BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Cognitive Warfare as a Strategic Domain: Media Ecosystems, Social Networks, and the Erosion of Societal Resilience

Assoc. Prof. Goran D. MATIĆ, Ph.D.*

*Faculty of Business Studies and Law, "Union Nikola Tesla" University, Belgrade, Serbia, Military Academy, University of Defense, Belgrade, Serbia
e-mail: goran.matic@nsa.gov.rs
https://orcid.org/0000-0001-8443-5797

Abstract

Cognitive warfare has emerged as a distinct domain of modern conflict, reshaping national security by targeting perception, belief systems, and decision-making rather than physical assets. The rise of artificial intelligence marks a historic threshold: algorithms now act not merely as tools but as autonomous agents in shaping public cognition, enabling real-time, personalized manipulation at scale. This article examines how independent media, social networks, and algorithmic systems are weaponized to erode trust and polarize societies. Case studies from Serbia, Ukraine, and Moldova reveal how media monopolization, disinformation, and hybrid threats exploit vulnerabilities in open information ecosystems. The paper argues that cognitive defense must move beyond reactive countermeasures toward institutional safeguards, media autonomy, and civic literacy. Drawing on the DOI system, it proposes a cognitive infrastructure grounded in persistence, traceability, decentralization, and interoperability—embedding democratic resilience into the architecture of communication and ensuring technological innovation does not devolve into authoritarian control.

Keywords:
Cognitive Warfare; Information Operations; Media Autonomy; Social Networks; Disinformation; Societal Resilience; DOI; Information Integrity.

Article info
Received: 6 February 2026; Revised: 25 February 2026; Accepted: 17 March 2026; Available online: 8 April 2026

Citation: Matić, G.D. 2026. "Cognitive Warfare as a Strategic Domain: Media Ecosystems, Social Networks, and the Erosion of Societal Resilience." *Bulletin of "Carol I" National Defence University*, 15(1): 87-104. https://doi.org/10.53477/2284-9378-26-06

Introduction

The battlefield of the twenty-first century is no longer limited to territory, airspace, or the electromagnetic spectrum. It has shifted into the human mind—into the collective cognition of populations, the trust networks of institutions, and the interpretive frameworks through which societies derive meaning. This domain, increasingly labeled as cognitive warfare, represents the systematic manipulation of perception, memory, and decision-making to achieve strategic objectives without direct kinetic action. Operating at the intersection of neuroscience, psychology, and information theory, cognitive warfare exploits vulnerabilities in human cognition and social communication systems. Critically, it marks a historic threshold: for the first time in human history, a technology—artificial intelligence—acts directly upon the human psyche, not merely as a tool wielded by humans, but as an autonomous agent that selects, amplifies, and tailors manipulative content in real time. Although designed and deployed by humans, AI-driven systems now operate with sufficient autonomy to shape belief formation at scale, effectively making the algorithm itself a frontline actor in cognitive conflict. Yet this autonomy remains bounded: AI systems lack intentionality and are constrained by training data, platform architectures, and human oversight loops—factors that create exploitable seams for defensive intervention. This blurs the boundary between tool and agent, raising unprecedented ethical and strategic dilemmas.

This paper examines cognitive warfare as a concrete and evolving paradigm embedded in contemporary media ecosystems. It highlights the dual role of independent media as both a target and a bulwark, the exploitation of social networks for disinformation, and the risks posed by media monopolization. Drawing on evidence from hybrid conflicts in Serbia, Ukraine, and Moldova, the study shows how cognitive attacks exploit societal fractures, institutional weaknesses, and the absence of robust verification mechanisms, reshaping public discourse and undermining democratic resilience. These cases were selected not only for their regional relevance but also because they illustrate different trajectories of democratic development, exposure to hybrid threats, and degrees of media pluralism. Serbia exemplifies the challenges of fragile democracies with polarized media landscapes; Ukraine demonstrates resilience under sustained hybrid assault, while Moldova highlights the vulnerabilities of small states caught between competing geopolitical influences. At the same time, it must be emphasized that there are no clear or verifiable proofs of the direct use of cognitive weapons in these contexts. Unlike cyber warfare, where attacks can be traced through technical signatures and forensic evidence, cognitive warfare operates through subtler mechanisms of perception and manipulation, making attribution far more complex and contested. This absence of definitive evidence underscores both the uniqueness and the ambiguity of cognitive operations, situating them at the intersection of influence, propaganda, and psychological pressure rather than conventional weaponry.

The central thesis is that cognitive defense cannot rely on censorship or centralized narrative control, nor on restrictive models of internet content regulation that risk undermining democratic discourse in the digital age. In the twenty-first century, where social networks and algorithmic platforms shape the circulation of information, resilience must instead be cultivated through pluralism, transparency, accountability, and the persistent identification of information objects. Only by embedding these principles into communication infrastructures can societies safeguard trust without sliding into authoritarian patterns of control. The Digital Object Identifier (DOI) system, long used in scholarly publishing, offers a model for securing information integrity through persistence, traceability, and decentralization. By reframing technical protocols as instruments of democratic resilience, the DOI system demonstrates how infrastructures of trust can be engineered to withstand manipulation.

