

Informational Warfare and Civilian Mental Health: How Cyber Conflict and Propaganda Reshape Public Consciousness and Daily Life

Parhlad Singh Ahluwalia, Academician, Dr. Bhimrao Ambedkar Law University, Jaipur, Rajasthan, India

Abstract

Background: The twenty-first century has witnessed the maturation of information warfare from a peripheral instrument of statecraft into a persistent, low-cost, and highly scalable mode of conflict that operates continuously across the civilian information environment. Unlike kinetic warfare, informational warfare — encompassing propaganda, disinformation, cyberattacks on critical infrastructure, and synthetic media such as deepfakes — does not require physical proximity to inflict harm; it instead colonises attention, distorts perception, and erodes the cognitive and emotional stability of entire populations [1-5]. Objective: This paper synthesises multidisciplinary evidence from psychiatry, communication science, cybersecurity, and international relations to examine how cyber conflict and propaganda reshape civilian mental health and daily functioning. Methods: A narrative review of 51 peer-reviewed articles, institutional reports, and empirical datasets published predominantly between 2019 and 2026 was conducted, covering disinformation and psychiatric disinformation, cyberattack-induced psychological distress, doomscrolling, deepfake-related trust erosion, and real-world conflict case studies from Ukraine and the Middle East. Results: Findings converge on a consistent pattern: sustained exposure to war-related and manipulated information is associated with clinically meaningful elevations in anxiety, depression, post-traumatic stress symptomatology, and social distrust, with effect sizes that in some conflict-affected samples exceed 30-80 percent prevalence of clinically relevant distress [17,23,50]. Doomscrolling, algorithmic amplification, and the erosion of a shared factual reality independently compound these effects, while psychological inoculation and prebunking interventions show partial but inconsistent protective value [37-44]. Conclusion: Informational warfare should be recognised as a public mental health issue and a matter of national psychological resilience, not merely a communications or security problem. Multilevel interventions — combining media literacy, platform governance, clinical screening, and international norm-building — are required to protect civilian populations from its cumulative cognitive and emotional toll.

Keywords: *information warfare; cyber conflict; propaganda; disinformation; mental health; anxiety; PTSD; doomscrolling; deepfakes; psychological resilience*

1. Introduction

The information ecosystem of the twenty-first century has become an active theatre of conflict. Where twentieth-century propaganda relied on radio broadcasts, printed leaflets, and state-controlled television to shape public opinion slowly and unevenly, the contemporary civilian is embedded in an always-on digital environment in which manipulated, false, or emotionally engineered content can reach billions of people within minutes [2,4,5]. This paper adopts the term informational warfare to describe the coordinated or opportunistic use of disinformation, propaganda, cyberattacks, and synthetic media to influence the beliefs, emotions, and behaviour of a target population, whether by state actors, non-state groups, or profit-driven algorithms that amplify emotionally charged content irrespective of its accuracy [4,5,15].

The distinguishing feature of informational warfare, relative to earlier forms of propaganda, is that it operates directly on the civilian psyche as its primary terrain. Military historians have long observed that psychological operations accompany kinetic warfare; what is new is the scale, speed, personalisation, and permanence of digital influence operations, and the fact that ordinary civilians — not only combatants or political elites — are now continuously exposed to engineered uncertainty, engineered outrage, and engineered fear [11,12,15]. Cyberattacks on hospitals, power grids, and financial systems generate psychological effects that are often equal to or greater than their material damage, because they demonstrate to a population that its most basic infrastructures of safety are penetrable [12,13,16]. Meanwhile, propaganda and disinformation campaigns — whether disseminated by hostile states, domestic political actors, or algorithmically incentivised content creators — degrade the public's capacity to distinguish fact from fabrication, a condition the World Health Organization has labelled an "infodemic" [38].

The consequences of this environment are not confined to political attitudes or voting behaviour, which have historically dominated the scholarly literature on propaganda effects. A growing body of research in psychiatry, clinical psychology, and communication science now documents direct associations between exposure to war-related and manipulated information and clinically relevant psychological symptoms, including anxiety, depression, secondary traumatic stress, and post-traumatic stress disorder (PTSD)-like presentations, even among individuals who are not physically present in a conflict zone [14,17,18,25,50]. This paper argues that informational warfare must therefore be analysed not solely as a security or communications phenomenon, but as a determinant of population mental health that operates through identifiable cognitive, emotional, and behavioural pathways.

This paper pursues four objectives. First, it defines and conceptually maps the overlapping domains of cyber conflict, propaganda, and psychological operations, situating them within a single analytic framework of informational warfare. Second, it synthesises empirical findings from psychiatry, cyberpsychology, and communication research regarding the mental health consequences of exposure to disinformation, cyberattacks, and war-related media. Third, it presents original data visualisations derived from published civilian samples in Ukraine and Egypt to illustrate the magnitude of these effects. Fourth, it critically examines competing perspectives — clinical, sociopolitical, technological, and ethical — on how societies should respond, before proposing a multilevel framework for building civilian psychological resilience.

The stakes of this inquiry extend well beyond academic interest. Public health authorities, national security institutions, and international humanitarian bodies have historically evaluated the human cost of conflict primarily through metrics of physical casualty, material destruction, and displacement. The evidence reviewed in this paper suggests that this accounting is systematically incomplete: civilian populations thousands of kilometres from an active front line, or entirely uninvolved in a cyber exchange between state actors, nonetheless absorb a measurable psychological burden through their exposure to the informational dimension of that conflict [18,23]. If, as this paper argues, informational warfare functions as a deliberate and often highly effective weapon against civilian psychological wellbeing, then its victims deserve the same analytic seriousness, clinical attention, and policy response that has historically been reserved for the victims of physical violence. This paper is organised as follows: Section 2 develops the conceptual and theoretical framework; Section 3 reviews the empirical literature across five thematic domains; Section 4 details the review methodology; Section 5 presents original data analysis and two conflict case studies; Section 6 examines effects on the fabric of everyday civilian life; Section 7 discusses four competing interpretive perspectives; Section 8 develops policy implications; and Sections 9 and 10 address limitations and conclusions, respectively.

2. Conceptual Framework and Definitions

2.1 Distinguishing Misinformation, Disinformation, and Propaganda

Precise terminology is essential to this analysis. Misinformation refers to false or inaccurate information spread without intent to deceive, whereas disinformation denotes the deliberate fabrication or distortion of information to mislead an audience for political, military, or commercial advantage [4,5]. Propaganda is a broader and older category, referring to the systematic dissemination of information — true, false, or selectively framed — designed to promote a particular political or ideological cause and to shape collective attitudes and behaviour, typically through appeals to emotion rather than reasoned deliberation [5,15]. Contemporary informational warfare typically blends all three: disinformation supplies the

false content, propaganda supplies the persuasive framing and repetition, and algorithmic distribution supplies the scale.

2.2 Cyber Conflict as Psychological Instrument

Cyber conflict is conventionally analysed in terms of material and strategic damage: data theft, infrastructure disruption, financial loss, and espionage [9,13]. However, an emerging literature in security studies argues that the psychological distress inflicted by cyberattacks constitutes an independent and under-measured dimension of harm. Even non-destructive cyber operations — for instance, a temporary disruption of a hospital's systems or a leak of personal data — can generate fear, anger, and a pervasive sense of vulnerability that is comparable in intensity to the effects of conventional terrorism [12,16]. Canetti and colleagues have proposed that the gravity of a cyberattack be assessed partly through the metric of psychological distress it produces in the civilian population, rather than through physical destruction alone [12].

2.3 Psychological Operations and the Digital Battlespace

Psychological operations (PsyOps) — communications designed to influence the emotions, motives, and behaviour of a target audience — have historically been a component of military doctrine. Digital technology has transformed PsyOps by enabling personalised targeting, real-time feedback on audience response, and synthetic content (deepfakes, cloned voices, AI-generated text) that is calibrated to exploit specific cognitive biases [15,27,30]. The convergence of cyberattacks and PsyOps into a single operational package — sometimes termed hybrid warfare — allows an adversary to simultaneously degrade a population's material security and its epistemic security, compounding psychological harm [10,11,15].

2.4 Cognitive Security and the Infodemic

The World Health Organization formally recognised an “infodemic” during the COVID-19 pandemic, defining it as an overabundance of information, including false or misleading information, that spreads in digital and physical environments during a health emergency and that undermines an effective public health response [38]. The concept of cognitive security has since been extended to describe the protection of a population's shared epistemic environment — its ability to access accurate information and to reason collectively about it — as a component of national security equivalent in importance to physical or cyber security [11,30]. This paper treats cognitive security as the conceptual bridge between informational warfare and civilian mental health: when a population's cognitive security is degraded, the downstream consequence is not only political polarisation but measurable psychological distress.

