Global Journal of Human-Social Science: H Interdisciplinary
Volume 25 Issue 4 Version 1.0 Year 2025
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-460X & Print ISSN: 0975-587X

Disrupting Perception, Shaping Conflict: Epistemic Power and Social Media Manipulation in Hybrid Digital Struggles

By Vusala Gulmaliyeva Logman Qizi

Institute of Philosophy and Sociology

Abstract- The evolution of modern conflict has increasingly shifted toward the digital domain, where perception, rather than territory, has become the central battlefield. This article conceptualizes cyber-based information warfare as an asymmetric and multidimensional form of conflict wherein state and non-state actors use social media, algorithmic amplification, and narrative engineering to influence public opinion and destabilize rival regimes. Drawing upon the epistemic power framework (Foucault, Castells, Zuboff) and the symbolic violence theory of Bourdieu, this paper develops a theoretical model that explains how platform dynamics reshape public perception and conflict behavior.

The study adopts a qualitative comparative approach, focusing on two major case studies: Russia's interference in the 2016 U.S. presidential elections and the Armenia–Azerbaijan digital conflict surrounding the 2020 war and its aftermath. It examines how social media manipulation—through disinformation campaigns, troll factories, and algorithmic distortions—transformed both public discourse and geopolitical narratives.

Keywords: *conflict strategies, escalation, de-escalation, post-conflict, governance.*

GJHSS-H Classification: *LCC Code: JZ1305-2060*

Strictly as per the compliance and regulations of:

Disrupting Perception, Shaping Conflict: Epistemic Power and Social Media Manipulation in Hybrid Digital Struggles

Vusala Gulmaliyeva Logman Qizi

Abstract- The evolution of modern conflict has increasingly shifted toward the digital domain, where perception, rather than territory, has become the central battlefield. This article conceptualizes cyber-based information warfare as an asymmetric and multidimensional form of conflict wherein state and non-state actors use social media, algorithmic amplification, and narrative engineering to influence public opinion and destabilize rival regimes. Drawing upon the epistemic power framework (Foucault, Castells, Zuboff) and the symbolic violence theory of Bourdieu, this paper develops a theoretical model that explains how platform dynamics reshape public perception and conflict behavior.

The study adopts a qualitative comparative approach, focusing on two major case studies: Russia's interference in the 2016 U.S. presidential elections and the Armenia–Azerbaijan digital conflict surrounding the 2020 war and its aftermath. It examines how social media manipulation—through disinformation campaigns, troll factories, and algorithmic distortions—transformed both public discourse and geopolitical narratives.

Empirically grounded and theoretically informed, the article addresses a key gap in political science literature by linking epistemic control to conflict escalation in hybrid digital struggles. It also evaluates the normative and legal implications of such practices, highlighting the urgent need for algorithmic transparency, media literacy, and updated regulatory frameworks. The findings suggest that contemporary information warfare is not merely a technical or operational threat but a strategic mode of exercising ideological power in the digital age.

By situating information warfare at the intersection of technology, discourse, and geopolitics, this article contributes to an emerging research agenda on epistemic contestation and hybrid warfare in international relations.

Keywords: conflict strategies, escalation, de-escalation, post-conflict, governance.

I. Introduction

In the contemporary digital era, conflict no longer unfolds solely through physical violence or conventional warfare. Instead, a growing share of geopolitical competition is taking place across algorithmically structured platforms and within epistemic spaces shaped by information flows, narratives, and perception management. Modern conflicts are increasingly shaped by hybrid forms of confrontation where information, rather than force, becomes the primary vector of influence. This transformation has blurred the traditional distinction between war and peace, between domestic and international politics, and between state and non-state actors.

The central aim of this article is to explore how cyber-based information manipulation—particularly via social media algorithms, bot networks, and narrative warfare—functions as a non-kinetic yet powerful instrument in shaping both public perception and the structural dynamics of modern geopolitical struggles. Drawing upon the theoretical frameworks of epistemic power (Foucault, 1980; Castells, 2009; Zuboff, 2019) and symbolic violence (Bourdieu, 1991), this study interrogates the mechanisms through which states and non-state actors alike deploy digital platforms to alter strategic narratives, disrupt social cohesion, and undermine epistemic trust.

Despite the growing literature on cyberwarfare, significant gaps remain in the understanding of how digital information operations intersect with broader conflict dynamics and platform governance. Previous studies have focused either on technical cyberattacks (Valeriano & Maness, 2015; Gartzke, 2013) or on isolated cases of disinformation. However, less attention has been paid to the structural role that platform dynamics, algorithmic visibility, and affective manipulation play in transforming modern conflicts into epistemic battles. Furthermore, normative frameworks addressing legal and ethical accountability in such contexts remain underdeveloped.

This paper addresses the following research question: How does information warfare —particularly through social media and algorithmic manipulation — transform the structure of modern conflicts and influence the formation of public opinion? The article advances the argument that epistemic power, operationalized through digital infrastructure, enables both state and non-state actors to control perception, engineer legitimacy, and engage in non-traditional forms of influence that can shape the trajectory of conflict itself.

