerabilities are not purely informational; they are socio-cognitive conditions affecting how societies process uncertainty, sustain legitimacy, and co-ordinate behaviour during crises.

- (4) Within defence and civil preparedness operational planning and exercises, communication readiness should be tested as a preparedness function in cognitively contested environments. Existing exercises often focus on adversarial narratives or disinformation content, with less emphasis on how uncertainty, contradictory information, emotional escalation, and institutional incoherence affect collective interpretation, and co-ordination under pressure. Exercises could incorporate communication-readiness injects, such as contradictory institutional guidance, information overload, fragmented authority structures, or rapidly evolving uncertainty, shifting evaluation from message delivery towards institutions' broader ability to sustain communicative coherence and co-ordinated decision-making under contested conditions. Narrative stress-testing would then serve, not only to identify hostile influence campaigns, but also to assess the resilience of communication ecosystems themselves, evaluating how systems respond when informational environments become saturated, emotionally charged, or epistemically unstable. This implies treating communication as a strategic preparedness capability, integrated into resilience planning and operational readiness, not merely an informational support function.

Despite its analytical utility, the framework proposed here remains conceptual and exploratory rather than predictive or empirically validated. The mechanisms identified are intended to provide an interpretive structure for understanding how communication environments shape societal vulnerability and preparedness across cognitively contested contexts, rather than a deterministic causal model applicable uniformly across all crises or political systems. The relative influence of each mechanism is likely to vary according to cultural, institutional, technological, and geopolitical conditions, as well as the specific characteristics of particular crises or influence operations. Moreover, the framework does not attempt to capture exhaustively all dimensions of cognitive warfare, but instead focuses specifically on the communicative and socio-cognitive dynamics linking information environments to societal resilience. Future empirical research, comparative case studies, simulation environments, and operational exercises will therefore be necessary to refine further, operationalise, and test the framework across different preparedness contexts. Future research should translate the conceptual dimensions proposed here into operational indicators and validated assessment instruments suitable for different organisational and national contexts.

Conclusions

This paper has argued that cognitive warfare operates, not only through hostile narratives and disinformation, but through the exploitation of underlying communicative fragilities

in trust, uncertainty management, collective sensemaking, emotional regulation, and societal co-ordination. Rather than treating communication solely as an instrument of influence, the paper reframes communication readiness as a socio-cognitive preparedness capability and develops a mechanism-based framework showing how exposure, interpretation, affective activation, social amplification, and behavioural and organisational response, jointly shape preparedness outcomes. Crucially, the same mechanisms that enable cognitive disruption also offer leverage points for resilience: communication readiness and risk communication capacities can stabilise collective sensemaking, reduce communicative fragility, and enhance preparedness under uncertainty.

The analysis further shows that many dynamics central to cognitive warfare scholarship have long been examined in risk communication and crisis management research. Extensive empirical work on disasters, pandemics, and public emergencies demonstrates that trust, transparency, message coherence, participatory engagement, and uncertainty management significantly shape behaviour and institutional legitimacy during crises. However, these insights have rarely been translated into defence-oriented frameworks as core capabilities of cognitive security and societal resilience.

Accordingly, the paper contributes to ongoing discussions on societal resilience, cognitive security, and strategic communication by proposing a translational bridge across these domains. It extends STRATCOM and resilience approaches beyond primarily offensive or counter-disinformation paradigms, emphasising the importance of resilient communication environments capable of sustaining trust, shared meaning, institutional legitimacy, and co-ordinated action under informational contestation. This perspective aligns with emerging whole-of-society resilience frameworks in NATO, the European Union, and Nordic preparedness strategies, and is consistent with recent defence analyses stressing the need to integrate institutional, technological, and societal dimensions of cognitive resilience.⁸²

Several research directions appear particularly relevant. Future studies could examine how communication readiness operates across different political cultures and resilience models; how trust dynamics evolve during prolonged cognitively contested crises; how preparedness exercises may operationalise communication-readiness assessments; and how communication environments interact with emerging technologies, algorithmic amplification, and AI-driven influence operations. Addressing these questions will be essential to translating communication readiness from a conceptual framework into an operational capability for societal resilience.