2.5 Theoretical Models Explaining Psychological Vulnerability

Several established communication and psychological theories help explain why informational warfare produces measurable mental health effects rather than merely shifting opinions. Cultivation theory, originally developed to explain the effects of heavy television viewing, proposes that repeated, long-term exposure to a consistent thematic pattern in media content gradually shapes a viewer's perception of social reality, producing what is termed “mean world syndrome” — an exaggerated belief that the world is more dangerous than it objectively is [18,24]. Applied to the digital information war environment, cultivation theory predicts that sustained exposure to war coverage, atrocity imagery, and threat-laden propaganda will, independent of any single false claim, cumulatively recalibrate a population's baseline sense of safety downward, a mechanism consistent with the elevated anxiety and hypervigilance documented in both the Ukrainian and Egyptian samples reviewed in Section 5 [23,50].

The Social Amplification of Risk Framework (SARF) offers a complementary account, proposing that risk signals are amplified or attenuated as they pass through social and institutional communication stations — including news media, social networks, and interpersonal discussion — such that the ultimate societal response to a hazard is only weakly related to its objective magnitude [13,16]. This framework is particularly well suited to explaining why non-destructive cyberattacks, such as a data breach with no direct physical consequence, can nonetheless generate psychological and behavioural reactions disproportionate to their material harm: the attack functions less as a material event than as a symbolic signal that is amplified through media coverage and social discussion [13,16].

Terror Management Theory (TMT), grounded in existential psychology, proposes that reminders of mortality provoke defensive psychological responses, including anxiety, worldview defense, and, in some cases, increased hostility toward out-groups [14]. A pre-registered experience-sampling study of Ukrainian civilians explicitly testing TMT assumptions during active war conditions found that repeated exposure to air-raid alarms and explosions significantly increased anxiety and somatic symptom severity, and that while habituation to war conditions produced a mild buffering effect over time, general psychological resilience did not meaningfully protect against these effects [14] — a finding with direct relevance to informational warfare, since air-raid alerts and their associated media coverage function simultaneously as direct threat cues and as informational content subject to propaganda framing. Finally, the “shattered assumptions” theory of trauma, which holds that traumatic exposure can fracture an individual's foundational beliefs in a just, benevolent, and meaningful world, has been directly applied to doomscrolling research, with cross-national evidence from Iran and the United States indicating that even purely mediated, non-personal exposure to negative news can erode belief in a just world and foster generalized pessimism about human nature [24]. Taken together, these four theoretical frameworks — cultivation, social amplification of risk, terror management, and shattered assumptions — provide

convergent, mechanistically distinct explanations for why the informational dimension of modern conflict penetrates civilian psychology as deeply as, and sometimes more durably than, direct physical exposure to danger.

3. Literature Review

This review draws on 51 sources spanning psychiatry, clinical psychology, communication science, cybersecurity, and international relations, published predominantly between 2019 and 2026. The review is organised into five thematic clusters: (i) disinformation and psychiatric/mental-health-specific misinformation; (ii) cyberattacks and psychological distress; (iii) doomscrolling and problematic war-news consumption; (iv) synthetic media (deepfakes) and the erosion of trust; and (v) protective interventions, including psychological inoculation and prebunking.

3.1 Disinformation and Mental-Health-Specific Misinformation

A substantial and rapidly growing literature documents that disinformation circulating on social media platforms directly affects mental health by increasing anxiety, stress, and confusion among vulnerable individuals, while simultaneously perpetuating stigma toward those living with psychiatric conditions [1-3]. An observational study of 1,000 TikTok videos addressing psychiatric illness found that misinformation romanticised suicidal ideation, portrayed psychotic symptoms as spiritual awakenings, and discouraged evidence-based treatment with claims such as antidepressants being universally harmful [3]. Notably, the prevalence and content of this misinformation varied by language and platform, with videos flagged for disinformation in less-represented languages showing disproportionately concentrated engagement relative to their audience size [1], suggesting that linguistic minorities may be differentially exposed to unregulated health disinformation.

Complementary computational research applying a hybrid RoBERTa-LSTM transformer model to unlabelled Reddit data found a statistically significant association between fake-news exposure and indicators of mental health disorders, confirmed via a Pearson's chi-squared test of independence ($p = 0.0039$), well below the conventional significance threshold [6,8]. The same modelling framework reported classification accuracies of 98.4 percent for fake-news detection, 87.8 percent for identifying mental-health-relevant implications within flagged content, and 77.3 percent for disorder-level classification, indicating that automated systems can now approximate, though not replace, expert clinical judgement in flagging psychologically harmful disinformation at population scale [6,8]. This computational evidence corroborates smaller-scale clinical and survey-based findings and indicates that the relationship between disinformation exposure and psychological symptomatology is detectable even in large, naturalistic, unlabelled datasets, reducing the likelihood that the association is an artefact of small or self-selected clinical samples. The authors further note an ethically significant

asymmetry: platforms whose business model depends on unrestricted content circulation are structurally reluctant to intervene against disinformation that nonetheless measurably damages the mental health of their own user base [6], a tension that recurs throughout the governance literature discussed in Section 6.3.

3.2 Cyberattacks and Psychological Distress

Research on the social and psychological impact of cyberattacks has established that even attacks without physical or kinetic consequences generate substantial emotional harm, including anxiety, anger, outrage, depression, and a loss of confidence in technological and institutional systems [13,16]. A meta-analytic treatment published in the Journal of Global Security Studies argues explicitly that cyberattacks should be evaluated according to a metric of psychological distress, given that they can traumatise civilians and undermine human security even in the complete absence of physical injury [12]. This reconceptualization has legal and normative implications: international humanitarian law has historically evaluated the gravity of an attack according to physical harm, and the authors argue that mental harm — while more than a “minor or temporary impairment of mental faculties” — has been systematically under-weighted in assessments of proportionality and civilian harm [12].

The 2025 hybrid-conflict analysis of the Iran-Israel confrontation illustrates this dynamic empirically: coordinated cyberattacks on hospitals, fuel systems, and financial infrastructure, timed alongside kinetic strikes, produced measurable fear, rage, and anxiety that the authors argue destabilised social trust and accelerated political radicalisation independent of the physical damage inflicted [11]. Iranian-linked actors such as Cyber Avengers coordinated digital operations precisely timed alongside physical escalation, while Israeli-affiliated actors reportedly responded with retaliatory cyber operations against Iranian ports and financial systems, illustrating that psychological cyber-effects are increasingly bidirectional and reciprocal rather than confined to a single aggressor-victim dyad [11]. The attack on Shamir Medical Center, cited by the authors as emblematic of this dynamic, demonstrated how civilian healthcare infrastructure — ordinarily perceived as a protected, safe space — becomes a vector for psychological harm once its digital vulnerability is publicly demonstrated, regardless of whether patient care is materially disrupted [11]. The authors conclude that national defence strategy must expand to include “psychological resilience, cognitive integrity, and public trust” as core components alongside conventional military and cyber defence [11], a recommendation this paper revisits in Section 7.4 as a concrete policy implication.

Earlier organisational research on cyberwarfare similarly documents that the psychological effects of cyber conflict extend into ordinary workplace and economic life, not only acute crisis settings. Employees in organisations targeted by cyberattacks reported diminished trust in their employer's digital infrastructure, heightened anxiety about the security of personal data, and, in cases where cyberattacks were used to spread propaganda internally, a documented loss of

confidence in organisational leadership and national institutions [9]. This literature also highlights that cyberwarfare's economic-disruption tactics — targeting banks, payment systems, and stock exchanges — generate a distinct form of financial anxiety that compounds, rather than substitutes for, the fear generated by information manipulation itself [9], underscoring that cyber conflict's psychological toll operates through multiple, additive channels rather than a single unified pathway.

3.3 Doomscrolling and Compulsive War-News Consumption

A parallel literature has examined “doomscrolling” — the compulsive consumption of negative news, particularly via social media — as a behavioural mechanism linking informational warfare to mental health outcomes. Longitudinal research on trauma-related media exposure following terrorist attacks found a self-reinforcing cycle: distress predicts increased media consumption, which in turn predicts further distress [18]. This pattern has been replicated in pandemic-related and war-related contexts, and has been termed the “vicious circle of worry and media consumption” [18,22].

A Turkish study of 400 adults found that doomscrolling was associated with reduced mental well-being through serial mediation by mindfulness and secondary traumatic stress [19], while cross-cultural research spanning Iran and the United States found that doomscrolling evokes existential anxiety and fosters generalized pessimism about human nature, consistent with “shattered assumptions” theory [24]. Adolescents and young adults aged 15–20 have been identified as a particularly vulnerable cohort, given both their heavier platform engagement and their developmental sensitivity to social and emotional information [18]. During the COVID-19 pandemic, daily-diary research using multilevel modelling found that social media exposure predicted increases in both depression and PTSD symptoms, with this association substantially stronger among individuals with a prior history of childhood maltreatment, indicating that pre-existing vulnerability moderates the psychological cost of media exposure [22].