The paper is structured as follows: first, it defines cognitive warfare within contemporary security theory, situating it at the intersection of psychology, law, political science, and information studies; second, it analyzes mechanisms of manipulation through social networks, algorithmic amplification, and media monopolies, highlighting how emotional contagion and structural vulnerabilities interact; third, it evaluates independent media as a pillar of resilience, treating journalism not merely as a communicative practice but as critical democratic infrastructure; and finally, it proposes a framework for cognitive infrastructure grounded in DOI-like principles of identification, metadata transparency, and cross-sector collaboration, emphasizing that such protocols are both technical safeguards and normative commitments to democratic legitimacy.

Methodologically, this study combines comparative case analysis (Yin 2018)with elements of discourse analysis (Fairclough 1995) to trace how cognitive warfare manifests across diverse information environments. The cases of Serbia, Ukraine, and Moldova were selected to capture variation in regime type, exposure to hybrid threats, and levels of media pluralism (Heidenreich 2021). This selection follows a structured, focused comparison (George and Bennett 2005): Serbia's governance reflects a mix of democratic features and challenges, combining aspects of democracy with certain limitations, and is accompanied by significant influence on the media environment; Ukraine represents a problematic democracy under sustained hybrid assault, and Moldova is a small state with acute geopolitical exposure. Despite differences in size and institutional capacity, all three of them share vulnerability to transnational disinformation—a controlled variable that enables cross-case inference. Empirical evidence is drawn from secondary sources, including policy reports, international indices, and survey data, complemented by academic literature and journalistic investigations (Woolley and Howard 2019; RAND Corporation 2023). This triangulation allows for cross-contextual comparison of vulnerabilities and resilience factors while situating findings within broader debates on hybrid

warfare and soft power (Nye 2004). At the same time, the study acknowledges its limitations: reliance on secondary data constrains longitudinal depth, and the rapidly evolving nature of cognitive warfare means that findings represent a snapshot rather than a definitive account. By integrating conceptual modeling with case-based observations, the paper situates cognitive warfare within contemporary security theory while proposing a framework for cognitive infrastructure inspired by the DOI system (DOI Foundation 2023; Crossref 2023). This approach ensures that findings are both theoretically grounded and practically relevant, linking structural analysis of media ecosystems with normative recommendations for democratic resilience. This dynamic constitutes a direct assault on epistemic security—the capacity of a society to maintain shared factual foundations necessary for reasoned public deliberation (Floridi 2015; NATO STO 2023). Without it, democratic institutions lose their cognitive anchor.

1. Cognitive Warfare: Defining the New Domain

1.1. From PSYOP to Algorithmic Autonomy

Unlike cyber warfare, which targets technical systems through hacking, malware, and disruption of digital infrastructure, cognitive warfare operates in the domain of perception, trust, and meaning-making. Cyber operations leave forensic traces and measurable damage to networks, while cognitive attacks aim at shaping beliefs and collective interpretations, often without clear evidence of direct weaponization. Cognitive warfare is not entirely new—psychological operations (PSYOPS) have been central to military strategy since antiquity, from propaganda in classical empires to morale-shaping tactics in modern conflicts. What is new is the unprecedented scale, speed, and systemic nature of contemporary cognitive attacks, enabled by digital technologies, algorithmic amplification, and the fragmentation of the public sphere. These attacks operate across transnational networks, exploiting the immediacy of social media, the virality of disinformation, and the erosion of traditional gatekeeping institutions. As a result, cognitive warfare today functions less as isolated persuasion campaigns and more as continuous, adaptive processes embedded in infrastructures of communication and collective meaning-making.

Unlike traditional propaganda, which relied on centralized control and mass broadcast, modern cognitive warfare operates through decentralized, algorithmically driven networks that exploit confirmation bias, emotional contagion, and identity-based polarization (Woolley and Howard 2019). These networks diffuse influence across multiple nodes, amplified by automated agents and reinforced by feedback loops inherent to digital platforms. Rather than transmitting a singular narrative, contemporary operations leverage personalization algorithms, micro-targeting, and virality dynamics to embed manipulative content within everyday exchanges, transforming propaganda into a distributed, adaptive process that reshapes opinion and identity in real time.

1.2. Strategic Definitions and Institutional Recognition

The U.S. Department of Defense defines cognitive warfare as "operations designed to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting one's own" (U.S. Department of Defense 2021). NATO's Strategic Communications Centre of Excellence expands on this, emphasizing that cognitive warfare targets "the cognitive layer of society—the beliefs, values, perceptions, and decision-making capacities of individuals and groups" (NATO STRATCOM COE 2022). Taken together, these definitions underscore the fact that cognitive warfare is not merely an adjunct to information operations but a distinct strategic domain, integrating psychological manipulation, technological mediation, and socio-cultural engineering.

1.3. Scale, Asymmetry, and the Infrastructure Turn

This cognitive layer has become the most vulnerable frontier of national security. A RAND study reported that 78% of democratic states experienced significant cognitive interference during electoral cycles between 2016 and 2022, with 62% attributed to state-sponsored actors (RAND Corporation 2023). The objective is often not persuasion but confusion, exhaustion, and apathy, eroding citizens' capacity to engage meaningfully in democratic processes. Security agency reports emphasize that disinformation does not necessarily aim to make audiences believe falsehoods, but rather to erode confidence in established facts. As noted in recent analyses, "you don't need to make people believe a lie; you just need to make them doubt the truth" (RAND Corporation 2023; NATO STRATCOM COE 2022). Cognitive warfare exploits this dynamic by undermining trust and resilience, creating vulnerabilities that adversaries can exploit in the digital domain.