Notes

1. Sara Russo and Navid Yazdanjue, 'Mapping the Cognitive Warfare Literature: A Strategic Analysis (1981–2025)', *Journal of Strategic Studies* (2026): 1–33, <https://doi.org/10.1080/01402390.2026.2640427>.
2. Bernard Clavier et al., 'Cognitive Warfare: The Future of Cognitive Dominance' (papers presented at the first NATO Scientific Meeting on Cognitive Warfare, Bordeaux, France, 21 June 2021).
3. Piotr Filipkowski and Ignas Kalpokas, 'Resilience Factors in Influence Operations in the Context of CTI Analysis', *Safety & Defense* 11, no. 2 (2025): 17–27, <https://doi.org/10.37105/sd.268>.

4. Ćosić Krešimir, Siniša Popović, and Brenda Kay Wiederhold, 'Emotionally Based Strategic Communications as a New Tool in Defensive Cognitive Warfare', *Frontiers in Psychology* 17 (2026): 1751406, <https://doi.org/10.3389/fpsyg.2026.1751406>.
5. Robert L. Heath and H. Dan O'Hair, eds., *Handbook of Risk and Crisis Communication* (New York: Routledge, 2009).
6. Matthew W. Seeger, Timothy L. Sellnow, and Robert R. Ulmer, *Communication and Organizational Crisis* (Westport: Praeger, 2003).
7. Cass R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media* (Princeton: Princeton University Press, 2017); Stephan Lewandowsky et al., 'Misinformation and Its Correction: Continued Influence and Successful Debiasing', *Psychological Science in the Public Interest* 13, no. 3 (2012): 106–31.
8. Jesper Falkheimer, and James Pamment (eds), *Psychological Defence and Information: A Textbook on Theory and Practice*, Swedish Psychological Defence Agency, 2025.
9. Swedish Government, *Totalförsvaret 2021–2025. Government Bill 2020/21:30* (Stockholm: Ministry of Defence, 2020).
10. Elina Jaakkola, 'Designing Conceptual Articles: Four Approaches', *AMS Review* 10 (2020): 18–26, <https://doi.org/10.1007/s13162-020-00161-0>; Richard J. Torraco, 'Writing Integrative Literature Reviews: Guidelines and Examples', *Human Resource Development Review* 4, no. 3 (2005): 356–67, <https://doi.org/10.1177/1534484305278283>; Hannah Snyder, 'Literature Review as a Research Methodology: An Overview and Guidelines.', *Journal of Business Research* 104 (2019): 333–39, <https://doi.org/10.1016/j.jbusres.2019.07.039>.
11. Sara Russo and Navid Yazdanjue, 'Mapping the Cognitive Warfare Literature: A Strategic Analysis (1981–2025)', 2026.