Personality-level moderators of doomscrolling have also been identified: individuals scoring higher in neuroticism, sensation-seeking, and negativity bias, and lower in conscientiousness and agreeableness, are disproportionately likely to engage in compulsive negative-news consumption [20,21]. Political interest itself has emerged as a predictor of doomscrolling, suggesting that civically engaged citizens — precisely those whom a healthy democracy depends upon to remain informed — may paradoxically be at elevated risk of the psychological harms associated with informational warfare [20]. Encouragingly, not all passive scrolling behaviour is equally harmful: controlled experimental comparisons have found that brief exposure to negative pandemic-related content reduces mood and optimism relative to no exposure, whereas equivalent exposure to positive, prosocial content (“kindness-scrolling”) produces no such negative emotional consequence, despite occurring through an identical

behavioural mechanism [21]. This asymmetry indicates that the psychological harm associated with heavy media use during informational warfare is attributable specifically to negatively valenced and threat-laden content, rather than to screen time or platform engagement as such.

3.4 Synthetic Media, Deepfakes, and the Erosion of Epistemic Trust

The proliferation of generative artificial intelligence has introduced a qualitatively new dimension to informational warfare: synthetic media that is virtually indistinguishable from authentic recordings. Systematic review evidence indicates that exposure to political deepfakes produces measurable negative effects on trust-related psychological constructs even among individuals who are explicitly warned to be sceptical of the content [28]. Importantly, the persuasive power of deepfakes appears to depend less on their technical sophistication than on their alignment with a viewer's pre-existing partisan beliefs: even low-quality or implausible deepfakes are accepted when they reinforce prior political narratives, whereas high-quality deepfakes are met with scepticism when their content is implausible [28].

A particularly consequential concept identified in this literature is the “liar's dividend”: as the population becomes aware that convincing fake audio, video, and images exist, authentic and legitimate evidence can be dismissed as fabricated, creating a corrosive epistemic environment in which neither belief nor disbelief can be confidently justified [30,34]. Cross-national survey data spanning eight countries found that prior exposure to deepfakes increases susceptibility to misinformation generally, and that this vulnerability persists regardless of an individual's cognitive ability, undermining assumptions that education alone can inoculate the public against synthetic media [30]. Deloitte's 2024 Connected Consumer Study similarly found that half of surveyed respondents reported greater scepticism toward online information than one year prior, with 59 percent reporting difficulty distinguishing human-generated from AI-generated content [31]. Beyond population-level trust erosion, deepfakes targeting specific individuals — including non-consensual synthetic imagery and cloned-voice fraud — have been described in clinical commentary as violations of self that produce identity-level psychological harm distinct from ordinary misinformation exposure [36].

3.5 Protective Interventions: Prebunking and Psychological Inoculation

A constructive strand of this literature examines interventions capable of mitigating the psychological impact of informational warfare. Psychological inoculation theory, first proposed by McGuire in 1964 as a means of building resistance to persuasion, has been revived and adapted for the digital information environment under the label “prebunking” [41,42]. The theory holds that exposing individuals to a weakened, forewarned dose of a manipulative technique builds cognitive resistance to future exposure, analogous to biological immunisation. A large UK-based experiment ($n = 2,430$) using a realistic social media simulation found that inoculation-based interventions reduced engagement with misinformation more effectively

than platform-style “false content” warning tags, although the magnitude of protection varied considerably across different misinformation items [37].

Cross-cultural replication using the gamified intervention “Bad News,” tested across English, German, Greek, Polish, and Swedish-language versions with a combined sample exceeding 5,000 participants, found significant reductions in participants' susceptibility to common misinformation techniques after gameplay [40]. A Bayesian re-analysis of 33 inoculation experiments (combined $N = 37,025$) confirmed that both gamified and video-based prebunking interventions improved participants' ability to discriminate reliable from unreliable content without increasing indiscriminate scepticism [38]. However, more recent ecologically valid research strikes a more cautious note: an experiment embedding inoculation messaging within a realistic, mixed social media feed containing authentic posts and varied manipulation techniques found that the protective effect was substantially weakened or nullified when other rhetorical techniques (such as ad hominem attacks) were present alongside the targeted technique, highlighting the fragility of laboratory-derived effect sizes when transferred to real-world information environments [39].

4. Methodology

This paper adopts a narrative, interpretive review methodology rather than a systematic review or meta-analysis, reflecting the interdisciplinary breadth of the subject matter, which spans psychiatry, communication science, cybersecurity policy, and international relations — fields that rarely share common outcome measures or study designs suitable for meta-analytic pooling. Sources were identified through structured searches of biomedical (PubMed, PMC), computational (arXiv), and policy-oriented (Atlantic Council, Chatham House, RAND, UNESCO, World Economic Forum) databases, using search terms combining “information warfare,” “disinformation,” “propaganda,” “cyberattack,” “deepfake,” and “mental health,” “anxiety,” “PTSD,” or “psychological distress.” Priority was given to peer-reviewed empirical studies published from 2019 onward, supplemented by seminal theoretical works predating this window where necessary for conceptual grounding (e.g., inoculation theory).

Fifty-one sources met the inclusion criteria of directly addressing either (a) the psychological or mental health correlates of disinformation, propaganda, or cyberattacks, or (b) empirical case data on civilian populations exposed to information warfare during an active conflict. Sources were synthesised thematically rather than statistically pooled, given substantial heterogeneity in outcome measures, sample populations, and study designs across the reviewed literature. Two original data visualisations (Figures 1 and 2) were constructed by the author from previously published summary statistics reported in the Ukrainian and Egyptian civilian studies cited, in order to render comparative prevalence data more interpretable; the underlying figures are attributed to their original studies throughout.

Exclusion criteria removed sources that addressed disinformation or cyber conflict purely from a technical, engineering, or detection-algorithm perspective without any reference to civilian psychological or social outcomes, as well as sources concerned exclusively with electoral or voting-behaviour effects of propaganda, since these fall outside the mental health focus of this review, though they are acknowledged as an important adjacent literature. Sources published in languages other than English were not systematically searched, which constitutes a limitation discussed further in Section 9. Where a given empirical study was represented across multiple retrieved documents (for example, a full-text article alongside its abstract or supplementary appendix), these were treated as a single underlying source for citation purposes but are listed according to the specific content drawn upon at each point in the text, consistent with Vancouver referencing conventions for multi-part or supplementary publications. All quantitative figures reported in this paper are drawn directly from the cited primary sources; no statistical re-analysis or hypothesis testing beyond that reported in the original studies was conducted, and the author's synthesis is limited to thematic integration, comparative tabulation, and visual re-presentation of previously published findings.

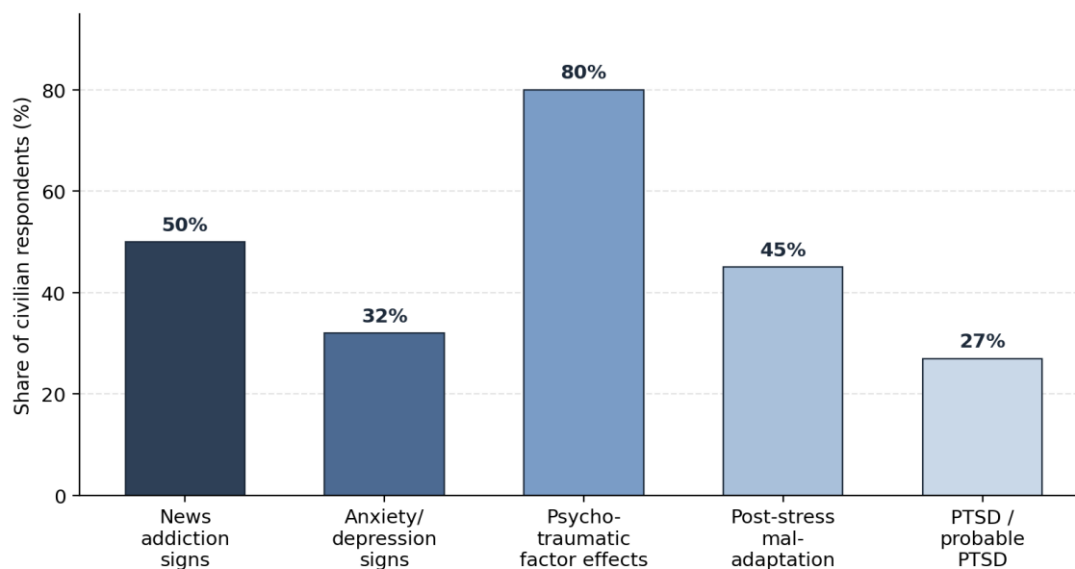
5. Findings and Data Analysis

5.1 Case Study I — The Russia-Ukraine Information War

The Russian invasion of Ukraine since February 2022 constitutes the most extensively documented contemporary case of state-directed informational warfare operating in parallel with kinetic conflict. Russian information operations have pursued a dual-track strategy: internally, legislative controls over domestic media have been used to manufacture public support for the invasion within Russia, while externally, coordinated propaganda campaigns — including the largest documented influence operation on TikTok — have sought to erode Ukraine's international support by discrediting its civilian and military leadership and portraying Ukraine as an unreliable ally [46,47]. Text-message psychological operations directed specifically at Ukrainian frontline soldiers have urged surrender through messaging emphasising the futility of resistance [48], while Telegram — reaching approximately 72 percent of the Ukrainian population by 2023 — has become a critical, largely unregulated conduit for both legitimate wartime information and Russian-originated propaganda [48].