Empirical analysis focuses on two key case studies: (1) Russia's strategic use of disinformation during the 2016 U.S. presidential election, and (2)

Author: Researcher at the Department of Ethics, Institute of Philosophy and Sociology, ANAS. e-mail: vusalagulmaliyeva86@mail.ru
ORCID: 0009-0006-4572-2455

Armenia–Azerbaijan information campaigns during and after the 2020 Nagorno-Karabakh war. By analyzing these episodes through the lens of epistemic conflict and platform governance, this study contributes to a growing body of scholarship at the intersection of international security, communication studies, and critical technology theory. In doing so, it also proposes ethical and legal recommendations for mitigating algorithmic manipulation, strengthening media resilience, and rethinking information sovereignty in an increasingly digitized world.

II. Theoretical Framework: Epistemic Power, Platform Dynamics, and the Weaponization of Information

Understanding contemporary information warfare requires moving beyond a purely technological or tactical interpretation. Instead, it must be viewed through the lens of "epistemic power relations", "discursive hegemonies", and "platform structures". Information does not circulate neutrally; its production, dissemination, and reception are shaped by socio-technical architectures and ideological filters (Foucault, 1980; Castells, 2009).

Michel Foucault (1980) introduces the concept of "regimes of truth" to explain how dominant actors construct and institutionalize what counts as 'truth' in society—not through coercion, but through the organization of knowledge. In this context, information warfare becomes a strategic form of "modern epistemic governance": What we see, what we consider credible, and what demands public concern are all shaped by intentional information structures.

Shoshana Zuboff (2019) builds on this by conceptualizing the era of **surveillance capitalism**, where digital platforms collect vast behavioral data and leverage it to influence human decision-making. In such a system, information becomes both an **economic asset** and a **political instrument**, creating new forms of power beyond traditional state structures.

Pierre Bourdieu (1991) defines control over information and discourse as a form of **symbolic violence**—a soft but pervasive form of domination that operates through social and linguistic normalization. Judith Butler's (2005) performativity theory similarly argues that repeated discursive acts do not merely reflect reality but actively construct it.

Information warfare, particularly via social media, is thus not only about disinformation but about **ideological engineering**. Content becomes a weapon, shaping public consciousness not through force, but through frames, metaphors, and symbolic representations that reconfigure perception.

In the networked society, digital platforms do not simply transmit information; they filter, amplify, and prioritize it based on algorithmic criteria. Castells (2009) explains how network logics structure modern power, while Gillespie (2018) and Karpf (2024) describe platforms like Facebook, X (formerly Twitter), and YouTube as **algorithmic gatekeepers**.

Studies show that emotionally charged, misleading, or polarizing content is systematically prioritized by platform algorithms (Vosoughi, Roy, & Aral, 2018). This creates an **information ecosystem** where virality is rewarded over truth, enabling disinformation to spread rapidly, shape public discourse, and erode trust in institutions. In such a context, platforms are not neutral actors but **active participants** in contemporary conflict.

The field of political science has increasingly focused on how **information operations** intersect with cyber conflict. Scholars like Gartzke (2013), Valeriano & Maness (2015), and Rid (2020) point to the strategic use of digital technologies in shaping conflict trajectories. These studies emphasize that information warfare is not merely a set of isolated attacks, but a **systematic component** of modern geopolitical rivalry.

In this framework, the power to influence perception becomes central to conflict: states and non-state actors alike seek not only to dominate the physical battlefield but also to shape the **narrative terrain**. Epistemic power, then, is about controlling access to visibility, legitimacy, and meaning in digital arenas.

III. Methodology

This research adopts a **qualitative interpretivist case-study methodology**, grounded in critical political analysis. The central aim is to explore how cyber-enabled information warfare functions as a strategic tool in contemporary conflicts. In particular, the study investigates how digital instruments are mobilized to construct narratives, establish symbolic dominance, and organize discursive disruptions. Unlike traditional operational approaches that focus narrowly on cyberattacks or digital infrastructure sabotage, this research positions information warfare within broader political, ideological, and societal dimensions.

Situated at the intersection of political science, critical security studies, and media theory, the methodological framework is fundamentally **multidisciplinary**. It enables an in-depth understanding of information warfare not only as a component of national security strategies but also as a mechanism for shaping public opinion, manipulating collective memory, and influencing identity politics. By combining interpretive approaches with empirical examination, this study analyzes how digital platforms and technologies enable new forms of political power and turn the **informational domain itself into a contested battlespace**.

The empirical component of the study centers on two purposefully selected cases:

1. **Russia's cyber and information operations during the 2016 U.S. presidential election**
2. **Information warfare and cyber tactics in the Armenia–Azerbaijan conflict (particularly the 2020 war)**

These cases have been selected according to the following criteria:

"Strategic significance" in cyber conflict literature and international security studies.

"Availability of Open-Source Intelligence (OSINT" and digital forensics data.

"Relevance to hybrid conflict frameworks" and the analytical potential to reflect non-conventional, yet systematic forms of conflict.

The comparative lens aims to identify both similarities and divergences in the deployment of information warfare tactics across diverse geopolitical and socio-political environments. The inclusion of one global-level (Russia–US) and one regional-level (South Caucasus) conflict allows the study to capture variation in digital conflict intensity, platform usage, and discursive strategy.

This research employs a **triangulated methodological strategy**, drawing upon the following analytical tools:

Critical Discourse Analysis (CDA): Applied to social media campaigns, political speeches, visual content, and official state communications to assess narrative construction and symbolic framing;

Process Tracing: Used to map the chronological development and escalation of cyber operations and information campaigns, identifying patterns of coordination and strategic escalation;

Secondary Data Synthesis: Incorporates data from cybersecurity threat reports (e.g., FireEye, CrowdStrike), academic publications, cyber conflict datasets (e.g., DCID), and policy documents from governmental and non-governmental institutions.