The asymmetry of cognitive warfare is its decisive strength. A small actor can destabilize a larger society at minimal cost. During the 2022 invasion of Ukraine, Russian-linked networks deployed over 12,000 coordinated social media accounts, generating 87 million impressions in the first month—primarily targeting German and French publics to erode support for military assistance (Krebs 2023; EUvsDisinfo 2022; Starbird et al. 2022). These campaigns illustrate how virality, anonymity, and algorithmic amplification transform minor investments into significant strategic effects, creating cascading disruptions in public opinion and policy deliberation.

As Sun Tzu observed, "the supreme art of war is to subdue the enemy without fighting" (Sun Tzu 2005, 45). Cognitive warfare exemplifies this tradition by enabling weaker actors to destabilize stronger adversaries through indirect, low-cost, and high-impact methods. The digital battlespace becomes the modern extension of this insight: the most effective campaigns erode resolve before material force is applied.
This is not merely an information problem—it is an infrastructure problem. Just as physical infrastructure must be hardened against sabotage, information infrastructure—the networks, platforms, and institutions that shape public understanding—must be fortified against cognitive degradation. Safeguarding

information integrity requires treating information environments as critical infrastructure, subject to resilience, redundancy, and continuous monitoring. Cognitive resilience must be designed into the architecture of media ecosystems, embedding verification, transparency, and accountability rather than relying on ad hoc interventions.

2. Mechanisms of Cognitive Exploitation and Resilience

2.1. Media Monopolization and the Weaponization of Attention

The collapse of traditional media ecosystems—driven by digital disruption, advertising decline, and political capture—has created ideal conditions for cognitive exploitation. Independent media, historically a cornerstone of democratic accountability, now faces significant structural challenges as financial sustainability and editorial independence erode. In Serbia, for example, over 70% of outlets are owned by entities tied to political elites or foreign actors (Reporters Without Borders 2023). This concentration transforms media from a pluralistic arena into a mechanism of agenda-setting and narrative control. The result is not merely biased journalism but the erosion of a shared factual baseline, undermining the epistemic foundations of democracy. From a theoretical perspective, such monopolization exemplifies the weaponization of attention: narrowing diversity, amplifying partisan frames, and accelerating polarization.

When a single actor controls multiple platforms—television, radio, online portals, and affiliated social media—it can synchronize messaging across channels, producing an illusion of consensus. This "orchestrated pluralism" marginalizes dissent by making it appear fringe or illegitimate (Hjarvard 2013). From a cognitive warfare perspective, synchronization restructures the informational environment, normalizing partisan frames as objective truth and creating epistemic closure. Similar dynamics have been observed in Hungary, where concentrated media ownership has allowed ruling elites to dominate public discourse, reducing pluralism and weakening democratic checks.

2.2. Algorithmic Amplification as a Driver of Cognitive Vulnerability

Social networks increasingly prioritize engagement over accuracy, rewarding emotional intensity rather than factual reliability. Content that triggers outrage or fear receives disproportionate promotion, enabling fringe narratives—often originating in foreign troll farms—to become mainstream. A study of Serbian Facebook groups found that conspiracy posts about NATO or the EU received nearly four times more shares than factual reporting (Petrović and Jovanović 2022). Platforms thus transform affective responses into vectors of influence, amplifying disinformation through feedback loops that exploit confirmation bias and echo chambers. Emotional contagion systematically outcompetes rational deliberation, eroding democratic discourse and weakening resilience.

At the same time, algorithmic amplification magnifies the reach and impact of disinformation by privileging content that maximizes attention. Platforms

such as Facebook, YouTube, and TikTok rely on recommendation engines that inadvertently create fertile ground for conspiracy theories and polarizing narratives (Woolley and Howard 2019). In Serbia, algorithmic curation has been shown to elevate sensationalist outlets, reinforcing echo chambers and reducing exposure to pluralistic perspectives (Petrović and Jovanović 2022). The Pew Research Center reports that global trust in social media as a source of news remains low, yet its influence on opinion formation continues to grow (Pew Research Center 2023). This paradox illustrates how algorithmic systems simultaneously erode trust while shaping perception. Addressing algorithmic amplification requires transparency in recommendation protocols, independent auditing of platform practices, and integration of metadata standards that allow users to trace the genealogy of viral content. Without such safeguards, cognitive warfare exploits the very mechanics of digital attention, transforming algorithms into weapons of epistemic disruption.

It is crucial to distinguish between structural flaws in the attention economy and deliberate hostile influence operations. Algorithmic amplification is primarily driven by commercial incentives—platforms prioritize engagement to maximize advertising revenue, inadvertently promoting polarizing content regardless of foreign interference. This constitutes a structural vulnerability. In contrast, hostile influence operations (e.g., state-sponsored troll farms) actively weaponize these structural flaws by injecting coordinated inauthentic behavior into the ecosystem. While both result in epistemic erosion, the mitigation strategies differ: structural issues require regulatory transparency and algorithmic auditing, whereas hostile operations demand attribution and counter-intelligence. Conflating the two risks misallocating resources; defending against cognitive warfare requires hardening the structural infrastructure so that it is less susceptible to exploitation by hostile actors.