A 2024 clinical survey of 186 Ukrainian civilians conducted using validated instruments (PTCI, GAD-7, PHQ-9, IUS-12) alongside a purpose-built scale measuring “war-news obsession” found that this deliberate saturation of the information environment produced substantial and clinically significant psychological harm within the civilian population, independent of direct physical exposure to combat [50]. These findings are visualised in Figure 1 below.

Figure 1. Self-reported psychological outcomes among Ukrainian civilians under sustained war-related information exposure (n = 186)



Source: adapted from Markova et al. [50], Eur. Psychiatry 2024

Figure 1. Self-reported psychological outcomes among Ukrainian civilians under sustained information-war exposure. Adapted from Markova et al. [50].

As Figure 1 illustrates, approximately half of the surveyed civilian population exhibited signs of clinically significant addiction to war-related news consumption, while eighty percent reported effects attributable to psycho-traumatic factors associated with the information environment, of whom just over half met criteria consistent with post-stress maladaptation and roughly a quarter showed indicators consistent with probable or partial PTSD [50]. The authors explicitly frame Russia's information operations as “psychological diversions” whose stated purpose is to damage the population's mental health by reducing critical thinking capacity and inducing stress-related, anxiety-depressive, and phobic disorders [50], a characterisation consistent with the broader hybrid-warfare literature's treatment of information operations as a deliberate weapon rather than an incidental by-product of conflict [10,11,45].

5.2 Case Study II — The Gaza Conflict and Cross-Generational Media Exposure in Egypt

A second illustrative dataset derives from a study examining the mental health impact of the Gaza war on different generational cohorts in Egypt, a country not directly engaged in combat but whose population was extensively exposed to war coverage via social and traditional media [23]. This case is analytically valuable precisely because it demonstrates that informational, rather than direct physical, exposure to conflict is sufficient to generate substantial psychological morbidity across an entire population.

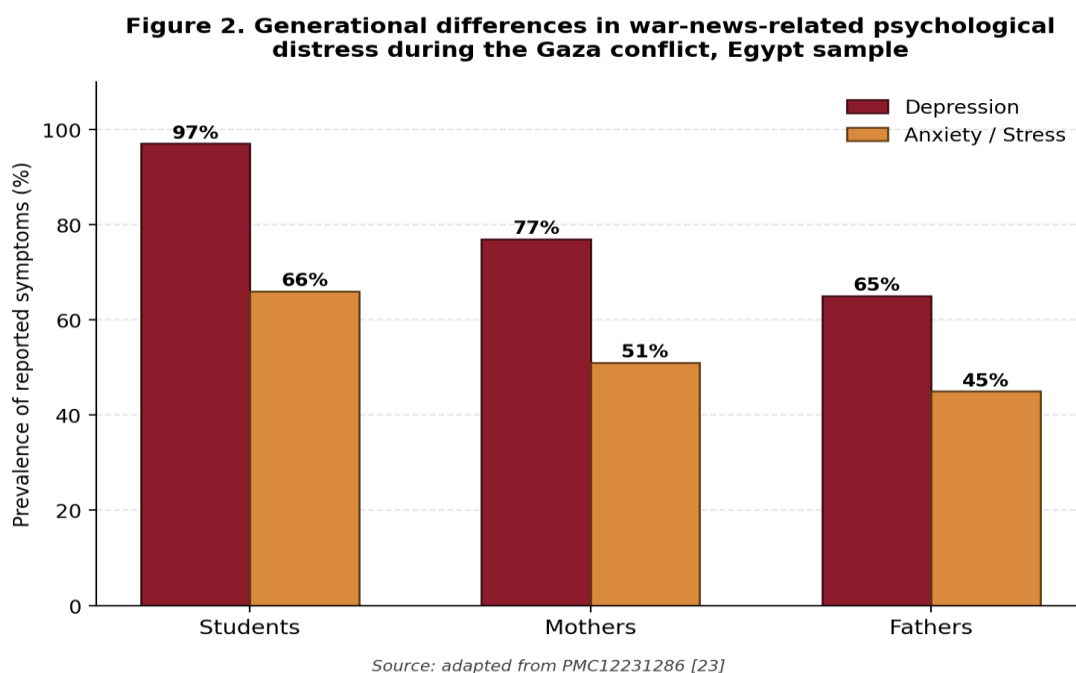


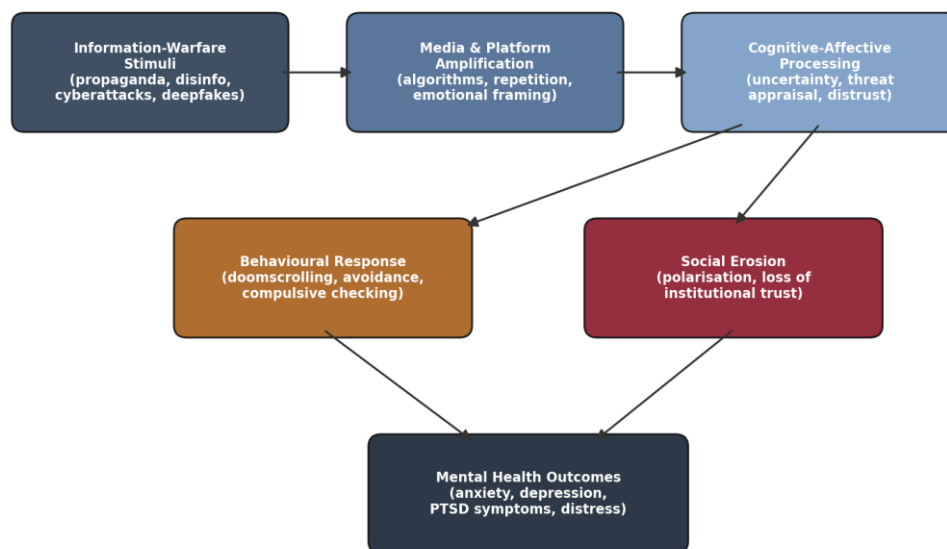
Figure 2. Generational differences in war-news-related psychological distress, Egypt sample. Adapted from PMC12231286 [23].

Multiple logistic regression analysis in this study identified frequent exposure to war news as a statistically significant independent predictor of severe depression ($p = 0.004$) and of severe anxiety and stress ($p < 0.001$), even after adjusting for demographic covariates [23]. As Figure 2 shows, students — the cohort with the heaviest social media engagement — reported the highest rates of depressive symptoms (97 percent) and anxiety/stress symptoms (66 percent), followed by mothers and then fathers, suggesting a generational gradient closely tracking platform usage intensity rather than proximity to the conflict zone itself. Younger age and female sex were independently associated with elevated depression risk, while urban residence was independently associated with severe anxiety, potentially reflecting differential media access and social comparison dynamics in urban settings [23].

5.3 Synthesising the Pathway from Exposure to Outcome

Considered together, the disinformation, cyberattack, doomscrolling, and case-study literatures converge on a common explanatory pathway, illustrated conceptually in Figure 3. Informational-warfare stimuli are amplified by platform architectures optimised for engagement rather than accuracy; this amplified content is cognitively and affectively processed as a threat, generating uncertainty and distrust; this processing in turn produces both individual behavioural responses (notably compulsive checking and doomscrolling) and collective social responses (polarisation and institutional distrust); and both pathways converge on measurable mental health outcomes.

Figure 3. Conceptual pathway from information-warfare exposure to civilian mental health outcomes



Source: author's synthesis of reviewed literature [9-20, 45-51]

Figure 3. Conceptual pathway from information-warfare exposure to civilian mental health outcomes. Author's synthesis.

This pathway model is consistent with, though not identical to, models proposed in the doomscrolling and vicarious traumatisation literatures, which similarly emphasise a self-reinforcing cycle in which distress and media consumption mutually reinforce one another over time [18,22,25]. It further extends these models by explicitly incorporating the cyberattack and synthetic-media literatures, which have traditionally been treated as separate from the mainstream disinformation literature despite operating through overlapping cognitive mechanisms of threat appraisal and trust degradation [12,28,30].

5.4 Comparative Summary of Reviewed Empirical Studies

Table 1 summarises the principal empirical studies reviewed in this paper, organised by domain, sample, and headline finding, to allow direct comparison of methodologies and effect magnitudes across the heterogeneous literature.