This combination allows for a **multi-dimensional understanding** of information warfare's mechanics and effects across digital and geopolitical spaces.

IV. Theoretical Framework

The theoretical lens guiding this research integrates insights from **Michel Foucault's theory of knowledge/power**, **Pierre Bourdieu's concepts of symbolic capital and symbolic violence**, and the cyber conflict literature of scholars such as **Valeriano, Maness**, and **Gartzke**. These frameworks allow for a non-material, epistemically informed understanding of how information is used not merely for communication or sabotage, but as a tool for **cognitive and sociopolitical control**.

Drawing from Foucault's notion of "regimes of truth," the study examines how dominant actors construct accepted realities through digital discourse. Bourdieu's theory offers a lens to understand **how digital information becomes a vehicle of symbolic violence**, shaping public opinion in subtle, often unrecognized ways. The work of Valeriano and Maness (2015), as well as Gartzke (2013), complements this by situating cyber operations within state strategic behavior and deterrence theory.

In essence, the methodology is built to examine how **epistemic power functions** in digital conflicts: who controls narrative production, what counts as "truth" in mediated conflict zones, and how platform affordances amplify or distort conflict dynamics.

a) *Case One: Russia's Information Operations and the 2016 U.S. Presidential Election*

The 2016 U.S. presidential election represents a paradigmatic example of hybrid information warfare in the digital age. Unlike conventional interstate conflict, this operation relied not on kinetic force but on epistemic disruption, aiming to undermine public trust, manipulate political discourse, and shape electoral outcomes through strategic use of digital platforms. The Russian campaign, as documented by the U.S. Senate Intelligence Committee (2019), combined cyber intrusion, disinformation, and social media amplification to create an ecosystem of confusion, polarization, and delegitimization.

A central component of the campaign was the Internet Research Agency (IRA), a Russian entity that operated thousands of fake accounts across Facebook, Twitter (now X), YouTube, and Instagram. These accounts impersonated American citizens, posed as activists from both ends of the political spectrum, and disseminated divisive content on topics such as race, immigration, religion, and gun rights (DiResta et al., 2018). This strategy reflects Foucault's notion of **"truth regimes"**, where dominant actors construct and disseminate selective knowledge structures to frame social reality (Foucault, 1980).

Through algorithmic amplification, emotionally charged disinformation outperformed factual content, exploiting the commercial logic of platform engagement metrics (Zuboff, 2019). Hashtags like #MAGA and #BlackLivesMatter were simultaneously co-opted by opposing bots to intensify social fragmentation. This reflects what Valeriano and Maness (2015) call **"strategic restraint through digital chaos"** — where the attacker achieves goals not through coercion, but by distorting information flows.

Importantly, the Russian operation did not aim to support one candidate exclusively, but rather to erode democratic legitimacy. As Benkler et al. (2018) demonstrate, the most impactful content was designed to deepen distrust in mainstream media, electoral

institutions, and political elites. This aligns with Nye's (2011) theory of **soft power inversion** — when information is weaponized to weaken trust rather than promote attraction.

While traditional cybersecurity focused on technical defenses, the 2016 case revealed the vulnerability of democratic epistemic infrastructures. The Russian operation relied on **platform asymmetry**: Western social media companies prioritized growth and engagement, failing to recognize their platforms as arenas of geopolitical contestation. As Gillespie (2018) argues, algorithms that elevate provocative content inevitably benefit those who aim to disrupt, not inform.

This case illustrates that information warfare is not merely about access to data but about **shaping the architecture of perception**. The Russian operation demonstrated how digital manipulation could achieve strategic impact without physical intervention — undermining institutional credibility, inflaming societal cleavages, and influencing political behavior. It marks a shift from coercion to cognition, from military power to epistemic power.

b) *Case Two: The Armenia–Azerbaijan Conflict and the 2020 Information War***

The 2020 Second Nagorno-Karabakh War between Armenia and Azerbaijan not only reignited long-standing territorial tensions but also inaugurated a new phase of hybrid warfare, in which digital information operations played a central strategic role. While conventional military engagements unfolded on the battlefield, a parallel struggle for narrative dominance and international legitimacy took place across digital platforms — notably Telegram, Facebook, YouTube, and Twitter.

Unlike the U.S.–Russia case, which targeted democratic institutions through epistemic destabilization, the Armenia–Azerbaijan conflict featured a dual-track information war: **internal mobilization and external legitimation**. Both sides deployed extensive social media campaigns to galvanize domestic support, demonize the adversary, and attract sympathy from the global public. This effort included the circulation of battlefield videos, nationalistic imagery, and emotionally charged rhetoric, often blurring the line between factual reporting and strategic propaganda (Sambaluk, 2020).

Telegram emerged as a critical vector in this conflict. Its encrypted architecture and decentralized distribution mechanisms enabled both state and non-state actors to disseminate unverified videos, casualty reports, and victory claims faster than traditional media outlets. These communications were not merely informative — they were **performative** acts aimed at shaping public morale and international perception. Butler's theory of **performativity** helps explain how repetitive dissemination of emotionally framed content constructs conflict narratives and solidifies national identities (Butler, 2005).

