Revista Latino-Americana de
RELAÇÕES INTERNACIONAIS
Campos Neutrais

FURG
UNIVERSIDADE FEDERAL
DO RIO GRANDE

ARTIGO

From psychological operations to cyber influence operations: the evolution of the battle for the mind

Das operações psicológicas às operações de influência cibernética*: a evolução da batalha pela mente*

Luciano Vaz Ferreira

Resumo

A consolidação do ciberespaço como um domínio central de interação política, econômica e social transformou profundamente a projeção de poder nas relações internacionais. As operações de influência cibernética surgiram como instrumentos estratégicos capazes de moldar percepções, atitudes sociais e processos decisórios no domínio cognitivo, explorando a velocidade, a escala e a interconectividade das redes digitais. Este artigo investiga a evolução das operações psicológicas (PSYOPS) e suas continuidades e transformações nas operações de influência cibernética contemporâneas. Por meio de uma revisão de literatura fundamentada em estudos estratégicos, relações internacionais e comunicação, são analisadas tanto fontes históricas, incluindo o trabalho de Paul M. A. Linebarger, quanto a produção acadêmica contemporânea sobre desinformação digital. O estudo desenvolve um referencial analítico comparativo e teoricamente fundamentado para compreender como as PSYOPS se adaptaram ao ambiente digital. O artigo está estruturado em duas seções principais: a primeira aborda as dimensões históricas das PSYOPS, enquanto a segunda examina sua transformação digital, incluindo um breve estudo de caso sobre campanhas contemporâneas de influência cibernética. Conclui-se que as operações de influência cibernética devem ser entendidas como uma continuação e amplificação dos princípios das PSYOPS na era digital

Palavras-chave: Operações Psicológicas; Operações Cibernéticas de Influência; Estudos Estratégicos.

Abstract

The consolidation of cyberspace as a central domain of political, economic, and social interaction has profoundly transformed the projection of power in international affairs. Cyber influence operations have emerged as strategic instruments that shape perceptions, social attitudes, and decision-making within the cognitive domain, exploiting the speed, scale, and interconnectivity of digital networks. This article investigates the evolution of psychological operations (PSYOPS) and their continuities and transformations in contemporary cyber influence operations. Using a literature review grounded in strategic studies, international relations, and communication, it analyzes both historical sources, including the work of Paul M. A. Linebarger, and contemporary scholarship on digital disinformation. The study develops a comparative and theoretically informed framework to understand how PSYOPS have adapted to the digital environment. The article is structured in two main sections: the first addresses the historical dimensions of PSYOPS, while the second examines their digital transformation, including a brief case study of contemporary cyber influence campaigns. In conclusion, cyber influence operations should be understood as a continuation and amplification of PSYOPS principles in the digital age.

Keywords: Psychological Operations; Cyber Influence Operations; Strategic Studies.

1 INTRODUCTION

In the early decades of the twenty-first century, the consolidation of cyberspace as a structural domain of political, economic, and social interaction has profoundly transformed the projection and contestation of power in international affairs. No longer confined to territorial or purely military arenas, strategic competition increasingly unfolds within digitally mediated environments where information circulates instantaneously and audiences are both global and granular. In this context, cyber influence operations have emerged as central instruments of statecraft, enabling actors to project power beyond borders while minimizing the costs and risks associated with kinetic force.

Rather than relying primarily on physical coercion, these operations operate within the cognitive domain, seeking to shape perceptions, recalibrate social attitudes, and influence decision-making processes at both collective and individual levels. By exploiting the structural features of highly networked digital ecosystems characterized by speed, scale, interconnectivity, and algorithmic curation, state and non-state actors can amplify selected narratives, manipulate informational visibility, and fragment public discourse with unprecedented precision. Influence thus becomes embedded in the architecture of everyday communication technologies, transforming the informational sphere into a persistent and contested battlespace.

This article investigates the following research problem: How have psychological operations (PSYOPS) evolved over time, and what continuities and transformations can be identified in their adaptation to contemporary cyber influence operations? Methodologically, the study adopts a literature review with a strong historical orientation, grounded in strategic studies, international relations, and communication. It systematically examines the influential work of Paul M. A. Linebarger alongside contemporary scholarship on cyber operations and digital disinformation. By conducting a comparative analysis of historical and contemporary sources, the article develops a theoretically informed analytical framework to explain the evolution of psychological operations from pre-digital contexts to today's digital environment.

The article is organized into two main sections. The first section explores the historical dimensions of PSYOPS, particularly in the twentieth century. The second section examines the transition of PSYOPS into the digital domain, focusing on the emergence of cyber influence

operations. A brief case study concludes this section, highlighting key dynamics in contemporary digital influence campaigns.

2 FOUNDATIONS OF PSYCHOLOGICAL OPERATIONS AND LINEBARGER'S CONTRIBUTION

Psychological Operations (PSYOPS) are defined as planned psychological activities using methods of communications and other means directed to approved audiences in order to influence perceptions, attitudes and behavior, affecting the achievement of political and military objectives (North Atlantic Treaty Organization, 2007). Unlike propaganda, which constitutes a broader communicative phenomenon employed by diverse actors, including political, religious, ideological, and commercial groups to influence opinions and behaviors in a general sense (Olejnik, 2024), PSYOPS possess a distinct military and security character. They are formally embedded within the structures and doctrinal frameworks of the armed forces and intelligence services, operating as a strategic instrument in the international arena.