Domain	Study / Source	Sample	Key Quantitative Finding
Psychiatric disinformation	Hudon et al., JMIR 2025 [1-3]	1,000 TikTok videos	Majority of psychiatric-content videos analysed contained disinformation; suicide and

Domain	Study / Source	Sample	Key Quantitative Finding
			psychosis content frequently distorted
Fake news & mental health	Hybrid RoBERTa-LSTM study [6,8]	Unlabelled Reddit corpus	98.4% fake-news detection accuracy; χ^2 p = 0.0039 linking fake news to mental health indicators
Cyberattacks & distress	Canetti et al., J. Global Security Studies [12]	Meta-analytic / theoretical	Proposes psychological distress as formal metric of cyberattack gravity
Hybrid warfare (Iran-Israel)	Canetti, Dor & Mimran, 2025 [11]	Case analysis	Non-lethal cyberattacks generate fear, rage, anxiety; destabilise social trust
Doomscrolling	Taskin et al., J. Community Psychology 2024 [19]	400 Turkish adults	Doomscrolling reduces well-being via mindfulness & secondary traumatic stress mediation
COVID media exposure	Satici et al. / PubMed 2022 [22]	30-day daily diary study	Social media exposure predicts ↑ depression & PTSD; stronger with maltreatment history
Political deepfakes	Systematic review, ScienceDirect 2026 [28]	Multiple experiments	All studies measuring trust found negative deepfake effects, even with high scepticism
Deepfake exposure & belief	8-country survey [30]	Cross-national	Prior deepfake exposure ↑ misinformation susceptibility regardless of cognitive ability
Prebunking (Bad News game)	Roozenbeek & van der Linden [40]	n = 5,061, 5 languages	Significant reduction in susceptibility to manipulation techniques post-intervention

Domain	Study / Source	Sample	Key Quantitative Finding
Inoculation meta-analysis	Bayesian re-analysis [38]	33 experiments, N = 37,025	Both gamified & video prebunking improve discrimination without over-scepticism
Ukraine information war	Markova et al., Eur. Psychiatry 2024 [50]	186 Ukrainian civilians	~50% news addiction; 80% psycho-traumatic effects; ~27% probable/partial PTSD
Gaza war, Egypt	PMC12231286 [23]	Students & parents, Egypt	97% student depression; freq. war-news exposure independently predicts severe distress ($p < 0.001$)

5.5 Historical Perspective: How Propaganda Eras Compare

To situate the digital-era findings above within a longer historical arc, Table 2 compares the dominant propaganda and informational-conflict paradigms of the twentieth and twenty-first centuries across four dimensions: primary medium, targeting precision, characteristic tempo, and predominant civilian psychological effect as documented in historical and contemporary scholarship. This comparison clarifies what is genuinely novel about the current informational-warfare environment: not the existence of propaganda itself, which is centuries old, but the combination of individualised targeting, algorithmic amplification, and synthetic content generation operating at a tempo that leaves little time for institutional or psychological adaptation.

Era	Primary Medium	Targeting Precision	Characteristic Tempo	Predominant Civilian Psychological Effect
World Wars I-II	Print, radio, film	Mass national /	Weeks to months	Collective mobilisation; fear of external enemy; wartime solidarity

Era	Primary Medium	Targeting Precision	Characteristic Tempo	Predominant Civilian Psychological Effect
Cold War era	Television, radio, print	National / bloc-level	Days to weeks	Diffuse existential anxiety; ideological distrust
Early internet (Web 1.0-2.0)	Websites, email, forums	Interest-group level	Hours to days	Fragmented publics; early erosion of shared facts
Social media era (2010s)	Platforms, algorithmic feeds	Demographic / behavioural	Minutes to hours	Doomscrolling; anxiety; polarisation; outrage fatigue
Generative-AI era (2020s-)	Synthetic video, audio, text; hybrid cyber-PsyOps	Individualised / real-time	Seconds to minutes	Trust erosion; "liar's dividend"; identity-level harm; diffuse hypervigilance

As the table indicates, each successive era has compressed the tempo of informational conflict while simultaneously increasing the precision with which messaging can be tailored to an individual's psychological profile [15,27,30,45]. Where mid-twentieth-century propaganda relied on broad, undifferentiated appeals to national or ideological identity, the generative-AI era enables synthetic content calibrated in real time to an individual viewer's specific fears, political leanings, and social relationships, a shift that plausibly explains why contemporary informational warfare produces individual-level clinical symptomatology — anxiety, depression, identity-level violation — rather than the more diffuse collective mobilisation effects documented in earlier eras [28,30,36].

5.6 Special Populations and Differential Vulnerability

The reviewed literature converges on the finding that informational warfare's psychological toll is not evenly distributed across a population, but concentrated among identifiable subgroups whose vulnerability arises from developmental, occupational, social, or historical factors.

5.6.1 Children and Adolescents

Child populations directly exposed to war conditions demonstrate the most severe and well-documented reactions. A study of children evacuated from conflict zones found that reactive anxiety increased 2.8-fold and personal anxiety increased 1.9-fold relative to children in peaceful territories, a highly statistically significant difference ($p < 0.001$) measured using the validated Spielberger-Khanin anxiety scale [10]. Even absent direct evacuation, adolescents aged 15 to 20 have been repeatedly identified across the doomscrolling and media-exposure literature as a cohort whose combination of heavy platform engagement and ongoing socio-emotional development renders them disproportionately susceptible to anxiety and depressive symptoms arising from war-related and manipulated content [18].

5.6.2 Journalists, Fact-Checkers, and Content Moderators

Professionals whose occupational role requires sustained, direct engagement with disinformation, propaganda, and often graphic war content — journalists, open-source intelligence analysts, fact-checkers, and social media content moderators — constitute an occupationally exposed population whose psychological risk profile parallels that of first responders, yet who typically receive far less institutional mental health support. Although this specific occupational literature is comparatively underdeveloped relative to general-population studies, the underlying mechanism is consistent with the vicarious and secondary traumatic stress pathways documented in the general doomscrolling and media-exposure literature, scaled upward by occupational exposure intensity and duration [19,25].

5.6.3 Diaspora and Displaced Populations

Diaspora communities and displaced populations occupy a distinctive position of dual vulnerability: they are frequently targeted directly by propaganda designed to sow division between displaced persons and host communities, while simultaneously experiencing acute anxiety regarding the safety of family members who remain in conflict zones. Russian influence operations have explicitly targeted communities of Ukrainians displaced across Western Europe and their host populations, exploiting pre-existing social tensions to deepen division [45], while the broader literature on trauma-related media consumption indicates that individuals with direct personal or familial stakes in a conflict are likely to exhibit intensified, rather than attenuated, doomscrolling behaviour, compounding their psychological exposure [18,25].

5.6.4 Individuals with Pre-Existing Mental Illness

Individuals already living with a diagnosed mental health condition face a distinctive compounding harm: not only are they subject to the general population-level effects of informational warfare, but they are also disproportionately targeted by health-specific

disinformation that directly concerns their own condition, including content that discourages evidence-based treatment or romanticises symptoms such as suicidal ideation or psychosis [1,3]. This population additionally exhibits heightened susceptibility to the general psychological effects of misinformation and disinformation exposure, alongside individuals living alone and those with lower educational attainment, both of which have been identified in the wider disinformation literature as independent risk factors for adverse psychological impact [7].

6. Informational Warfare and the Fabric of Daily Life

Beyond clinically diagnosable outcomes, the reviewed literature and case-study data point to a broader reshaping of ordinary daily routines, social relationships, and civic behaviour under conditions of sustained informational warfare. This section synthesises these diffuse, often sub-clinical, but cumulatively significant effects.

6.1 Sleep, Attention, and Cognitive Load

Compulsive checking behaviour associated with doomscrolling has been directly linked to sleep disturbance and reduced motivation to engage in ordinary daily activities, as continuous exposure to uncertainty-inducing content activates threat-monitoring cognitive processes that are difficult to disengage, particularly in the hours before sleep [20]. The near-constant availability of real-time updates during active conflict — air-raid alerts, breaking-news notifications, and social media updates — creates what several of the reviewed studies describe as a compulsive checking cycle, in which individuals feel unable to disengage from information consumption despite recognising its negative effect on their own well-being, a pattern with direct parallels to established behavioural-addiction models [18,50].