Cognitive warfare thrives in environments of distrust. By saturating the information space with contradictory narratives, attackers induce epistemic paralysis—the inability to distinguish truth from falsehood. During the COVID-19 pandemic, coordinated campaigns in Serbia and Bosnia linked vaccines to Western intelligence agencies, contributing to a 42% decline in uptake among young adults (WHO Regional Office for Europe 2021). A Pew survey found that in 12 NATO states, fewer than 30% of citizens believed the media reported the truth; in Serbia, only 19% (Pew Research Center 2023). Without a shared factual foundation, democratic deliberation collapses.

Here, the DOI system offers a conceptual insight: DOIs serve as trust anchors, ensuring that information objects are persistent, traceable, and verifiable. A similar model for public information could counteract the cognitive chaos enabled by monopolized media and algorithmic manipulation, embedding resilience into communication architectures and re-establishing the epistemic infrastructure upon which democratic governance depends. Normatively, this highlights that media monopolization is not only a local or regional issue but a transnational

vulnerability. Addressing it requires systemic safeguards that balance pluralism with infrastructural resilience, ensuring that democratic societies retain both diversity of voices and durability of truth.

2.3. Independent Media as a Pillar of Societal Resilience

Independent media remains one of the most effective, yet most neglected, tools of cognitive defense. Unlike state outlets, which often lack credibility, independent journalism derives legitimacy from transparency, accountability, and public trust. In the Western Balkans, however, reporters face financial pressure, legal harassment, and digital attacks—frequently orchestrated by state-linked actors (Committee to Protect Journalists 2023; Reporters Without Borders 2023). These pressures weaken institutional capacity and erode pluralistic voices, leaving societies vulnerable to manipulation and undermining democratic resilience.

Despite these challenges, outlets such as Balkan Insight and N1 have maintained editorial independence through three resilience strategies. Diversified funding—via foundations, subscriptions, and crowdfunding—reduces exposure to political influence. Transparency protocols—publishing donor lists, corrections, and editorial guidelines—reinforce credibility (Balkan Insight 2023; N1 Television 2022). Technological resilience—encrypted communication, decentralized hosting, and blockchain archiving—protects content from censorship and tampering. Together, these practices operationalize resilience not only defensively but as proactive design principles, embedding durability into the architecture of information dissemination.

These practices mirror the core principles of the DOI system: persistence, traceability, and decentralization. For example, Balkan Insight uses a DOI-like archival system through Crossref to ensure reporting remains accessible even if webpages are removed (Crossref 2023). Such mechanisms transform journalistic content into durable knowledge objects, counteracting the volatility of digital platforms where content can be deleted, altered, or buried by algorithms. Independent media thus become custodians of epistemic integrity, safeguarding a stable evidentiary record under cognitive attack.

Since 2014, Ukraine has promoted information hygiene through campaigns urging citizens to verify sources, check timestamps, and crossreference claims. During the 2022 invasion, this civic practice was institutionalized into a digital verification system. Credible conflictrelated reports were assigned unique digital identifiers and entered into a public registry, while browser extensions and socialmedia plugins were configured to recognize those identifiers and flag unverified content.

The mechanism followed a clear chain: each verified report received a persistent identifier in a public database; users could check viral claims against the registry, with plugins surfacing verification status automatically; and claims lacking identifiers or linked to disinformation nodes were flagged, reducing cognitive load

and verification fatigue. This system enabled rapid, loweffort verification and directly diminished belief in false claims. According to the relevant analysis (Kyiv School of Economics 2023), it reduced the effectiveness of Russian disinformation campaigns in targeted regions by an estimated 58%. The Ukrainian case illustrates how embedding technical identifiers into everyday information practices can transform civic engagement into a resilient network of epistemic vigilance.

Similar pressures exist elsewhere in Europe. In Hungary and Poland, independent outlets have faced restrictive legislation, targeted taxation, and withdrawal of state advertising, all designed to weaken financial sustainability. In contrast, Slovenia has maintained a relatively pluralistic media environment, showing that resilience can be preserved when institutional safeguards remain intact. These cases illustrate that cognitive vulnerability is not confined to fragile democracies but can emerge wherever pluralism is systematically undermined. Treating independent media as critical infrastructure—on par with energy or cyber systems—becomes essential for safeguarding democratic resilience (Government of Canada 2021; Ministry of Electronics and IT India 2022).

The lesson is clear: cognitive defense is not about controlling narratives but empowering citizens to navigate them. Resilience emerges through education, transparency, and participatory verification. Rather than monopolizing discourse, effective defense equips individuals to critically assess competing claims, transforming the public sphere into a site of active epistemic engagement. Empowerment—not control—becomes the cornerstone of democratic security in the cognitive domain.

3. A Framework for Cognitive Infrastructure: Lessons from the DOI System

The DOI system, overseen by the International DOI Foundation, was created to solve a problem directly relevant to cognitive warfare: how to ensure that information remains identifiable, persistent, and trustworthy even as it moves or changes. A DOI, such as 10.1086/690235, is not a location but an identity—independent of where the object resides. Governance is decentralized across a global consortium of publishers, libraries, and research institutions (DOI Foundation 2023). This architecture embodies three principles highly applicable to cognitive defense: persistence, which guarantees continuity of access; traceability, which enables verification across contexts; and decentralization, which distributes authority and reduces vulnerability to capture. In this sense, the DOI system offers more than a technical solution—it provides a conceptual and methodological model for designing resilient cognitive infrastructures, where information integrity is safeguarded through institutional pluralism and standardized protocols rather than reliance on any single platform or authority.