Visual manipulation was especially prominent. For example, clips from video games such as *Arma 3* were misrepresented as real war footage, and circulated to provoke emotional reactions and misinform audiences — a phenomenon also reported by BBC (2020). This reveals what Virilio (1998) calls the **"logistics of perception"**: in contemporary conflict, control over images and their timing becomes as powerful as control over territory.

Moreover, both governments actively shaped information flows. Azerbaijan's Ministry of Defense managed real-time battlefield updates, while Armenia's official channels emphasized victimization narratives and civilian suffering. Meanwhile, decentralized actors — including diaspora communities and nationalist influencers — flooded social platforms with hashtags, memes, and videos, creating **multi-nodal epistemic pressure**.

The conflict's information dimension also highlighted **algorithmic asymmetry**. Content moderation systems on global platforms, largely calibrated to Western political contexts, often failed to account for the historical, linguistic, and cultural specificities of the Caucasus region. As Flew (2021) notes, global tech infrastructures are ill-equipped to manage politically sensitive content in non-Western conflict zones — a dynamic that creates **epistemic inequity**.

The strategic objective, beyond battlefield success, was to control the **legitimacy narrative**. As Nye (2011) argues, soft power is rooted in attraction and credibility. In this case, both Armenia and Azerbaijan vied to appear as rightful actors before the international community, leveraging digital storytelling, selective truth-framing, and image curation.

This case exemplifies how modern information warfare operates across three levels: (1) **tactical**, through dissemination of real-time battlefield media; (2) **strategic**, by constructing dominant narratives; and (3) **epistemic**, by shaping what global audiences perceive as "truth." Unlike traditional kinetic war, victory here is not only territorial — it is **symbolic**, discursive, and digital.

V. Discursive Power and Epistemic Conflict

Contemporary information warfare is not merely a technological or tactical phenomenon; it operates on deeply discursive and epistemic planes as a structured form of power. In this regard, the notion of *epistemic conflict* becomes increasingly relevant. Epistemic conflict refers to the ideological and technological struggle between competing actors over what

constitutes "truth," which information is considered credible, and how societies define their shared sense of reality. This contest unfolds not through direct coercion but via the shaping of meaning, symbolic authority, and strategic narrative construction.

Michel Foucault's (1980) concept of "regimes of truth" is particularly salient here, illustrating how dominant power structures throughout history have constructed their own versions of reality not solely through force but through the organization and circulation of knowledge. Information warfare, in this light, becomes a strategic means of producing epistemic authority: determining what is visible, what is credible, and what provokes concern within a given sociopolitical context.

In today's geopolitical landscape, actors such as Russia and China do not simply disseminate information—they construct comprehensive informational ecosystems to frame specific ideas of "threat," "peace," and "enemy." This transcends disinformation; it constitutes the *design* of truth. Consequently, information warfare shifts from mere distortion of facts to the fabrication of coherent yet strategically manipulated realities.

This shift coincides with the emergence of the post-truth era, in which emotional appeals and personal beliefs increasingly override objective facts in shaping public opinion. Information warfare in this context does not merely involve the manipulation of data—it constructs *alternative realities*. The implications are profound: rational public discourse weakens, populist leaders rise, and political polarization deepens.

Shoshana Zuboff (2019) argues that in the age of surveillance capitalism, information is no longer just an economic commodity but a political instrument of control. Digital platforms collect behavioral data to predict and influence user behavior, often serving as tools for epistemic manipulation. Therefore, the epistemic conflict is no longer exclusive to state actors—technology companies have emerged as central epistemic authorities capable of shaping both knowledge and belief.

Epistemic power resides not only in the circulation of information but in the infrastructures that control its flow. Asymmetries emerge when some actors are able to restrict, decontextualize, or algorithmically amplify content in ways others cannot. This imbalance can be observed at both national and transnational levels. Those who control access points—platforms, algorithms, and trending mechanisms—become the primary architects of truth. As Michael Sambaluk (2019) notes: *"Whoever controls the trend controls the narrative, and ultimately the will of the people"*.

In this epistemic struggle, media literacy becomes a vital defense. Critical thinking is not merely a cognitive skill; it is an epistemic practice—a form of resistance against manipulation. In Scandinavia, for example, epistemic power is organized more transparently and pluralistically. Strong civil society institutions, public education in media ethics, and open access to diverse viewpoints create resilience against disinformation. In contrast, centralized control of information in authoritarian regimes amplifies epistemic asymmetry and suppresses competing truths.

Crucially, epistemic conflict manifests differently across political regimes. Authoritarian systems often centralize control over information, concentrating epistemic power in the hands of the state and leaving little room for alternative narratives. In democratic systems, although pluralism exists, the saturation of competing information under post-truth conditions fosters confusion and accelerates the spread of disinformation. Thus, epistemic conflict is both a product of information abundance and its monopolization.

VI. The Role of Global Platforms and Algorithmic Accountability

One of the defining characteristics of modern information warfare is the shift of the battlefield from interstate arenas to technological platforms. Social media platforms—Facebook (Meta), X (formerly Twitter), YouTube (owned by Google), TikTok, and Telegram—are no longer passive carriers of communication. Instead, they have become powerful global actors that influence public opinion, political polarization, and the trajectory of contemporary conflicts (Fuchs, 2021).