12. Lyneyve Finch, 'Psychological Propaganda: The War of Ideas on Ideas during the First Half of the Twentieth Century', *Armed Forces & Society* 26, no. 3 (2000): 367–86, <https://doi.org/10.1177/0095327X0002600302>; Martin F. Herz, 'Some Psychological Lessons from Leaflet Propaganda in World War II', *Public Opinion Quarterly* 13, no. 3 (1949): 471–86, <https://doi.org/10.1086/266096>; O. P. Araldsen, 'Norway and Soviet Psychological Warfare', *Royal United Services Institution Journal* 106, no. 624 (1961): 585–8, <https://doi.org/10.1080/03071846109420734>; Paul M. McGarr, 'The Information Research Department, British Covert Propaganda, and the Sino-Indian War of 1962: Combating Communism and Courting Failure?', *The International History Review* 41, no. 1 (2017): 130–56, <https://doi.org/10.1080/07075332.2017.1402070>; Kevin John McEvoy, 'Before the Rubble: Britain's Secret Propaganda Offensive in Chile 1960–1973', *Contemporary British History* 35, no. 4 (2021): 597–619, <https://doi.org/10.1080/13619462.2021.1971080>; Lori Clune, 'Waging War with Words, 1945–1963', In *A Companion to U.S. Foreign Relations: Colonial Era to the Present* (2020), 710–25, <https://doi.org/10.1002/9781119166139.ch33>; Bernard Claverie and François du Cluzel. *The Cognitive Warfare Concepts* (NATO ACT Innovation Hub. 2021), https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf (accessed May 4, 2026); Oliver Backes and Andrew Swab, *Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States* (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2019).
13. Claverie and du Cluzel, 'The cognitive warfare', 2021; Bernard Claverie, François du Cluzel, and Gilles Desclaux, 'Cognitive Warfare and C2: Operationalizing the Concept of Cognitive Warfare' (paper presented at the 2nd Scientific and Strategic Workshop on Cognitive Warfare, United States Military Academy, West Point, NY, 2022).
14. Amy F. T. Arnsten, 'Stress Signalling Pathways That Impair Prefrontal Cortex Structure and Function', *Nature Reviews Neuroscience* 10, no. 6 (2009): 410–22, <https://doi.org/10.1038/nrn2648>; Justin Storbeck, and Gerald L. Clore, 'On the Interdependence of Cognition and Emotion', *Cognition and Emotion* 21, no. 6 (2007): 1212–37, <https://doi.org/10.1080/02699930701438020>; Hadas Okon-Singer et al., 'The Neurobiology of Emotion-Cognition Interactions: Fundamental Questions and Strategies for Future Research', *Frontiers in Human Neuroscience* 9 (2015): 58, <https://doi.org/10.3389/fnhum.2015.00058>; Florin Dolcos, Alexandru D. Iordan, and Sanda Dolcos. 'Neural Correlates of Emotion-Cognition