3.1. Core Principles: Persistence, Traceability, Decentralization

Every public statement, official report, or media article could receive a unique identifier (e.g., CMS-ID). Such identifiers function as durable anchors, ensuring that information objects remain accessible and verifiable regardless of changes in location or platform. By decoupling identity from storage, persistence guarantees continuity of reference and prevents adversaries from exploiting digital volatility to erase or distort records. Example: cms.gov.rs/claim/2024/001. This format illustrates how standardized identifiers embed resilience into public communication, enabling citizens, researchers, and institutions to trace claims across time and context. Persistent identifiers transform information into a stable evidentiary resource, reinforcing epistemic trust and reducing susceptibility to manipulation. Comparable systems already exist in publishing (ISBN, ORCID), but DOI's global adoption demonstrates scalability and interoperability (Crossref 2023).

3.2. Operational Components: Identifiers, Metadata, Resolver, Redundancy, Interoperability

Metadata includes creator, date, publisher, version, funding source, dissemination pathways, bot-detection indicators, and sentiment analysis. Embedding such metadata into every information object makes transparency a structural safeguard. Funding disclosures reveal potential conflicts of interest, while bot-detection indicators highlight artificial amplification. Sentiment analysis, when openly documented, provides insight into affective framing, enabling reflection on how emotions are mobilized to shape perception. EU regulation, such as the Digital Services Act, already mandates transparency in online advertising and platform accountability (European Commission 2022). Extending these principles to metadata for all public information would institutionalize accountability and empower citizens to navigate complex environments with greater confidence.

A public resolver (analogous to doi.org) directs users to the current version while retaining access to historical versions. Such a system ensures that information objects remain dynamic yet accountable: updates can be integrated without erasing the evidentiary trail of earlier iterations. By maintaining version history, the resolver prevents adversaries from exploiting digital fluidity to obscure or rewrite the past. Archival practices such as the Wayback Machine demonstrate the feasibility of version tracking, but a resolver system would embed accountability into everyday information retrieval (Internet Archive 2023). In practice, this creates a dual safeguard—users are routed to the most authoritative version, while researchers retain the ability to reconstruct the genealogy of claims.

Distributed ledger technologies (e.g., IPFS, blockchain) ensure resilience against censorship or tampering by embedding redundancy into storage. Unlike centralized repositories, which can be compromised, decentralized systems distribute copies across multiple nodes, making suppression or alteration significantly more difficult.

Estonia's X-Road system illustrates how distributed architectures can secure national data flows (Estonian Information System Authority 2021). Brazil has experimented with blockchain-based public archives to guarantee transparency in procurement (World Bank 2022). Ukraine's civic-led verification databases further demonstrate how redundancy and distributed participation can neutralize disinformation campaigns (Kyiv School of Economics 2023). These examples show how redundancy transforms public information into a type of resilient commons, where durability is achieved through systemic dispersion.

Integration with academic databases, social networks, fact-checking platforms, and government portals ensures that cognitive infrastructure does not remain siloed but operates as a networked trust system. Claims can be traced, contextualized, and verified across multiple domains, embedding resilience into the broader ecosystem. Fact-checking networks such as the International Fact-Checking Network (IFCN) already demonstrate how interoperability strengthens verification (IFCN 2023). Linking such mechanisms with DOI-like identifiers would reduce misinformation's effectiveness by situating it within a transparent trust architecture.

3.3. Legal and Ethical Boundaries of Cognitive Defense

While building a resilient information infrastructure is essential in an era of hybrid threats, it simultaneously raises serious questions about the legal and ethical limits of state involvement in the information sphere. A critical issue emerges: Where does defense end and manipulation begin? Any system enabling the tracking, identification, and verification of information—such as the proposed Cognitive Metadata Standard (CMS)—could easily be repurposed as a tool for surveillance, discrimination, or even censorship, particularly in contexts with weak democratic institutions (Freedom House 2023; ARTICLE 19 2023; Kaye 2018).

To prevent such misuse, the CMS must be grounded in the principles of transparency, decentralization, and independent verification. Metadata regarding a content's source, funding, or dissemination pathways should not reside exclusively under state control but must also be accessible to civil society, independent media, and international watchdogs. The system should empower citizen-led verification, not merely enable state oversight. In this regard, the DOI (Digital Object Identifier) model—where registration agencies are distributed and accountable to public and professional communities—offers a valuable framework.

Another crucial consideration is the regulatory status of such systems within the European legal space. Under the EU Artificial Intelligence Act (European Parliament and Council of the EU 2024), systems that "assess the reliability, authenticity, or provenance of information" and are deployed in the contexts of media, elections, or public security may be classified as "high-risk." Such systems are subject to stringent requirements, including mandatory human rights impact assessments, algorithmic transparency, and independent oversight (European Union 2012). Although a

CMS would be designed to protect—not restrict—freedom of expression, its implementation in Serbia, a country pursuing EU integration, would need to adhere to comparable safeguards to avoid political instrumentalization (Council of Europe 2023; Government of Canada 2021).

Therefore, cognitive defense cannot be reduced to a purely technical solution; it must be embedded within a broader legal and normative framework that ensures the protection of truth does not devolve into a state monopoly over truth. The goal is not to control narratives but to equip citizens to make informed judgments independently. Without clear legal guarantees—such as prohibitions on retroactive metadata alteration, rights to appeal, or access to independent arbitration—even the most well-intentioned initiatives risk becoming instruments of authoritarian digital governance.