The core logic of these platforms is driven by attention-maximizing algorithms. Designed to prioritize emotionally charged, polarizing, and viral content, these algorithms inadvertently create an ideal environment for disinformation and psychological manipulation (Gillespie, 2018). Research by Vosoughi, Roy, and Aral (2018) has shown that false information spreads six times faster than accurate news, reinforcing an environment where virality supersedes veracity.

In several documented cases, platforms have either indirectly facilitated or failed to curb information warfare. For instance:

*Facebook's delayed response to Russian troll networks during the 2016 U.S. election (Aral & Eckles, 2018);

*TikTok's content moderation linked to Chinese state interests and censorship (Flew, 2021);

*YouTube's algorithmic amplification of polarizing and conspiratorial content (Gillespie, 2018).

Telegram represents a unique case in this ecosystem. With its end-to-end encryption, anonymous channels, and limited content moderation, Telegram has become a hub for both state-sponsored propaganda and non-state radical content (Fuchs, 2021). During the 2020 Nagorno-Karabakh conflict, both Armenian and Azerbaijani actors used Telegram to disseminate battlefield videos, patriotic messages, and propaganda.

Often, content circulated before official verification, blurring the lines between reality and psychological warfare.

This dynamic illustrates the dual-edged nature of algorithmic amplification. Platforms influence what is seen and by whom, reshaping visibility hierarchies and reinforcing echo chambers. As Karpf (2024) argues, *"algorithmic warfare" transforms networked propaganda into a structural feature of the digital sphere rather than an aberration*.

In addition, the absence of ethical moderation by platforms has enabled hate speech, dehumanizing content, and identity-based violence to thrive. Telegram's reluctance to moderate content during the Nagorno-Karabakh war highlights the platform's failure to assume ethical responsibility.

Another pressing issue is the application of universal algorithms to highly localized and culturally specific contexts. Western-based technology firms often apply content moderation and recommendation engines without sensitivity to the historical, ethnic, and geopolitical realities of regions such as the South Caucasus and Central Asia (Flew, 2021). This creates distortions and vulnerabilities, as algorithmic governance ignores the political nuances of these conflict zones.

Therefore, platforms must no longer be viewed as neutral intermediaries. They are now infrastructural actors in the geopolitical information struggle. Calls for algorithmic transparency, localized content policies, and legal accountability are not only ethical imperatives—they are strategic necessities for global information security.

VII. Legal and Ethical Perspectives of Information Warfare

The rise of information warfare (IW) as a central instrument of modern conflict presents unprecedented challenges to both international law and normative ethics. Unlike conventional armed conflicts—which are governed by well-established legal frameworks such as the UN Charter, Geneva Conventions, and customary international humanitarian law—cyber and informational operations often fall into legal grey zones. These operations are typically non-lethal, non-kinetic, and transnational in nature, thereby eluding the traditional criteria used to define acts of war or aggression.

One of the core legal challenges in regulating IW is **attribution**—the difficulty of assigning responsibility to a particular state or actor for cyber or disinformation campaigns. In conventional warfare, identifying the aggressor is often straightforward. However, in information warfare, actors operate through pseudonymous accounts, automated bots, or non-state proxies, complicating the application of *jus ad bellum* principles. The Tallinn Manual 2.0, developed by a group of legal scholars and commissioned by NATO, highlights that state responsibility in cyber operations requires clear evidence of direction, control, or acquiescence. Yet in practice, this standard is rarely met due to the covert and decentralized nature of digital interventions.

The 2016 Russian interference in the U.S. presidential election, for instance, involved troll farms and fake social media profiles rather than official military operations. Despite widespread acknowledgment of Russian involvement by intelligence agencies (U.S. Senate Report, 2019), the legal consequences remained minimal due to the absence of binding mechanisms for accountability in the information domain. This case underscores the **disconnect between legal theory and digital reality**, a gap that leaves liberal democracies vulnerable to cognitive subversion without clear legal remedies.

Furthermore, the UN Charter's Article 2(4) prohibits the use of force against the territorial integrity or political independence of any state. But whether coordinated disinformation campaigns—targeting public trust in electoral processes or sowing societal discord—constitute a violation of sovereignty remains a subject of intense debate. The International Court of Justice has recognized *non-intervention* as a principle of customary international law, yet the application of this principle to online influence operations remains unsettled.

Additionally, international legal norms such as the **prohibition on propaganda for war** (Article 20 of the International Covenant on Civil and Political Rights) are limited in scope and lack strong enforcement mechanisms. In essence, international law has **yet to catch up** with the speed, complexity, and ambiguity of information operations in the digital age.

Beyond legality, information warfare poses serious **ethical dilemmas**, particularly in democratic societies that value freedom of speech and open information flows. Traditional warfare involves physical harm, but IW targets cognitive structures—beliefs, emotions, and perceptions. When individuals are manipulated without their awareness, the ethical breach becomes both **invisible and profound**.

Jürgen Habermas (1984) has long argued that democratic legitimacy depends on *deliberative public spheres* where rational discourse and informed consent are possible. Information warfare undermines this principle by flooding digital spaces with emotionally charged disinformation, polarizing content, and algorithmically amplified falsehoods. Individuals are not merely misinformed—they are structurally conditioned to trust sources that reaffirm their biases and distrust dissenting views.

This **erosion of epistemic autonomy** has far-reaching implications. When citizens can no longer distinguish between fact and fabrication, democratic

participation loses its meaning. The *echo chamber* and *filter bubble* effects (Sunstein, 2017) reinforce epistemic isolation, further weakening the ethical foundation of democratic deliberation.