- Interactions: A Review of Evidence from Brain Imaging Investigations', *Journal of Cognitive Psychology* 23, no. 6 (2011): 669–94, <https://doi.org/10.1080/20445911.2011.594433>; Florin Dolcos, Lihong Wang, and Mara Mather, 'Current Research and Emerging Directions in Emotion-Cognition Interactions', *Frontiers in Integrative Neuroscience* 8 (2014): 83, <https://doi.org/10.3389/fnint.2014.00083>; Jay J. Van Bavel et al., 'How Social Media Shapes Polarization', *Trends in Cognitive Sciences* 25, no. 11 (2021): 913–16, <https://doi.org/10.1016/j.tics.2021.07.013>.
15. Claverie and du Cluzel, 'The Cognitive Warfare Concepts', 2021; Backes and Swab, 'Cognitive Warfare', 2019.
 16. Andrew Dawson, and Martin Innes, 'How Russia's Internet Research Agency Built Its Disinformation Campaign', *The Political Quarterly* 90, no. 2 (2019): 245–56, <https://doi.org/10.1111/1467-923X.12690>; Peter Pomerantsev *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia* (New York: PublicAffairs, 2014); Samantha Bradshaw, and Philip N. Howard, *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation* (Oxford: Oxford Internet Institute, 2018).
 17. Jesús C. Aguerri, Mario Santisteban, and Fernando Miró-Llinares, 'The Fight against Disinformation and Its Consequences: Measuring the Impact of Russia State-Affiliated Media' on Twitter.', *Crime Science* 13, no. 1 (2024): 17, <https://doi.org/10.1186/s40163-024-00215-9>; Larissa Doroshenko, and Josephine Lukito, 'Trollfare: Russia's Disinformation Campaign during Military Conflict in Ukraine', *International Journal of Communication* 15 (2021): 4662–89, <https://ijoc.org/index.php/ijoc/article/view/16895> (accessed May 4, 2026); Marcus Bösch, and Tom Divon, 'The Sound of Disinformation: TikTok, Computational Propaganda, and the Invasion of Ukraine', *New Media & Society* 26, no. 9 (2024): 5081–106, <https://doi.org/10.1177/14614448241251804>; Yunkang Yang, Stefan McCabe, and Matthew Hindman, 'Does Russian Propaganda Lead or Follow? Topic Coverage, User Engagement, and RT and Sputnik's Agenda Influence on US Media', *The International Journal of Press/Politics* 30, no. 4 (2024): 956–79, <https://doi.org/10.1177/19401612241271074>; Rebecca Marigliano, Lynnette Hui Xian Ng, and Kathleen M. Carley, 'Analyzing Digital Propaganda and Conflict Rhetoric: A Study on Russia's Bot-Driven Campaigns and Counter-Narratives during the Ukraine Crisis', *Social Network Analysis and Mining* 14, no. 1 (2024): 173, <https://doi.org/10.1007/s13278-024-01322-w>.
 18. Luis Alonso-Martin-Romo, Miguel Oliveros-Mediavilla, and Enrique Vaquerizo-Domínguez, 'Perception and Opinion of the Ukrainian Population Regarding Information Manipulation: A Field Study on Disinformation in the Ukrainian War', *El Profesional de la Información* 32, no. 4 (2023), <https://doi.org/10.3145/epi.2023.jul.05>; Vladyslava Batyrgareieva, and Nataliia Netesa, 'Assessment of the Danger of Glorification of Russian Aggression against Ukraine and Its Participants: Social-Legal, Economic, and Criminological Analysis', *Baltic Journal of Economic Studies* 10, no. 4 (2024): 71–81, <https://doi.org/10.30525/2256-0742/2024-10-4-71-81>; Holger Mölder, and Vladimir Sazonov, 'The Impact of Russian Anti-Western Conspiracy Theories on the Status-Related Conflict in Ukraine: The Case of Flight MH17', *Baltic Journal of European Studies* 9, no. 3 (2019): 96–115, <https://doi.org/10.1515/bjes-2019-0024>.
 19. Dolcos et al., 'Neural Correlates of Emotion', 2011; Dolcos et al., 'Current Research and Emerging', 2014; Okon-Singer et al., 'The Neurobiology of Emotion', 2015.
 20. Claverie and du Cluzel, 'The Cognitive Warfare Concepts', 2021; Backes & Swab, 'Cognitive Warfare', 2019.
 21. Robert Lawrence Heath, and Dan O'Hair, (eds), *Handbook of risk and crisis communication* (New York: Routledge, 2009).
 22. Federal Emergency Management Agency (FEMA), *National Response Framework*. 3rd ed (Washington, DC: U.S. Department of Homeland Security, 2019).
 23. Paul Slovic, *The Perception of Risk* (London: Earthscan, 2000); Ortwin Renn, *Risk Governance: Coping with Uncertainty in a Complex World* (London: Earthscan, 2008); Barbara Reynolds, and Matthew W. Seeger, 'Crisis and Emergency Risk Communication as an