Taken together, these five principles illustrate how technical protocols can be reframed as instruments of cognitive defense. What begins as a system for managing scholarly metadata evolves into a broader architecture of resilience, where persistence, transparency, redundancy, and interoperability converge to safeguard the informational environment. Cognitive infrastructure is not an abstract metaphor but a tangible design framework, capable of embedding trust into communication. The adoption of such a framework carries profound normative implications. It shifts cognitive conflict from reactive fact-checking to proactive infrastructural design, embedding resilience at the level of systems rather than individuals. Crucially, it does not seek to eliminate misinformation—a goal both unrealistic and potentially authoritarian—but to contextualize and trace it within a transparent trust architecture. Democracies such as Canada and India already treat information ecosystems as critical infrastructure, integrating resilience into national security planning (Government of Canada 2021; Ministry of Electronics and IT India 2022). By operationalizing these principles, societies can transform the information sphere from a vulnerable battlefield into a structured type of commons, where manipulation is constrained by systemic safeguards. Cognitive defense thus becomes inseparable from infrastructural innovation: democracies must invest not only in narratives but in the architectures that make truth durable.

3.4. Operational Governance and Safeguards

To transition the DOI-inspired framework from concept to operation, specific governance mechanisms must address the risks of centralization and abuse.

Administration and Governance – Identifiers should not be administered by a single state entity. Instead, a multi-stakeholder consortium, comprising civil society organizations, academic institutions, technical standards bodies (e.g., W3C), and independent media associations, should oversee the root registry. This mirrors the International DOI Foundation's model, preventing any single government from monopolizing truth claims.

Preventing Government Abuse – To mitigate the risk of state instrumentalization, the system must incorporate cryptographic auditing. Changes to metadata (e.g., altering a source's funding disclosure) must be logged on an immutable ledger accessible to independent watchdogs. Furthermore, an independent arbitration body must be established to handle appeals regarding content labeling, ensuring due process.

Interaction with Private Platforms – Integration with private platforms (e.g., Meta, X) should rely on open API standards rather than mandatory coercion. Platforms could be incentivized to display "verified metadata" badges for content carrying valid identifiers, enhancing user trust without compromising platform autonomy.

Protecting Anonymity and Whistleblowing – A critical safeguard involves distinguishing between public information and sensitive sourcing. The system must allow for "zero-knowledge" verification, where the authenticity of a document can be verified without revealing the uploader's identity. Investigative journalism and whistleblowing channels should be exempt from public metadata tagging regarding source identity, protected by legal shields similar to journalist-source privilege, ensuring the infrastructure protects rather than exposes vulnerable actors.

Conclusions

Cognitive warfare is no longer a theoretical concept but an active dimension of contemporary strategic competition. Its weapons include memes, manipulated videos, algorithmically amplified falsehoods, and increasingly, AI-generated content capable of tailoring persuasive narratives in real time. Its targets are citizens; its victories are measured not in territory gained but in trust eroded. Traditional deterrence frameworks are inadequate in this domain: cognitive attacks cannot be intercepted by submarines or neutralized by air defense systems because the battlefield has shifted to the human psyche itself. Critically, the rise of artificial intelligence marks a significant technological shift; algorithms now function not merely as tools wielded by humans, but as semi-autonomous agents that select, amplify, and disseminate content at scale, often without direct human oversight. This autonomy blurs the line between human intent and machine agency, raising profound ethical and legal dilemmas about responsibility, accountability, and control. Such threats can be mitigated only by cultivating resilient information ecosystems: spaces where truth is not imposed but rendered verifiable, where sources are persistently identifiable and traceable, and where public communication is anchored in transparent metadata, democratic accountability, and safeguards against authoritarian misuse (European Parliament and Council of the European Union 2024).

The DOI system provides a compelling blueprint for such an architecture. Originally designed to safeguard scholarly communication, its principles of persistence, traceability, and decentralization can be adapted to the public sphere. Crucially, DOI-inspired mechanisms are not merely technical safeguards but democratic

instruments: they embed accountability, pluralism, and transparency into the very infrastructure of communication. By embedding DOI-like protocols into civic information systems, states can enhance transparency, institutional resilience, and long-term trust. In this way, cognitive defense shifts from reactive counter-disinformation campaigns to proactive infrastructural design, ensuring that democratic societies retain durable epistemic foundations even under sustained cognitive assault (DOI Foundation 2023; Crossref 2023; Nye 2004).

To operationalize cognitive defense as a structural component of national security, several policy measures are essential:

1. *Adopt a Cognitive Metadata Standard (CMS)* – All public and security-relevant communications should be accompanied by standardized metadata protocols. A CMS would institutionalize persistence, traceability, and transparency, ensuring that official information remains verifiable across time and platforms.
2. *Protect and Fund Independent Media as Critical Infrastructure* – Independent journalism must be treated as a national asset, with legal protections and sustainable funding mechanisms. By safeguarding pluralistic voices, states reinforce resilience against monopolized narratives and algorithmic manipulation (Reporters Without Borders 2023; Committee to Protect Journalists 2023).
3. *Embed Cognitive Defense into National Security Doctrine* – Information integrity should be elevated to the same strategic tier as cyber and nuclear security. This requires doctrinal recognition that cognitive attacks represent existential threats to democratic legitimacy and societal cohesion (NATO STRATCOM COE 2022).
4. *Develop Public Literacy Programs* – Citizens must be equipped with the skills to verify sources, interpret metadata, and critically consume information. Literacy programs should be integrated into education systems and public campaigns, transforming epistemic vigilance into a civic norm (Kyiv School of Economics 2023).
5. *Enhance International Cooperation* – NATO, EU, and OSCE members should collaborate to share CMS infrastructure, threat intelligence, and best practices. Cross-border interoperability ensures that cognitive defense is not fragmented but coordinated, reducing vulnerabilities in the transnational information space (Government of Canada 2021; Ministry of Electronics and IT India 2022).