Even more troubling is the role of private technology companies in enabling or even profiting from these dynamics. Platforms such as Facebook, YouTube, and Twitter have been criticized for failing to regulate harmful content or for engaging in selective moderation. Their algorithms, optimized for engagement and profitability, often prioritize divisive, sensationalist content over accuracy or social responsibility (Zuboff, 2019). In doing so, they act not merely as neutral intermediaries but as **structural participants in epistemic conflict**.

A growing body of scholarship has called for the ethical regulation of platforms under the principles of **algorithmic accountability**, **content neutrality**, and **procedural justice** (Gillespie, 2018; O'Neil, 2016). If social media platforms function as digital public spheres, then they must also uphold democratic values—including transparency, fairness, and respect for pluralism.

From an ethical standpoint, there is a pressing need to differentiate between *harmful misinformation* and legitimate political dissent. Overregulation risks suppressing dissenting voices, while underregulation enables the viral spread of hate speech, incitement, and foreign propaganda. This tension demands nuanced, context-sensitive policies that go beyond simplistic binary filters.

The ethical framework for IW must also consider the **intent** and **impact** of information campaigns. For example, simulated war footage disseminated on social media platforms during the 2020 Nagorno-Karabakh conflict was found to originate from video games such as *Arma 3* and *Call of Duty*. These were circulated as real combat visuals, misleading audiences and stoking nationalist sentiments (BBC, 2020). The ethical harm lies not only in misinformation but in the **emotional mobilization** of populations for war through fabricated visual stimuli.

In such contexts, *visual ethics* becomes critical: the aesthetic presentation of conflict is no longer incidental but instrumental. Images are no longer passive representations—they are active participants in war discourse. Paul Virilio (1998) refers to this as the "logistics of perception," where perception itself becomes a battlefield manipulated through speed, repetition, and emotional intensity.

Recent studies in political communication and media theory emphasize the centrality of emotion—particularly fear, anger, and outrage—in shaping digital political behavior. In the context of information warfare, affective dynamics function as a strategic resource for both state and non-state actors seeking to mobilize publics and reinforce epistemic hierarchies.

Building upon the work of Sara Ahmed (2004) and Zizi Papacharissi (2015), emotions are not passive byproducts of discourse but active forces that circulate, attach, and intensify meaning within digital platforms. Ahmed introduces the notion of "affective economies", wherein emotions "stick" to signs, symbols, and narratives, generating political orientations. Similarly, Papacharissi argues that affective publics, shaped by algorithmically curated content, can rapidly mobilize in response to emotionally resonant messages—thus transforming isolated feelings into collective action.

In the context of the 2016 U.S. election, Russian troll farms exploited affective triggers to engineer distrust, racial tension, and ideological polarization. Content that elicited outrage—on immigration, religion, or national identity—received disproportionate engagement, indicating that emotional intensity often supersedes factual accuracy in algorithmic amplification.

The 2020 Armenia–Azerbaijan digital conflict likewise relied heavily on emotionally charged visuals, patriotic rhetoric, and real-time war footage—disseminated to generate solidarity, fear, or moral outrage. These tactics underscore how emotive narratives shape both domestic cohesion and international perception, particularly in environments of geopolitical volatility.

In sum, affect functions as symbolic ammunition in epistemic conflict. Rather than merely conveying emotion, digital media architectures are designed to amplify affect, creating feedback loops where perception, emotion, and identity become entangled. Recognizing this dynamic is essential for understanding how information warfare reshapes conflict not only cognitively but emotionally—turning emotion into an instrument of soft coercion.

Given the inadequacy of existing legal norms, scholars have proposed the creation of **a dedicated legal and ethical framework** for information warfare. This framework could include:

***The Principle of Distinction**:* Separating legitimate political speech from psychological warfare;

***The Principle of Proportionality**:* Ensuring that information interventions do not cause disproportionate cognitive harm;

***The Principle of Necessity**:* Limiting strategic communications to contexts of legitimate self-defense or national interest.

In parallel, **institutional resilience** must be enhanced through public education, independent fact-checking, algorithmic transparency, and international cooperation. Without such efforts, liberal democracies risk being destabilized not by external military threats but by **internal epistemic corrosion**.

Finally, the redefinition of core concepts such as **sovereignty**, **agency**, and **legitimacy** is

essential. If perception and belief become the new terrain of warfare, then political theory, ethics, and law must evolve accordingly. The future of international order may well depend on how societies regulate—not only the movement of weapons—but the movement of meaning.

The increasing reliance on algorithmic systems to curate, filter, and amplify content has transformed digital platforms into infrastructures of perception. As digital intermediaries mediate not only access to information but also visibility, credibility, and salience, they have become governing agents in the epistemic domain.

Drawing upon Foucault's concept of "governmentality" and Zuboff's critique of "surveillance capitalism", algorithmic governance can be understood as a non-coercive yet deeply structuring form of power. It operates through the calibration of what users see, what is recommended, and what is concealed. This hierarchy of visibility profoundly affects how publics interpret conflict, legitimacy, and political threat.

Platforms such as Facebook, X (formerly Twitter), YouTube, and TikTok do not merely host content—they prioritize virality over veracity. Emotionally charged, polarizing, or misleading content is algorithmically elevated due to its high engagement potential (Vosoughi et al., 2018). Consequently, disinformation is not just a matter of falsehood, but of systemic amplification engineered into platform architecture.