- Integrative Model', *Journal of Health Communication* 10, no. 1 (2005): 43–55, <https://doi.org/10.1080/10810730590904571>.
24. Nathan Clark et al., 'Strengthening All-of-Society Approaches for Disaster Resilient Societies through Competency Building: A European Research Agenda', *International Journal of Disaster Risk Reduction* 121 (2025): 105345, <https://doi.org/10.1016/j.ijdrr.2025.105345>.
 25. W. Lance Bennett, and Steven Livingston, 'The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions', *European Journal of Communication* 33, no. 2 (2018): 122–39, <https://doi.org/10.1177/0267323118760317>.
 26. Robert M. Entman, 'Framing: Toward Clarification of a Fractured Paradigm', *Journal of Communication* 43, no. 4 (1993): 51–58, <https://doi.org/10.1111/j.1460-2466.1993.tb01304>.
 27. Sten Hansson et al., 'Communication-Related Vulnerability to Disasters: A Heuristic Framework', *International Journal of Disaster Risk Reduction* 51 (2020): 101931, <https://doi.org/10.1016/j.ijdrr.2020.101931>.
 28. Leon Festinger, *A Theory of Cognitive Dissonance* (Stanford, CA: Stanford University Press, 1957); Joel Cooper, *Cognitive Dissonance: Fifty Years of a Classic Theory* (London: SAGE Publications, 2007).
 29. Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011).
 30. Roger E. Kasperson, et al, 'The Social Amplification of Risk: A Conceptual Framework', *Risk Analysis* 8, no. 2 (1988): 177–87, <https://doi.org/10.1111/j.1539-6924.1988.tb01168.x>.
 31. Toni G. L. A. van der Meer, and Yan Jin, 'Seeking Formula for Misinformation Treatment in Public Health Crises: The Effects of Corrective Information Type and Source', *Health Communication* 35, no. 5 (2020): 560–75, <https://doi.org/10.1080/10410236.2019.1573295>; World Health Organization. *COVID-19 Global Risk Communication and Community Engagement Strategy: Interim Guidance, 23 December 2020* (Geneva: World Health Organization, 2020) (<https://iris.who.int/handle/10665/33805>); Bernadette Hyland-Wood et al., 'Toward Effective Government Communication Strategies in the Era of COVID-19', *Humanities and Social Sciences Communications* 8, no. 1 (2021): 30, <https://doi.org/10.1057/s41599-020-00701-w>; Serena Tagliacozzo, Frederike Albrecht, and Nazife Emel Ganapati, 'International Perspectives on COVID-19 Communication Ecologies: Public Health Agencies' Online Communication in Italy, Sweden, and the United States', *American Behavioral Scientist* 65, no. 7 (2021): 934–55, <https://doi.org/10.1177/0002764221992832>.
 32. Brooke Fisher Liu, Lucinda Austin, and Yan Jin, 'How Publics Respond to Crisis Communication Strategies: The Interplay of Information Form and Source', *Public Relations Review* 37, no. 4 (2011): 345–53, <https://doi.org/10.1016/j.pubrev.2011.08.004>.
 33. Ward van Zoonen, and Toni G. L. A. van der Meer, 'The Importance of Source and Credibility Perception in Times of Crisis: Crisis Communication in a Socially Mediated Era', *Journal of Public Relations Research* 27, no. 5 (2015): 371–88.
 34. W. Timothy Coombs, 'Impact of Past Crises on Current Crisis Communication: Insights from Situational Crisis Communication Theory', *The Journal of Business Communication* 41, no. 3 (2004): 265–89, <https://doi.org/10.1177/0021943604265607>.
 35. Lu et al., 'How Publics Respond', 2025.
 36. James Badu, Bjørn Ivar Kruke, and Gunhild Birgitte Sætnen, 'Crisis Communication and Trustworthiness among Crisis Actors: Towards a Typology of Crisis Management Difficulties', *Safety in Extreme Environments* 5, no. 2 (2023): 119–30, <https://doi.org/10.1007/s42797-023-00074-8>.
 37. Barbara Reynolds, and Matthew W. Seeger, *Crisis and Emergency Risk Communication*, Atlanta: Centers for Disease Control and Prevention, 2014, <https://www.cdc.gov/cerc/php/cerc-manual/index.html>.
 38. Harri Jalonen, 'Epistemic Governance in the Context of Crisis: A Complexity-Informed Approach', *Administration & Society* 57, no. 2 (2025): 218–53.
 39. European Group of Five Defence Ministers, 'Joint Statement from the Meeting of the European Group of Five Defence Ministers in Kraków', Press release, February 20, 2026, <https://>