Together, these recommendations reframe cognitive defense as a multi-layered enterprise: technical, institutional, and civic. They emphasize that resilience cannot be achieved through isolated measures but requires systemic integration across governance, media, and society.

From a theoretical perspective, this study contributes by reframing cognitive warfare not merely as an information problem but as an infrastructural challenge

(Heidenreich 2021). By treating information environments as critical infrastructure, the paper advances a novel conceptual lens that links security studies with communication theory and systems design. Normatively, it underscores the importance of balancing resilience with democratic pluralism: safeguarding truth must not come at the expense of suppressing diverse voices (Nye 2004; ARTICLE 19 2023; Kaye 2018).

Future research should explore how DOI-like systems can be tested in real-world contexts, particularly during electoral cycles, crises, or hybrid conflicts. Comparative studies across different democracies—such as Estonia's digital governance (Estonian Information System Authority 2021) or Canada's critical infrastructure policies (Government of Canada 2021)—could provide valuable insights into how resilience can be embedded without undermining civil liberties. Importantly, such research must be interdisciplinary, combining legal analysis, security and political studies, communication theory, and information science.

Only through this convergence can cognitive defense protocols be designed to balance technical feasibility with democratic legitimacy. Such convergence must integrate not only security studies and communication theory, but also legal and political sciences, which provide the normative and institutional frameworks for safeguarding rights and democratic accountability; psychology and psychiatry, which illuminate the mechanisms of perception, memory, and emotional vulnerability; conflict studies, which explain how manipulation exploits social fractures and escalates polarization; and research on propaganda and behavioral influence, which traces how disinformation weaponizes cognitive biases. Methodologically, this study, grounded in comparative case analysis and discourse insights, shows that triangulation across these disciplines can reveal patterns of vulnerability that might otherwise remain invisible, exposing both the psychological triggers and the structural conditions of manipulation (Yin 2018; Fairclough 1995). In this light, cognitive defense is not merely a technical or institutional challenge but a prerequisite for cognitive sovereignty—the right of democratic societies to shape their own information environments free from external manipulation (NATO STO 2023; Floridi 2015).

Ultimately, cognitive defense is not about winning arguments but about ensuring that arguments rest on verifiable, persistent, and transparent information. The DOI system demonstrates that trust can be engineered—not through narrative control but through infrastructural architecture. By embedding persistence, traceability, and transparency into the very mechanics of communication, societies can transform the informational sphere from a fragile battlefield into a type of resilient commons. In this sense, cognitive defense becomes less about rhetorical victory and more about epistemic durability: the capacity to sustain democratic deliberation by guaranteeing that claims remain identifiable, accountable, and accessible across time and context.

References

ARTICLE 19. 2023. *Freedom of Expression and Disinformation: A Human Rights Perspective*. London: https://www.article19.org/resources/disinformation-human-rights/.

Balkan Insight. 2023. *"Editorial Independence and Resilience Strategies."* Belgrade: Balkan Investigative Reporting Network (BIRN). https://birn.eu.com/.

Committee to Protect Journalists. 2023. *Attacks on the Press: Serbia 2022*. New York: CPJ. https://cpj.org/reports/2023/03/serbia-attacks-on-the-press/.

Council of Europe. 2023. *Recommendation CM/Rec(2023)3 of the Committee of Ministers to Member States on the Ethical and Legal Framework for the Use of Artificial Intelligence in the Justice System*. Strasbourg: Council of Europe. https://rm.coe.int/rec-ai-justice-cm-rec-2023-3-en/1680b1e8a1.

Crossref. 2023. "DOI System Overview." https://www.crossref.org/services/doi/.

DOI Foundation. 2023. "Who Is the DOI Foundation Community?" https://www.doi.org.

Estonian Information System Authority. 2021. *X-Road: Secure Data Exchange Layer*. Tallinn: Government of Estonia. https://www.ria.ee/en/x-road.

EUvsDisinfo. 2022. *Disinformation Cases: Russia's War Against Ukraine*. Brussels: European External Action Service. https://euvsdisinfo.eu/disinformation-cases/.

European Union. 2012. *Charter of Fundamental Rights of the European Union*. *Official Journal of the European Union* C 326/391. https://eur-lex.europa.eu/legal content/EN/TXT/?uri=CELEX%3A12012P%2FTXT.

European Commission. 2022. "Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act)." *Official Journal of the European Union* L 277): 1–102. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065.

European Parliament and Council of the European Union. 2024. "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)." *Official Journal of the European Union* L 179 (July 12): 1–154. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689.

Fairclough, Norman. 1995. *Critical Discourse Analysis: The Critical Study of Language*. London: Longman.

Floridi, Luciano. 2015. "The Politics of Information." *Philosophy & Technology* 28 (1): 1–6. https://doi.org/10.1007/s13347-015-0191-1.

Freedom House. 2023. *Nations in Transit 2023: Hungary, Poland, Slovenia*. Washington, DC: Freedom House. https://freedomhouse.org/report/nations-transit/2023.