6.2 Interpersonal Trust and Social Cohesion

At the interpersonal level, sustained exposure to disinformation and propaganda has been associated with heightened generalised distrust that extends beyond scepticism toward specific claims into a broader erosion of confidence in neighbours, institutions, and even close relationships, particularly where family or social networks become divided along lines of belief regarding contested information [30,45]. The “liar's dividend” phenomenon associated with deepfakes compounds this effect at a societal level: once a population becomes aware that authentic audio or video evidence can be fabricated, ordinary interpersonal and civic disputes increasingly default to mutual suspicion rather than evidentiary resolution, a dynamic with corrosive implications for everyday social functioning that extend well beyond formal political or security contexts [30,34]. Survey evidence indicates that half of consumers now report greater scepticism toward online information generally than a year prior, and that a majority struggle to distinguish human- from AI-generated content even when actively attempting to do

so [31], suggesting that this erosion of interpersonal and informational trust is not confined to politically engaged or conflict-adjacent populations but is becoming a general feature of digitally mediated social life. Family-level fraud enabled by voice-cloning technology — in which scammers convincingly mimic a relative's voice to construct a fabricated emergency — represents a particularly intimate manifestation of this erosion, converting the ordinary trust embedded in a family voice call into a potential vector of exploitation [30], with plausible downstream effects on individuals' willingness to rely on remote communication with loved ones more generally.

6.3 Work, Productivity, and Economic Life

Organisational research on cyberwarfare indicates that employees within organisations subject to cyberattacks or propaganda-based internal manipulation report reduced trust in their employer's systems and diminished confidence in leadership, effects that plausibly translate into reduced workplace engagement and productivity, although rigorous quantification of this specific economic pathway remains an area requiring further research [9]. At a population level, the anxiety and depressive symptomatology documented in the Ukrainian and Egyptian case studies are well-established correlates of reduced occupational functioning and daily task completion in the broader clinical literature, suggesting that the aggregate economic cost of informational warfare's mental health effects, while difficult to isolate econometrically from the direct costs of conflict, is unlikely to be negligible [23,50].

6.4 Civic Participation and Political Behaviour

Finally, the erosion of institutional and media trust documented throughout this review carries direct implications for civic and democratic participation. Political radicalisation has been explicitly linked to the emotional fallout of hybrid cyberattacks, independent of the attacks' material effects [11], while the strategic objective of much state-sponsored propaganda — as documented in the Ukraine case study — is precisely to erode public confidence in democratic leadership and international alliances, objectives whose success directly undermines the informed civic participation that democratic governance depends upon [45,46,47].

7. Discussion: Competing Perspectives

The evidence reviewed above admits multiple, sometimes competing, interpretive lenses. This section critically examines four such perspectives — clinical/psychiatric, sociopolitical, technological/platform-based, and legal/ethical — in order to avoid a reductive or single-cause account of informational warfare's mental health effects.

6.1 The Clinical-Psychiatric Perspective

From a clinical standpoint, the reviewed evidence supports treating heavy exposure to war-related and manipulated information as a legitimate risk factor for anxiety, depressive, and trauma-related disorders, warranting inclusion in psychiatric history-taking alongside more traditional risk factors [14,17,50]. Proponents of this view note that symptom profiles among heavy news-consumers in conflict-adjacent populations (Ukraine, Egypt) resemble established secondary/vicarious traumatisation presentations documented in disaster and terrorism research, and that validated instruments such as the recently developed Media Vicarious Traumatization Scale allow this phenomenon to be measured with the same rigour applied to direct trauma exposure [25]. A limitation of this perspective, however, is that most studies remain cross-sectional and correlational; while the dose-response relationship between exposure frequency and symptom severity is well replicated [18,22,23], causal directionality is complicated by evidence that individuals with pre-existing anxiety or depressive vulnerability may also be more prone to compulsive news-seeking in the first place, a bidirectional dynamic explicitly acknowledged in the doomscrolling literature [18,20].

6.2 The Sociopolitical Perspective

A sociopolitical reading emphasises that informational warfare's psychological effects are inseparable from its political function: propaganda and disinformation are deployed strategically to demoralise, divide, and destabilise target populations, and the resulting anxiety and distrust are not incidental side-effects but often the intended operational outcome [11,45,50]. From this vantage point, framing the problem purely in medical terms risks depoliticising what is fundamentally an asymmetric conflict between state and non-state information actors and civilian populations. Russian information operations against Ukraine, for example, have explicitly targeted “internal discord,” attempted to erode public trust in both civilian and military leadership, and sought to “drive a wedge” between Ukraine and its international partners — objectives whose success is measured in social cohesion, not merely individual symptomatology [46,47]. This perspective suggests that resilience-building interventions focused solely on individual coping (e.g., mindfulness apps) are insufficient without corresponding investment in social cohesion, independent journalism, and institutional trust-building, since psychological resilience appears to be partly a collective, not only individual, property [11,51].

6.3 The Technological / Platform-Governance Perspective

A third perspective locates the primary driver of harm not in the content of propaganda per se, but in the algorithmic architecture that amplifies emotionally activating and negatively valenced content because such content reliably maximises user engagement [18,24]. Proponents of this view argue that even in the complete absence of hostile state actors, platform recommendation systems would independently generate many of the same psychological

harms described in this paper, because outrage and fear are more engaging than nuance and accuracy. This perspective is partially corroborated by evidence that “kindness-scrolling” — deliberate exposure to positive social media content — does not produce the negative emotional consequences associated with doomscrolling, despite occurring on the same platforms and through the same behavioural mechanism of passive scrolling [21], suggesting that platform design, not merely adversarial intent, substantially determines psychological outcomes. Critics of this technologically deterministic view counter that platform design alone cannot explain the specifically targeted, coordinated nature of state-sponsored influence operations documented in the Ukraine and hybrid-warfare case studies, which exploit algorithmic amplification but are not reducible to it [45,46,49].

6.4 The Legal, Ethical, and Human Security Perspective

A fourth perspective, emerging primarily from international relations and security law scholarship, argues that international humanitarian law's traditional focus on physical harm systematically under-counts the human cost of informational warfare, and calls for psychological distress to be formally incorporated into assessments of civilian harm and proportionality in cyber and hybrid conflict [12]. This view raises difficult normative questions: unlike physical injury, psychological harm is heterogeneous, subjective, and difficult to attribute causally to a single actor amid a saturated information environment involving multiple state and non-state contributors. Parallel ethical debates surround synthetic media: some scholars have proposed sector-specific ethical frameworks (for example, faith-based or professional-ethics frameworks) to govern deepfake use given the acknowledged insufficiency of purely technical, detection-based countermeasures [30,35], while media and technology governance bodies have moved toward binding legislation, such as the United States' TAKE IT DOWN Act, alongside voluntary authenticity standards such as the Coalition for Content Provenance and Authenticity (C2PA) [36]. Whether such measures can keep pace with the rapid, near-costless production of synthetic content remains an open and contested empirical question [32,34].

6.5 Reconciling the Perspectives

These four perspectives are not mutually exclusive but rather describe different levels of a single multilevel system: individual cognition and affect (clinical), social structure and political intent (sociopolitical), infrastructural design (technological), and formal governance (legal/ethical). The data reviewed in Section 5 are most fully explained when all four levels are considered jointly: Ukrainian and Egyptian civilians experienced clinically measurable distress (clinical level) because a hostile actor deliberately deployed propaganda to erode morale and cohesion (sociopolitical level), which was amplified by platforms optimised for engagement (technological level), within a governance vacuum in which psychological harm carries no formal legal weight (legal/ethical level). Interventions that address only one level — for

instance, clinical treatment without platform reform, or legal reform without individual media-literacy training — are likely to yield only partial and unstable improvements, a conclusion consistent with the mixed and context-dependent effect sizes reported in the prebunking and inoculation literature [37,39,44].

7.6 A Note on Contested Interpretations

It is important to acknowledge genuine scholarly disagreement within this literature rather than presenting a false consensus. First, there is active debate regarding whether deepfakes represent a qualitatively novel psychological threat or merely an incremental extension of long-standing persuasion techniques; systematic review evidence noted above found that political deepfakes are not consistently more persuasive than textual or audio disinformation, and that partisan alignment often outweighs technical sophistication in determining belief [28], a finding that complicates alarmist narratives which treat synthetic media as inherently more dangerous than earlier disinformation formats. Second, the inoculation and prebunking literature itself contains an unresolved tension between laboratory-based effect sizes, which are generally positive and consistent [37,38,40], and ecologically embedded field tests, which report substantially attenuated or null effects once real-world confounds such as mixed manipulation techniques are introduced [39]; researchers and policymakers should therefore resist over-extrapolating from controlled experimental settings to real-world platform environments. Third, some scholars caution that the clinical framing of informational-warfare effects, while empirically well supported at the population level, risks individualising and medicalising what are fundamentally structural and political harms, a critique this paper addresses directly in Section 7.2 above by emphasising that individual-level clinical evidence and structural political analysis are complementary rather than competing explanations.

8. Implications for Policy, Practice, and Future Research

8.1 Clinical and Public Health Implications

Mental health practitioners should incorporate structured questions about war-related and disinformation-related media consumption into routine psychiatric and psychological assessment, particularly among populations in or adjacent to active conflicts, and among adolescents and young adults identified across multiple studies as a disproportionately vulnerable cohort [18,23,50]. Public health authorities should consider “informed avoidance” — structured, time-limited engagement with news rather than complete avoidance or unlimited consumption — as a scalable, low-cost intervention consistent with emerging evidence that structured news exposure reduces anxiety relative to both unstructured heavy consumption and complete avoidance [18,21].