- www.difesa.it/assets/allegati/2026feb20_joint_statement_krak_w_third_round_of_consultations_v2_2026.02.20.14.17.46.419.pdf.
40. Ieva Gajauskaite, 'Defining Societal Resilience as a Defensive Power', In *Democratic Resilience in the Baltics*, vol. 2, edited by Smaliukiene Rasa, David Schultz, and Vaida Giedraityte. Baltic Security and Defence, Cham: Springer, 2026. https://doi.org/10.1007/978-3-032-10146-4_1.
 41. NATO 2024, 'Resilience, Civil Preparedness and Article 3', November 13, 2024. https://www.nato.int/cps/en/natohq/topics_132722.htm.
 42. E. H. Christie and K. Bērziņa, *NATO and Societal Resilience: All Hands on Deck in an Age of War* (Washington, DC: German Marshall Fund of the United States, 2022).
 43. Ibid.
 44. Janet M. Blatny et al., Resilience: NATO Chief Scientist Research Report 2025', NATO Science & Technology Organization; Gajauskaite, 'Defining Societal Resilience', 2026.
 45. Blatny et al., Resilience: NATO, 2025.
 46. Fabian Cataldo et al., *Rethinking Societal Resilience in a Time of Polycrisis* (Luxembourg: European Commission, Joint Research Centre, 2025), <https://publications.jrc.ec.europa.eu/repository/handle/JRC142772>.
 47. Fabian Cataldo et al., *Rethinking Societal Resilience in a Time of Polycrisis*, 2025.
 48. Rainer Jungwirth et al., *Hybrid Threats: A Comprehensive Resilience Ecosystem*, EUR 31104 EN. Luxembourg: Publications Office of the European Union, 2023, JRC129019, <https://doi.org/10.2760/37899>.
 49. Finnish Government, *Security Strategy for Society*, Helsinki: Prime Minister's Office, 2017; Swedish Government, *Totalförsvaret 2021–2025. Government Bill 2020/21:30* (Stockholm: Ministry of Defence, 2020), <https://www.regeringen.se/globalassets/regeringen/dokument/forsvarsdepartementet/forsvarsproposition-2021-2025/totalforsvaret-2021-2025-prop.-20202130.pdf>.
 50. Finnish Government, *Security Strategy for Society*, 2017.
 51. Norwegian Ministry of Justice and Public Security, *Societal Security in a Changing World*, White Paper. 2022.
 52. OECD, *Building Resilience to the COVID-19 Pandemic: The Role of Centres of Government*, Paris: OECD Publishing, 2021; Mikael Wigell, Mariette Häggglund, Christian Fjäder, Emma Hakala, Johanna Ketola, and Harri Mikkola, *Nordic Resilience: Strengthening Cooperation on Security of Supply and Crisis Preparedness, FIIA Report 70* (Helsinki: Finnish Institute of International Affairs, 2022), <https://harisportal.hanken.fi/en/publications/nordic-resilience-strengthening-cooperation-on-security-of-supply/>.
 53. Claude E. Shannon, and Warren Weaver, *The Mathematical Theory of Communication* (Urbana: University of Illinois Press, 1949).
 54. Carl I. Hovland, Irving L. Janis, and Harold H. Kelley, *Communication and Persuasion: Psychological Studies of Opinion Change* (New Haven, CT: Yale University Press, 1953).
 55. Chang-Dae Ham, and Jeesun Kim, 'The Role of CSR in Crises: Integration of Situational Crisis Communication Theory and the Persuasion Knowledge Model', *Journal of Business Ethics* 158, no. 2 (2019): 353–72, <https://doi.org/10.1007/s10551-017-3706-0>; Christoph Deppe, and Gary S. Schaal, 'Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept', *Frontiers in Big Data* 7 (2024): 1452129, <https://doi.org/10.3389/fdata.2024.1452129>; Maria Constantinescu, 'Weaponizing the Mind: Emerging Technologies in Cognitive Warfare', *Defense & Security Analysis* (2026), doi:10.1080/14751798.2026.2641840.
 56. J. L. Austin, *How to Do Things with Words* (Oxford: Clarendon Press, 1962); John R. Searle, *Speech Acts: An Essay in the Philosophy of Language* (Cambridge: Cambridge University Press, 1969).
 57. Katsuya Yamori, 'Disaster Information from the Viewpoint of Speech Act Theory: Constative, Performative, and Declarative Utterances', *Journal of Disaster Information Studies* 14 (2016): 1–10, https://doi.org/10.24709/jasdis.14.0_1; Max Tsung-Chi Yu, and Karl Ho', COVID and Cognitive Warfare in Taiwan', *Journal of Asian and African Studies* 58, no. 2 (2022): 249–