Although PSYOPS are formally codified within contemporary military doctrine, their underlying strategic logic is far from novel. The premise that information can operate as a decisive instrument of power has deep historical roots in both the practice and theory of warfare. In The Art of War, attributed to Sun Tzu (5th century BCE), the principle of "winning without fighting" occupies a central position. For Sun Tzu, the highest form of victory lies not in the physical destruction of the enemy, but in the systematic erosion of the adversary's will to resist, thereby achieving strategic objectives without recourse to direct confrontation (Sun Tzu, 2009).

Historical records likewise provide illustrative examples of practices analogous to contemporary PSYOPS. In the thirteenth century, the Mongol Empire deliberately cultivated a reputation for ruthlessness, annihilating cities that resisted while granting clemency to those that surrendered. This calibrated use of violence and mercy functioned as a psychological mechanism designed to induce early capitulation and reduce the need for prolonged military engagement (May, 2007). Another example can be found in the United States during its wars against Indigenous populations between the 17th and 19th centuries, when narratives disseminated through newspapers, school textbooks, and literary works contributed to normalizing genocide and obscuring the resistance of these communities (Newitz, 2018). In both cases, the deliberate construction and circulation of narratives served strategic purposes

by influencing expectations, perceptions, and collective attitudes in support of political and military objectives.

The first half of the twentieth century witnessed a profound transformation in PSYOPS, which at the time were referred to as psychological warfare. This transformation was driven by the expansion of mass communication technologies, particularly the press and radio, as well as by the growing professionalization and systematization of their planning and execution. Over time, these activities became institutionalized and were progressively entrusted to specialized state agencies.

During World War I, British and American authorities directed their efforts not only toward domestic propaganda, aimed at fostering nationalism and sustaining public support for the war, but also toward the conduct of PSYOPS abroad. A diverse array of communication tools was employed, including newspaper articles, films, radio broadcasts, and printed leaflets. Among the most significant innovations of this period was the use of aerial delivery systems, such as aircraft, balloons, and mortars, to disseminate leaflets over enemy-held territory and neutral countries. These initiatives sought to delegitimize the adversary through allegations of atrocities, undermine morale, and encourage surrender (Linebarger, 1954; Goldman, 2024).

In the Second World War, PSYOPS reached a new level of sophistication and were systematically employed by both the Allied and Axis powers, consolidating the classification of propaganda into white, gray, and black categories. White propaganda consisted of messages openly attributed to official governmental sources, including materials produced by state agencies and broadcasts transmitted through national radio services. Gray propaganda relied on ambiguous attribution, deliberately obscuring its governmental origin. Black propaganda, by contrast, involved the deliberate fabrication of information designed to appear as though it originated from a source other than its true author, frequently relying on false narratives, forged documents, and deceptive communications (Linebarger, 1954).

This environment gave rise to a genuine battle of narratives, waged through radio waves and the printed press. Clandestine radio broadcasts of uncertain provenance were widespread, often transmitted in the enemy's language and in flawless accents, disseminating carefully crafted disinformation. Pseudo-independent correspondents and alleged insiders were frequently employed to convey messages that concealed their direct ties to state authorities. Prominent figures such as William Joyce (known as *Lord Haw-Haw*), Mildred Gillars (*Axis*

Sally), and Iva Toguri (*Tokyo Rose*) served as English-language broadcasters for Axis governments. Following the end of the war, all were prosecuted and convicted on charges of treason, underscoring the perceived strategic significance of their roles within the broader framework PSYOPS (Linebarger, 1954; Goldman, 2024).

The strategic importance of PSYOPS during the Second World War is clearly illustrated by their role in the Allied deception campaign preceding the Normandy landings. As part of Operation Bodyguard, the Allies conducted a comprehensive disinformation effort aimed at persuading German forces that the main invasion would take place in the Pas-de-Calais region rather than in Normandy. Central to this effort was the creation of the fictitious First U.S. Army Group (FUSAG), a non-existent force designed to simulate a large-scale invasion army. This deception relied on a wide range of measures, including the deployment of inflatable tanks, the construction of fake airfields, and the simulation of intense radio traffic to create the illusion of operational activity. The FUSAG was officially commanded by General George S. Patton, whose reputation as one of the most capable and aggressive Allied commanders lent substantial credibility to the deception effort. The effectiveness of this psychological and informational campaign contributed significantly to Allied success by delaying and dispersing German defensive responses at a decisive moment (Brown, 1975).

During the Cold War, PSYOPS remained a central instrument of competition between the United States and the Soviet Union. One of the most influential thinkers in the theory and practice of PSYOPS was the American scholar Paul Myron Anthony Linebarger, author of the 1948 book Psychological Warfare. Born in Milwaukee in 1913, he spent much of his formative years in Asia and Europe due to his father's close involvement with the Chinese Nationalist leadership. This early exposure to diverse political and cultural environments endowed him with multilingual proficiency and a sophisticated understanding of non-Western political dynamics, far surpassing the mainstream perspectives of his time (Stimpson; Irtenkauf, 2018).