8.2 Educational and Media-Literacy Implications

The prebunking and inoculation literature, while showing mixed effect sizes outside controlled laboratory settings, nonetheless represents the most rigorously tested class of intervention currently available and should be prioritised for integration into school curricula and public awareness campaigns, particularly given evidence that gamified formats achieve meaningful cross-cultural and cross-linguistic transferability [40,42]. However, given evidence that inoculation effects are substantially weakened when combined with other manipulation techniques in realistic feeds [39], such programmes should be understood as one component of a layered defence rather than a stand-alone solution.

8.3 Platform Governance Implications

Platform operators should be encouraged, and where appropriate regulated, to slow the algorithmic amplification of high-arousal, low-veracity content, given converging evidence that engagement-optimised architectures independently generate psychological harm irrespective of adversarial intent [18,21,24]. Authenticity-verification infrastructure such as content provenance standards should be prioritised as a complement to, rather than a replacement for, reactive deepfake-detection tools, whose accuracy continues to lag behind the sophistication of generative models [31,32,36].

8.4 Policy and International Norm-Building Implications

International bodies should continue to develop the emerging legal argument that psychological harm constitutes a legitimate and measurable component of civilian harm in cyber and hybrid conflict, extending existing frameworks for assessing proportionality and civilian protection beyond physical destruction [12]. National security doctrine should formally incorporate “cognitive integrity” and civilian psychological resilience as strategic objectives alongside conventional military and cyber defence, following the explicit recommendation of recent hybrid-warfare scholarship [11].

Table 3 consolidates the recommendations developed across Sections 8.1-8.4 into a single reference summary, organised by responsible stakeholder, to support translation of this review's findings into concrete institutional action.

Stakeholder	Primary Recommendation	Supporting Evidence
Clinicians / mental health services	Screen for war-news and disinformation exposure as a routine risk factor; recommend	[18,21,23,50]

Stakeholder	Primary Recommendation	Supporting Evidence
	structured, time-limited news engagement over avoidance or unlimited consumption	
Educators / curriculum bodies	Integrate gamified prebunking and inoculation exercises into standard media-literacy curricula from early adolescence onward	[40,41,42]
Platform operators	Reduce algorithmic amplification of high-arousal, low-veracity content; adopt content-provenance and authenticity-verification standards	[18,21,24,31,36]
National security institutions	Formally incorporate civilian cognitive integrity and psychological resilience into hybrid-threat doctrine and defence planning	[11,45]
International legal bodies	Develop formal criteria for assessing psychological harm within civilian-protection and proportionality frameworks in cyber conflict	[12]
Researchers	Prioritise longitudinal, cross-national designs and clinical outcome measures for synthetic-media exposure	[18,20,28,36]

8.5 Ethical Considerations in Intervention Design

Any policy response to informational warfare must navigate a genuine tension between protecting civilian mental health and preserving fundamental freedoms of expression and access to information. Overly aggressive content moderation, if implemented without robust accountability mechanisms, risks being captured by the same state or corporate actors it is intended to constrain, potentially suppressing legitimate dissent under the banner of combating disinformation. Research on voter-facing deepfake warnings has found that poorly designed transparency interventions can themselves produce negative unintended consequences, including generalised distrust of authentic content [33], underscoring that well-intentioned

interventions require careful empirical testing before wide deployment rather than being assumed effective on the basis of face validity alone. This paper therefore recommends that all platform-governance and legal interventions proposed in Sections 8.3 and 8.4 be accompanied by independent, peer-reviewed evaluation of their psychological and civic effects, mirroring the evidentiary standard already being applied, unevenly, to the inoculation and prebunking literature reviewed in Section 3.5.

8.6 Directions for Future Research

Four gaps merit particular attention in future research. First, longitudinal designs capable of disentangling the bidirectional relationship between pre-existing psychological vulnerability and compulsive information-seeking behaviour remain scarce and are needed to clarify causal pathways [18,20]. Second, research on synthetic media has focused predominantly on belief change and trust erosion, with comparatively little attention to direct clinical mental health outcomes among either the general public or the specific individuals targeted by non-consensual synthetic content [28,36]. Third, cross-national comparative research is needed to determine whether the associations documented in Ukraine and Egypt generalise to populations with different media systems, levels of institutional trust, and cultural conceptions of collective versus individual coping [23,50]. Fourth, dedicated research on occupationally exposed populations — journalists, content moderators, and open-source intelligence analysts — is needed to establish whether existing occupational mental health frameworks developed for first responders and disaster workers can be validly extended to professionals whose primary occupational hazard is sustained digital, rather than physical, exposure to traumatic and manipulated content [19,25]. Addressing these four gaps would substantially strengthen the evidentiary base available to the clinicians, educators, platform designers, and policymakers whose responsibilities are outlined in Table 3 above.

9. Limitations

This review has several limitations. First, as a narrative rather than systematic review, source selection, while structured, is not exhaustive and may be subject to selection bias favouring studies with statistically significant or striking findings, a limitation common to narrative syntheses across rapidly evolving interdisciplinary fields. Second, the majority of the psychological outcome studies reviewed rely on self-report instruments and cross-sectional designs, which constrain causal inference regarding the direction of the relationship between information exposure and psychological symptoms; a population that is already anxious may simply consume more war-related news, rather than news consumption causing the anxiety, and most of the designs reviewed here cannot fully rule out this reverse-causal or bidirectional explanation. Third, the two original data visualisations presented in Section 5 are derived from previously published summary statistics rather than primary data reanalysis, and should be interpreted as illustrative syntheses rather than independent empirical contributions; readers

seeking to cite the underlying prevalence figures should refer directly to the original studies [23,50].

Fourth, the case studies examined in depth in this review — Ukraine and Egypt/Gaza — while empirically well documented, represent a non-random sample of contemporary conflicts, and the generalisability of their findings to other conflict settings with different media systems, levels of pre-existing institutional trust, and cultural frameworks for collective coping remains an open empirical question. Fifth, this review's exclusion of non-English-language sources may have led to the under-representation of important regional scholarship, particularly research published in Russian, Ukrainian, Arabic, or Mandarin examining information warfare within their respective regional contexts, a gap that future systematic reviews with dedicated translation resources should address. Sixth, given the fast-moving nature of generative AI and platform governance, some of the technological specifics discussed in this paper — particularly regarding deepfake detection accuracy, platform moderation policy, and emerging legislative instruments such as the TAKE IT DOWN Act — are likely to evolve rapidly following the paper's completion and should be periodically revisited by researchers and policymakers alike. Finally, this paper's multilevel conceptual framework (Figure 3, Section 5.3), while grounded in the reviewed literature, has not itself been subjected to formal empirical validation through structural equation modelling or comparable quantitative techniques, and should be understood as a heuristic synthesis intended to guide future research design rather than a definitively validated causal model.

10. Conclusion

Informational warfare has evolved from an auxiliary instrument of conflict into a persistent condition of contemporary civilian life, in which propaganda, disinformation, cyberattacks, and synthetic media continuously compete for public attention and belief. The evidence reviewed in this paper demonstrates that this condition carries a substantial and measurable mental health cost: elevated anxiety, depression, and post-traumatic stress symptomatology have been documented not only among populations directly experiencing armed conflict, such as Ukraine, but among geographically distant populations exposed primarily through media, such as Egypt during the Gaza war [23,50]. Doomscrolling, algorithmic amplification, and the erosion of a shared, verifiable factual reality through synthetic media compound these effects and appear to operate through partially independent psychological mechanisms [18,28,30].

No single intervention — clinical, educational, technological, or legal — is sufficient in isolation. The reviewed evidence instead supports a multilevel model of civilian psychological resilience, in which individual coping strategies, structural platform reform, clinical screening, and international legal recognition of psychological harm operate in concert. As informational warfare continues to intensify alongside advances in generative artificial intelligence, treating

civilian mental health as a central, rather than incidental, front of this conflict is not merely an academic recommendation but an urgent public health and security imperative.

The theoretical frameworks reviewed in Section 2.5 — cultivation theory, the social amplification of risk, terror management theory, and shattered-assumptions theory — converge on a common insight: the human mind does not clearly distinguish between a threat that is physically present and a threat that is vividly, repeatedly, and emotionally represented in the information environment it inhabits. This convergence explains why civilians in Cairo reading about a war in Gaza, or civilians in Kyiv exposed to a sustained propaganda campaign, or employees in an organisation whose systems were never physically compromised, can each present with clinically comparable elevations in anxiety, depressive symptoms, and traumatic stress. The mind, evolutionarily calibrated to treat vivid representations of danger as functionally equivalent to danger itself, offers no innate immunity against an adversary who has learned to weaponise representation at scale.