- 73, <https://doi.org/10.1177/00219096221137665>; Kostiantyn Yanchenko, and Edda Humprecht, 'Strategic Narratives on Social Media: How Information Environments Shape the Russian-Ukrainian War Discourse in Seven European Countries', *International Journal of Communication*, August 29, 2025, <https://ijoc.org/index.php/ijoc/article/view/25136>.
58. James W. Carey, *Communication as Culture: Essays on Media and Society* (Boston: Unwin Hyman, 1989); Roger E. Kasperson et al., 'The Social Amplification of Risk: A Conceptual Framework', *Risk Analysis* 8, no. 2 (1988): 177–87. <https://doi.org/10.1111/j.1539-6924.1988.tb01168.x>
59. Elina R. Tachkova, 'Enhancing Post-Crisis Communication through Memorials: The Case of the Bonfire Crisis at Texas A&M', *Corporate Communications: An International Journal* 25, no. 3 (2020): 395–411, <https://doi.org/10.1108/CCIJ-12-2019-0146>.
60. Peter L. Berger, and Thomas Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge* (Garden City, NY: Doubleday, 1966).
61. Chad M. Briggs, and Anita Tusor, 'Surveying New Battlegrounds: Ukraine and the Future of Cognitive Warfare', *Journal of Strategic Security* 18, no. 4 (2025), <https://digitalcommons.usf.edu/jss/vol18/iss4/12/>.
62. Jürgen Habermas, *The Theory of Communicative Action*. Volume 1: Reason and the Rationalization of Society (Boston: Beacon Press, 1984); Habermas Jürgen, *The Theory of Communicative Action*, Volume 2: Lifeworld and System: A Critique of Functionalist Reason (Boston: Beacon Press, 1987).
63. Barbara Reynolds, and Matthew W. Seeger, 'Crisis and Emergency Risk Communication as an Integrative Model', *Journal of Health Communication* 10, no. 1 (2005): 43–55, <https://doi.org/10.1080/10810730590904571>.; World Health Organization, *COVID-19 Global Risk Communication and Community Engagement Strategy: Interim Guidance*, 23 December 2020 (Geneva: World Health Organization, 2020), <https://iris.who.int/handle/10665/33805>.
64. Michel Foucault, *The Archaeology of Knowledge and the Discourse on Language*, trans. A. M. Sheridan Smith (New York: Pantheon Books, 1972).
65. Cynthia Hardy, and Steve Maguire, 'Organizing Risk: Discourse, Power, and 'Riskification.' *Academy of Management Review* 41, no. 1 (2016): 80–108, <https://doi.org/10.5465/amr.2013.0106>; Tzu-Chieh Hung, and Tzu-Wei Hung, 'How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars', *Journal of Global Security Studies* 7, no. 4 (2022): ogac016, <https://doi.org/10.1093/jogss/ogac016>.
66. Mats Eriksson, 'Lessons for Crisis Communication on Social Media: A Systematic Review of What Research Tells the Practice', *International Journal of Strategic Communication* 12, no. 5 (2018): 526–51, <https://doi.org/10.1080/1553118X.2018.1510405>; Charity S. Jacobs, Lynnette Hui Xian Ng, and Kathleen M. Carley, 'Tracking China's Cross-Strait Bot Networks against Taiwan', In *Social, Cultural, and Behavioral Modeling*, 115–25. Lecture Notes in Computer Science 14161 (Cham: Springer, 2023), https://doi.org/10.1007/978-3-031-43129-6_12.
67. Stephan Lewandowsky, Ullrich K. H. Ecker, and John Cook, 'Beyond Misinformation: Understanding and Coping with the 'Post-Truth' Era', *Journal of Applied Research in Memory and Cognition* 6, no. 4 (2017): 353–69, <https://doi.org/10.1016/j.jarmac.2017.07.008>; Sander van der Linden, Jon Roozenbeek, and Josh Compton, 'Inoculating against Fake News about COVID-19', *Frontiers in Psychology* 11 (2020): 566790, <https://doi.org/10.3389/fpsyg.2020.566790>.
68. Louise K. Comfort, Arjen Boin, and Chris C. Demchak, eds, *Designing Resilience: Preparing for Extreme Events* (Pittsburgh: University of Pittsburgh Press, 2010).
69. Bradshaw and Howard, *Challenging Truth and Trust*, 2018; Claverie and du Cluzel, 'Cognitive Warfare and C2', 2021.
70. Dawson and Innes, 'How Russia's Internet Research', 2019; Yang et al., 'Does Russian Propaganda', 2024.
71. European Commission, *Citizens' Panel on Preparedness: Final Recommendations*, Brussels: European Commission, May 24, 2026. Available at <https://citizens.ec.europa.eu/document/>