This form of governance is largely opaque and unaccountable. Users are rarely aware of how algorithms shape their informational environment, creating what some scholars refer to as algorithmic epistemologies—a condition in which knowledge and truth are indirectly curated by non-human decision systems designed for profit maximization.

During the Armenia–Azerbaijan conflict, for example, Telegram's unmoderated channels and real-time forwarding dynamics created a digital battleground of visual dominance, where perception of victory or victimhood was shaped before facts could be verified. This illustrates how algorithmic affordances not only enable information flows but structure symbolic warfare.

Understanding modern conflict thus requires an epistemic shift: from analyzing content to analyzing infrastructures of perception. Algorithmic governance is not politically neutral; it is the new terrain upon which visibility, legitimacy, and ideology are contested.

VIII. Limitations and Future Research

While this study provides a theoretically grounded and empirically comparative analysis of information warfare in hybrid conflicts, it is not without limitations. First, the reliance on open-source intelligence (OSINT) and publicly available social media data imposes constraints on the depth and granularity of the findings. Due to the covert nature of many digital operations—particularly those conducted by intelligence services or proxy networks—certain patterns of influence or coordination may remain undetected.

Second, the comparative framework used in this study focuses primarily on macro-level discursive and platform dynamics. Although useful for capturing structural patterns, this approach does not account for individual-level user behavior, such as cognitive susceptibility to disinformation or emotional responses to digital propaganda. Future research would benefit from integrating micro-level studies, including surveys, eye-tracking technologies, and sentiment analysis, to examine how audiences process and internalize manipulated content.

Third, the analysis is limited in linguistic and regional scope. For instance, the Armenia–Azerbaijan case involves complex language politics and diasporic communication flows that may not be fully captured through English-language analysis. Future studies could incorporate multilingual natural language processing (NLP) models to better understand narrative dynamics across cultures and geographies.

Finally, while this study focuses on two high-profile conflicts, further research should explore less visible or emerging digital battlefields, such as the manipulation of climate discourse, AI-generated propaganda in developing states, or algorithmic polarization in fragile democracies. Expanding the case universe could refine the theoretical model of epistemic conflict and offer a broader understanding of how information warfare evolves in diverse political ecosystems.

These limitations notwithstanding, the findings of this paper underscore the urgency of integrating epistemic analysis into the study of digital security, international conflict, and political communication.

IX. Conclusion and Scholarly Contribution

This paper demonstrates that information warfare in contemporary geopolitical conflicts is not merely a supplementary tool but a core strategic mechanism that shapes both the structure and outcomes of modern conflicts. The analysis reveals that manipulative information tactics—especially those involving social media disinformation campaigns, troll networks, bot accounts, and algorithmic targeting—have become as impactful as conventional diplomatic or military instruments for both state and non-state actors.

The empirical findings indicate that information warfare exerts influence on two critical levels: (1) the construction of epistemic power structures and (2) the mobilization of emotional public engagement. The case of Russia's cyber operations during the 2016 U.S.

presidential election illustrates the synchronization of cyber and informational tools aimed at manipulating public opinion and generating sociopolitical polarization. Similarly, the Armenia–Azerbaijan conflict revealed how social media platforms such as Telegram, YouTube, and Twitter were employed not only to mobilize domestic audiences but also to shape the narrative in international discourse.

The study suggests that information warfare goes beyond the distortion of facts; it encompasses the architectural design of "truth" itself, aligning with Michel Foucault's notion of "regimes of truth" and Pierre Bourdieu's concept of symbolic violence. In this light, information warfare in the post-truth era serves to construct alternative realities, not merely to misinform. This directly contributes to declining rational discourse in democratic societies, the rise of populist leadership, and intensified political polarization.

Theoretical contributions of the paper lie in its framing of information warfare not solely through a technical or military lens, but within the conceptual domains of **epistemic power, symbolic order, and platform dynamics**. In the contemporary information landscape, platforms such as Meta, Google, TikTok, and Telegram have emerged as new centers of power by controlling the architecture of information distribution. This has made the legal and ethical regulation of information warfare increasingly complex.

Methodologically, the study combines an interpretive political analysis with a case-based qualitative research strategy. Critical discourse analysis, process tracing, and open-source intelligence (OSINT) are integrated to analyze content, narratives, and chronological evolution of information campaigns. The findings are situated within a multidisciplinary framework combining political science, security studies, and critical media theory.

In terms of **legal and ethical implications**, the paper highlights a significant normative gap between existing international legal frameworks and the realities of digital conflict. While documents such as the Tallinn Manual 2.0 offer some guidance, there is no comprehensive international legal norm addressing psychological manipulation, emotional mobilization, or algorithmic warfare in cyberspace. Responsibility attribution, a core principle in international law, remains highly ambiguous in information warfare, particularly when anonymous actors and decentralized campaigns are involved.

Ethically, the paper argues that information warfare not only distorts facts but compromises citizens' cognitive autonomy, erodes democratic deliberation, and transforms platforms into psychological battle-grounds. The manipulation of public perception through visual propaganda, deepfakes, and emotionally charged content requires urgent consideration by both legal scholars and technology governance institutions.

This study's **scholarly contribution** lies in its multidimensional framing of information warfare, placing epistemic structures and symbolic strategies at the center of analysis. While most literature focuses on cybersecurity and legal norms, this paper integrates discursive, emotional, and ideological dimensions to provide a more comprehensive understanding of modern conflict.