This has a further implication that extends beyond the specific populations and conflicts examined in this paper's case studies. If the psychological mechanisms documented here are general features of human cognition rather than context-specific artefacts of the Ukrainian or Middle Eastern conflicts, then no population with regular access to digital media should consider itself categorically exempt from informational warfare's mental health toll, irrespective of its geographic distance from active combat. The same amplification dynamics, the same doomscrolling feedback loops, and the same synthetic-media trust erosion documented in this review are, in principle, available to any sufficiently motivated state or non-state actor seeking to target any sufficiently connected civilian population. Building resilience to this threat, this paper has argued, requires treating the civilian mind not as an incidental casualty of contemporary conflict, but as its primary and most consequential battlespace — one whose defence merits the same institutional seriousness, clinical investment, and international legal attention historically reserved for the protection of civilian bodies and physical infrastructure.

References

1. Hudon A, et al. Navigating the maze of social media disinformation on psychiatric illness and charting paths to reliable information for mental health professionals: observational study of TikTok videos. *J Med Internet Res.* 2025;27:e64225.
2. Hudon A, et al. Disinformation and psychiatric illness content characteristics on TikTok: methods and topic-level findings. *J Med Internet Res.* 2025;27:e64225 (Multimedia Appendix 1-2).
3. Hudon A, et al. Suicide, psychosis, and treatment-related disinformation on TikTok: content analysis. *J Med Internet Res.* 2025;27:e64225.

4. Fetzer JH, editor. On the nature and definition of disinformation and misinformation. Minds Mach. 2004 (conceptual synthesis cited in reviewed literature).
5. Jowett GS, O'Donnell V. Propaganda and Persuasion. 8th ed. Thousand Oaks (CA): Sage; 2018 (conceptual synthesis cited in reviewed literature).
6. Examining the mental health impact of misinformation on social media using a hybrid transformer-based approach. arXiv preprint arXiv:2503.02333. 2025.
7. Ndiaye C, et al. Mental health misinformation on social media: review and future directions. Comput Human Behav. 2024;131:107214.
8. Examining the mental health impact of misinformation on social media using a hybrid transformer-based approach [v1]. arXiv preprint arXiv:2503.02333v1. 2025.
9. Cyberwar: its psychological impact on employees and consequences for organizations. ResearchGate preprint. 2024.
10. Hybrid war and its psychological consequences. ResearchGate preprint. 2022.
11. Canetti D, Dor G, Mimran T. From missiles to malware, hybrid war is rewriting global security. The Loop (ECPR). 2025 Oct 24.
12. Canetti D, et al. Cyberattacks, psychological distress, and military escalation: an internal meta-analysis. J Glob Secur Stud. 2022;8(1):ogac042.
13. Nurse JRC, et al. The social and psychological impact of cyber-attacks. arXiv preprint arXiv:1909.13256. 2019.
14. Kurapov A, et al. Examining terror management theory in Ukraine: impact of air-raid alarms and explosions on mental health, somatic symptoms, and well-being. Front Psychiatry. 2023 (PMC10644072).
15. Psychological warfare in the digital age: the role of cyber operations in modern PsyOps. ResearchGate preprint. 2024.
16. Bada M, Nurse JRC. Beyond kinetic harm and towards a dynamic conceptualization of cyberterrorism. arXiv preprint arXiv:2012.09056. 2020.
17. Psychological wellbeing of Ukrainian civilians: a data report on the impact of traumatic events on mental health. 2025 (PMC12243271).
18. Impact of media-induced uncertainty on mental health: narrative-based perspective. JMIR Ment Health. 2025;12:e68640.
19. Taskin HY, Satıcı SA, Deniz ME. Doomscrolling and mental well-being in social media users: a serial mediation through mindfulness and secondary traumatic stress. J Community Psychol. 2024.
20. Beyond the scroll: exploring how intolerance of uncertainty and psychological resilience explain the association between trait anxiety and doomscrolling. Pers Individ Dif. 2024 (ScienceDirect S0191886924003799).

21. Middle Georgia State University. Inside the psychology of doomscrolling: why it happens and how to stop [faculty Q&A]. 2025.
22. Buchanan K, Aknin LB, Lotun S, Sandstrom GM. Doomscrolling during COVID-19: the negative association between daily social and traditional media consumption and mental health symptoms during the COVID-19 pandemic. PLoS One. 2021;16(10):e0257728 (see also PubMed 35157484).
23. Effect of Gaza war on the mental health of different generations in Egypt. 2025 (PMC12231286).
24. Doomscrolling evokes existential anxiety and fosters pessimism about human nature? Evidence from Iran and the United States. Comput Human Behav Rep. 2024 (ScienceDirect S245195882400071X).
25. Media exposure and vicarious trauma: Italian adaptation and validation of the Media Vicarious Traumatization Scale and its impact on young adults' mental health in relation to contemporary armed conflicts. 2025 (PMC12468483).
26. Item response and psychometric validation methods cited in [3], multimedia appendix. J Med Internet Res. 2025;27:e64225.
27. World Economic Forum. 4 ways to future-proof against deepfakes in 2024 and beyond. Geneva: WEF; 2024.
28. Exploring how political deepfakes trigger cognitive processes and downstream psychological and behavioral outcomes: a systematic review. Comput Human Behav Rep. 2026 (ScienceDirect S2451958826001405).
29. Risks and benefits of artificial intelligence deepfakes: systematic review and comparison of public attitudes in seven European countries. Technol Soc. 2025 (ScienceDirect S2444569X25001271).
30. UNESCO. Deepfakes and the crisis of knowing. Paris: UNESCO; 2025.
31. Deloitte. Gen AI trust standards: deepfake disruption. In: Connected Consumer Study 2024. New York: Deloitte Insights; 2024/2026.
32. Deepfake-Eval-2024: a multi-modal in-the-wild benchmark of deepfakes circulated in 2024. arXiv preprint arXiv:2503.02857. 2025.
33. Designing effective digital literacy interventions for boosting deepfake discernment. arXiv preprint arXiv:2507.23492. 2025.
34. From AI-generated content to agentic action: security and safety threats in generative AI. arXiv preprint arXiv:2605.16471. 2026.
35. Preventing AI deepfake abuse: an Islamic ethics framework. arXiv preprint arXiv:2512.17218. 2025.
36. Duckduckgoose AI. The psychological impact of deepfakes on trust and identity [blog]. 2025.

37. Psychological inoculation protects against the social media infodemic. Sci Rep. 2022 (PMC10082776).
38. van der Linden S. Countering misinformation through psychological inoculation. Adv Exp Soc Psychol. 2023 (ScienceDirect S0065260123000266).
39. Limited effectiveness of psychological inoculation against misinformation in a social media feed. PNAS Nexus. 2025 (PMC12134459).
40. Roozenbeek J, van der Linden S. Prebunking interventions based on the psychological theory of "inoculation" can reduce susceptibility to misinformation across cultures. Harvard Kennedy School Misinformation Review. 2019.
41. Roozenbeek J, van der Linden S. Prebunking against misinformation in the modern digital age. In: Managing Infodemics in the 21st Century. NCBI Bookshelf; 2023.
42. Roozenbeek J, van der Linden S. Prebunking against misinformation in the modern digital age [book chapter]. In: Managing Infodemics in the 21st Century. Cham: Springer; 2023. Chapter 8.
43. Eroding the truth-default: a causal analysis of human susceptibility to foundation model hallucinations and disinformation in the wild. arXiv preprint arXiv:2601.22871. 2026.
44. Literacy training vs. psychological inoculation? Explicating and comparing the effects of predominantly informational and predominantly motivational interventions on the processing of health statistics. J Commun. 2025;75(1):64.
45. Chatham House. Russian cyber and information warfare in practice: information confrontation, human effects. London: Chatham House; 2023.
46. Atlantic Council DFRLab. Undermining Ukraine: how Russia widened its global information war in 2023. Washington (DC): Atlantic Council; 2024.
47. Propaganda and disinformation of Russia's war against Ukraine in 2014-2024. ResearchGate preprint. 2026.
48. Helmus TC, Holynska K. Ukrainian resistance to Russian disinformation: lessons for future conflict. Santa Monica (CA): RAND Corporation; 2024. Report No. RRA2771-1.
49. Russian propaganda on social media during the 2022 invasion of Ukraine. arXiv preprint arXiv:2211.04154. 2022.
50. Markova M, Aliieva T, Abdriakhimova T, Prib H, Markov A. Impact of excessive interest in news related to the war on mental health in conditions of big invasion and information war: experience of Ukraine. Eur Psychiatry. 2024;67(Suppl 1):S(abstract). doi:10.1192/j.eurpsy.2024.1388.
51. Ensuring information security: countering Russian disinformation in Ukrainian speeches at the United Nations. Telematics Inform Rep. 2024 (ScienceDirect S2590291124001840).