download/18d21e80-380f-4acf-ba9b-3b0afe5cdd08_en?filename=Citizens%27%20Panel%20on%20Preparedness%20-%20final%20recommendations.pdf

72. Storbeck and Clore, 'On the Interdependence', 2007; Claverie et al., 'Cognitive Warfare and C2', 2022.
73. Dawson and Innes, 'How Russia's Internet Research', 2019.
74. Deanna D. Sellnow, Derek R. Lane, Timothy L. Sellnow, and Robert S. Littlefield, 'The IDEA Model as a Best Practice for Effective Instructional Risk and Crisis Communication', *Communication Studies* 68, no. 5 (2017): 552–67.
75. Denis Hilton, 'Emotional Tone and Argumentation in Risk Communication', *Judgment and Decision Making* 3, no. 1 (2008): 100–10.
76. Arnsten, 'Stress Signalling Pathways', 2009; Dolcos et al., 'Neural Correlates of Emotion', 2011; Dolcos et al., 'Current Research and Emerging Directions', 2014; Okon-Singer et al., 'The Neurobiology of Emotion', 2015.
77. Van Bavel et al., 'How Social Media Shapes Polarization', 2021; Arribas et al., 2023.
78. Reynolds and Seeger, 'Crisis and Emergency Risk Communication', 2014.
79. Roger E. Kaspelson et al., 'The Social Amplification of Risk: A Conceptual Framework', *Risk Analysis* 8, no. 2 (1988): 177–87. <https://doi.org/10.1111/j.1539-6924.1988.tb01168.x>
80. Backes and Swab, *Cognitive Warfare*, 2019; M. Haigh, H. A. Birch, and T. V. Pollet, 'Does 'Scientists Believe ...' Imply 'All Scientists Believe ...'? Individual Differences in the Interpretation of Generic News Headlines', *Collabra: Psychology* 6, no. 1 (2020): 17174, doi:10.1525/collabra.17174; A. Taylor et al., 'The Effect of Likelihood and Impact Information on Public Response to Severe Weather Warnings', *Risk Analysis* 44, no. 5 (2024): 1237–53.
81. Claverie and du Cluzel, 2021; Claverie et al., 2022.
82. Christie and Bërziņa, *NATO and Societal Resilience*, 2022; Rainer Jungwirth et al., *Hybrid Threats: A Comprehensive Resilience Ecosystem* (Luxembourg: Publications Office of the European Union, 2023); Mikael Wigell et al., *Nordic Resilience: Strengthening Cooperation on Security of Supply and Crisis Preparedness* (Helsinki: Finnish Institute of International Affairs, 2022); Constantinescu, 'Weaponizing the Mind', 2026.

Acknowledgements

The author would like to thank colleagues and practitioners working in the fields of cognitive warfare, crisis communication, civil preparedness, and societal resilience whose discussions and insights contributed to the development of the ideas presented in this paper.

Author contributions

All authors contributed to the conceptual development of the manuscript. All authors read and approved the final manuscript.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Sara Russo is a PhD candidate in the Defence and Security Studies PhD Programme, jointly offered by the School of Advanced Defence Studies (CASD), Rome, and the University of Turin. Her research focuses on cognitive warfare, societal resilience, and the influence dimension of contemporary conflict, drawing on organisational studies and social network analysis to explore communication, decision-making, and preparedness in contested environments. She has

participated in multinational defence exercises and collaborates with European academic and defence institutions on emerging security challenges.

Serena Tagliacozzo is a researcher at the Department of Electronics, Information and Bioengineering, Politecnico di Milano. Her research focuses on disaster risk reduction, crisis and emergency management, risk communication, and societal resilience. She has conducted extensive research on disaster preparedness, emergency governance, and the role of communication in supporting effective response and recovery, with particular expertise in security and disaster studies.

Juan Camilo Urazan Chinchilla is a researcher at the Centro Regional de Estudios Estratégicos en Seguridad (CREES), Escuela Superior de Guerra “General Rafael Reyes Prieto”, Colombia. His research focuses on strategic and defence studies, hybrid threats, cognitive warfare, and regional security dynamics. His work examines emerging forms of conflict, strategic competition, and the implications of technological and informational change for contemporary security environments.

Lina Maria Manrique-Villanueva is a researcher at the Centro Regional de Estudios Estratégicos en Seguridad (CREES), Escuela Superior de Guerra “General Rafael Reyes Prieto”, Colombia. Her research focuses on strategic studies, security and defence policy, and emerging security challenges, with particular interests in hybrid threats, cognitive warfare, and resilience. Her work contributes to the analysis of contemporary security environments and the development of strategic approaches to complex threats.

ORCID

Sara Russo  <http://orcid.org/0009-0004-8176-8712>