Ultimately, information warfare in the 21st century is no longer confined to conventional tools of coercion. It is a struggle over **truth, visibility, and public consciousness**. In this context, information is not merely a medium of conflict—it is the terrain of conflict itself. Future research must therefore engage with information warfare not only as a technological or legal issue but also as a central field of **epistemic power, democratic resilience, and ideological confrontation**.

X. Policy Implications and Strategic Recommendations

In light of the findings from this study, several critical policy implications emerge concerning the regulation of digital information environments, the role of platform accountability, and the safeguarding of epistemic stability in conflict-prone societies. As information warfare becomes a structural component of hybrid conflicts, the need for coordinated and interdisciplinary policy interventions is more pressing than ever.

One of the core findings of this research is the manipulative capacity of social media algorithms in amplifying conflictual and emotionally charged content. Therefore, digital platforms such as Meta, TikTok, YouTube, and Telegram must be subjected to stricter regulatory frameworks that ensure transparency of recommendation systems, content moderation policies, and data-sharing mechanisms. Regulatory bodies — such as the European Union's Digital Services Act or the proposed US Algorithmic Accountability Act — can serve as foundational models for global policy convergence.

There is a growing need to develop multilateral legal frameworks that recognize and protect the digital sovereignty of states without endorsing censorship. Existing international law fails to adequately address the extraterritoriality of information manipulation campaigns. Hence, an international code of conduct, coordinated through the UN or regional security organizations, must establish red lines for cross-border information interventions, including coordinated disinformation campaigns and psychological influence operations.

This study highlights the importance of public epistemic resilience against manipulative information flows. Therefore, states must invest in national media literacy programs starting from early education. These

programs should not merely teach technical media skills, but also foster critical thinking, fact-checking habits, and awareness of epistemic manipulation. Scandinavian states offer a strong institutional model for balancing freedom of expression with epistemic integrity.

In geopolitically sensitive zones such as the South Caucasus, Eastern Europe, and parts of Africa, disinformation and digital propaganda pose unique challenges. An independent international body — perhaps under the OSCE or a UN-affiliated cybersecurity forum — should be established to monitor information flows during active or latent conflicts. These structures could issue real-time alerts, coordinate fact-checking, and mitigate the weaponization of digital content.

Private tech companies must adopt a conflict-sensitive approach when operating in regions with high polarization. Just as environmental impact assessments are mandated for development projects, platforms should be required to conduct **Conflict Impact Assessments** (CIAs) before launching new features or algorithms in volatile regions. This would help anticipate potential harms and design mitigation strategies tailored to local sociopolitical contexts.

As highlighted in the legal analysis section, the issue of attribution remains a major obstacle in prosecuting information warfare. International cooperation is essential to standardize evidence thresholds, enhance cyber-forensics collaboration, and establish clear chains of accountability, especially when non-state actors and proxy networks are involved.

References Références Referencias

1. Aral, S., & Eckles, D. (2018). *Protecting elections from social media manipulation*. Science, 365 (6456), 858–861.
2. BBC. (2020). *Nagorno-Karabakh: How fake videos spread online*. Retrieved from https://www.bbc.com/news/technology
3. Benkler, Y., Faris, R., & Roberts, H. (2018). *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press.
4. Bourdieu, P. (1991). *Language and Symbolic Power*. Harvard University Press.
5. Butler, J. (2005). *Giving an Account of Oneself*. Fordham University Press.
6. Castells, M. (2009). *Communication Power*. Oxford University Press.
7. DiResta, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., & Beyer, B. (2018). *The tactics and tropes of the Internet Research Agency*. New Knowledge Report to the U.S. Senate Intelligence Committee.
8. Flew, T. (2021). *Regulating Platforms: Communication Policy and the Media Platform Era*. Palgrave Macmillan.
9. Foucault, M. (1980). *Power/Knowledge: Selected Interviews and Other Writings, 1972–1977*. Pantheon Books.
10. Fuchs, C. (2021). *Social Media: A Critical Introduction* (3rd ed.). Sage Publications.
11. Gartzke, E. (2013). *The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth*. International Security, 38(2), 41–73.
12. Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.
13. Habermas, J. (1984). *The Theory of Communicative Action: Reason and the Rationalization of Society* (Vol. 1). Beacon Press.
14. Karpf, D. (2024). *Network propaganda in the age of algorithmic warfare*. New Media & Society, 26(3), 519–535. https://doi.org/10.1177/14614448231234567
15. Nye, J. S. (2011). *The Future of Power*. Public Affairs.
16. O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown Publishing.
17. Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux.
18. Sambaluk, M. (2019). *Conflict in the 21st Century: The Impact of Cyber Warfare, Social Media, and Technology*. Praeger.
19. Sunstein, C. R. (2017). *#Republic: Divided Democracy in the Age of Social Media*. Princeton University Press.
20. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. (2017). Cambridge University Press.
21. U.S. Senate Intelligence Committee. (2019). *Report on Russian Active Measures Campaigns and Interference in the 2016 Election*. Volume 2.
22. Valeriano, B., & Maness, R. C. (2015). *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press.
23. Virilio, P. (1998). *The Vision Machine*. Indiana University Press.
24. Vosoughi, S., Roy, D., & Aral, S. (2018). *The spread of true and false news online*. Science, 359(6380), 1146–1151.
25. Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.