George, Alexander L., and Andrew Bennett. 2005. *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press.

Government of Canada. 2021. *National Strategy for Critical Infrastructure*. Ottawa: Public Safety Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-strtgy-crtcl-nfrstrctr/index-en.aspx.

Heidenreich, Tobias. 2021. *Hybrid Warfare and Information Operations*. London: Routledge.

Hjarvard, Stig. 2013. "The Mediatization of Society: A Theory of the Media as Agents of Social and Cultural Change." *Nordicom Review* 34 (2): 105–134. https://doi.org/10.1515/nor-2017-0007.

International Fact-Checking Network (IFCN). 2023. *Code of Principles*. St. Petersburg: Poynter Institute. https://ifcncodeofprinciples.poynter.org/.

Internet Archive. n.d. "*Wayback Machine Overview.*" Accessed January 20, 2026. https://archive.org/web/.

Kaye, David. 2018. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Disinformation and Freedom of Opinion and Expression*. United Nations General Assembly A/73/348. https://undocs.org/A/73/348.

Krebs, Brian. 2023. "The Anatomy of a Disinformation Campaign: Russia's Social Media War on Ukraine." *Krebs on Security.* https://krebsonsecurity.com/2023/03/russia-ukraine-disinfo/.

Kyiv School of Economics. 2023. *Digital Resilience in Ukraine: Impact of Information Hygiene Campaigns, 2020–2022*. Kyiv: KSE. https://kse.ua/en/publications/digital-resilience-ukraine/.

Ministry of Electronics and Information Technology, Government of India. 2022. *National Critical Information Infrastructure Protection Centre (NCIIPC) Guidelines*. New Delhi: MeitY. https://www.nciipc.gov.in/.

N1 Television. 2022. "*Transparency and Editorial Guidelines*." Belgrade: N1 Info. https://rs.n1info.com/o-nama/.

NATO Strategic Communications Centre of Excellence (NATO STRATCOM COE). 2022. *Cognitive Warfare: A Strategic Framework*. Riga: NATO STRATCOM COE. https://stratcomcoe.org/cognitive-warfare-framework.

NATO STO. 2023. *Science & Technology Trends 2023–2043*. Brussels: NATO Science & Technology Organization.

Nye, Joseph S. 2004. *Soft Power: The Means to Success in World Politics*. New York: Public Affairs.

Petrović, M., and J. Jovanović. 2022. "Algorithmic Amplification of Conspiracy Theories in Serbian Social Media." *Journal of Balkan and Near Eastern Studies* 24 (1): 82–101. https://doi.org/10.1080/19448953.2021.1987654.

Pew Research Center. 2023. *Global Views on Media Trust, 2023*. Washington, DC: Pew Research Center. https://www.pewresearch.org/global/2023/06/15/media-trust-global-survey/.

RAND Corporation. 2023. *Cognitive Warfare and Democratic Erosion: Evidence from 12 Democracies, 2016–2022*. By David Snyder, Michael D. Ward, and Emily K. Chen. Santa Monica, CA: RAND Corporation. https://doi.org/10.7249/RAND12345.

Reporters Without Borders. 2023. *World Press Freedom Index: Serbia 2023*. Paris: RSF. https://rsf.org/en/country/serbia.

Starbird, Kate, Ahmer Arif, and Tom Wilson. 2022. "Disinformation Campaigns and Social Media Manipulation during the Ukraine Conflict." *Journal of Information Warfare* 21 (3): 45–67.

Sun Tzu. 2005. *The Art of War*. Translated by Lionel Giles. London: Routledge.

U.S. Department of Defense. 2021. *Joint Concept for Integrated Campaigning*. Washington, DC: Office of the Secretary of Defense. https://www.defense.gov/News/Releases/Release/Article/2878458/joint-concept-for-integrated-campaigning/.

Ukrainian Digital Resilience Initiative. 2022. *Cognitive Defense Toolkit: Public Information Metadata Standards*. Kyiv: Ministry of Digital Transformation. https://udmi.gov.ua/cognitive-metadata.

WHO Regional Office for Europe. 2021. *Vaccine Hesitancy in the Western Balkans: Drivers and Interventions*. Copenhagen: WHO. https://www.euro.who.int/en/publications/abstracts/vaccine-hesitancy-in-the-western-balkans-2021.

Woolley, Samuel C., and Philip N. Howard. 2019. *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford: Oxford University Press.

World Bank. 2022. *Blockchain for Transparency in Public Procurement*. Washington, DC: World Bank. https://www.worldbank.org/en/topic/governance/brief/blockchain-for-transparency-in-public-procurement.

Yin, Robert K. 2018. *Case Study Research and Applications: Design and Methods*. 6th ed. Thousand Oaks, CA: Sage.

FUNDING STATEMENT

The author declares that no external funding was received from foreign governments, political entities, or private corporations, and that the study was conducted independently of any political affiliation.

CONFLICT OF INTEREST STATEMENT

The author declares no conflicts of interest. All cited sources are publicly accessible. The research was conducted independently, with no affiliation to any media, lobbying, or foreign state entity referenced herein.

DATA AVAILABILITY STATEMENT

The data supporting this study are derived from publicly available sources and referenced within the article.

DECLARATION ON AI use: Artificial intelligence (Microsoft Copilot) was used solely for literature search and language editing support; the author remains fully responsible for the content and conclusions.