After completing his doctorate in political science, Linebarger held an academic position at Johns Hopkins University, where he conducted research on East Asian politics and propaganda. His extensive first-hand international experience shaped an analytical approach to psychological conflict, which he understood as a culturally embedded and politically contingent phenomenon rather than a purely technical military instrument (Stimpson; Irtenkauf, 2018).

Linebarger's professional trajectory was marked by a rare integration of academic scholarship and operational practice. During World War II, he served as a U.S. Army officer and contributed to the organization of the Army's first psychological warfare section, directly engaging with influence and information activities. In the early Cold War period, he continued to advise U.S. government institutions, including collaboration with the Central Intelligence Agency (CIA), helping to translate wartime experience into doctrine and training (Stimpson; Irtenkauf, 2018).

Distinctively, Linebarger also pursued a parallel career as a science fiction writer under the pseudonym Cordwainer Smith. Through narratives exploring power and communication, he engaged with themes closely related to PSYOPS, such as narrative construction and the shaping of belief systems, enhancing his understanding of influence as a struggle over meaning and perception (Stimpson; Irtenkauf, 2018).

According to Linebarger (1954), modern conflicts are no longer primarily defined by the physical destruction of the enemy. Rather than seeking total material annihilation, contemporary warfare typically concludes when the adversary loses the capacity for political and military organization or retains it only to negotiate surrender on the victor's terms. In this sense, the ultimate aim of modern conflict is not destruction per se, but the reshaping of the enemy's will, organizational structure, and decision-making ability.

Within this framework, PSYOPS emerge as a central instrument of modern warfare, defined by the systematic employment of propaganda in situations of conflict. Rather than substituting for military force, they operate as a force multiplier, enhancing the effectiveness of both strategic and tactical operations. Their successful implementation requires meticulous planning and close integration with broader military and political efforts (Linebarger, 1954).

Importantly, PSYOPS are not confined to enemy combatants. They may also target neutral actors and friendly foreign audiences, whether civilian or military. In this capacity, they seek to shape perceptions, influence emotions, and orient decision-making in accordance with predefined objectives. Moreover, PSYOPS constitute a continuous mode of operation, conducted not only during periods of armed conflict but also in times of peace (Linebarger, 1954).

PSYOPS can be classified according to their time horizon, whether short-term or long-term, their purpose, offensive or defensive, and their intended effect. These effects encompass

conversionary propaganda aimed at shifting loyalties, divisive propaganda designed to foster internal fragmentation, consolidation propaganda used to control occupied populations, and counterpropaganda intended to directly refute enemy narratives (Linebarger, 1954).

Rooted in the psychological sciences, PSYOPS seek to shape cognition and behavior through strategically crafted communication. Their effectiveness depends on tailoring messages to the specific characteristics and vulnerabilities of the target audience. This requires a careful understanding of the audience's concrete concerns, the demonstration of empathy, and the framing of issues in ways that align with their realities. Successful PSYOPS are therefore context-sensitive rather than abstract, focusing on immediate and tangible matters instead of generic ideals. Practical concerns such as food security, wages, family welfare, postwar employment, and social inequalities often outweigh ideological or patriotic appeals. By anchoring messages in shared or relatable interests, PSYOPS enhances its credibility and persuasive power, sometimes shaping perceptions before the target even recognizes its adversarial origin (Linebarger, 1954).

Linebarger (1954) employed the classic distinction between white, gray, and black propaganda, as previously noted. For him, however, the central element was not merely the dissemination of disinformation, but the careful selection of factual information that could be strategically relevant and capable of placing the enemy at a disadvantage. The effectiveness of the message depended on its being tailored to a specific audience, articulated in clear and credible language, while avoiding excessive ideological tone or outdated terminology. It should also draw upon preexisting perceptions, biases, and cognitive vulnerabilities.

A recurrent strategy is to avoid direct attacks on the adversary's population, since this may provoke defensive reactions and aversion, and instead focus on delegitimizing enemy leaders by portraying them as selfish and corrupt, exposing scandals, inconsistencies, and contradictions. The objective is to undermine internal trust, attract external sympathy, and stimulate domestic pressure against the target government (Linebarger, 1954).

Meanwhile, on the other side of the Atlantic, the Soviet Union developed its own doctrine of PSYOPS. Euphemistically referred to as active measures (Russian: *aktivnye meropriyatiya*), this framework encompassed a broad spectrum of offensive instruments, including disinformation, deception, sabotage, destabilization, and espionage. These practices were deeply embedded in the Soviet state's strategic assumptions and foreign policy priorities,

functioning as integral components of its broader geopolitical posture. Their primary purpose was to influence and manipulate the perceptions and behavior of adversaries in ways that advanced Moscow's strategic objectives (Rid, 2021; Darzewska; Żochowski, 2017).

Although the scope of active measures extended to coercive practices such as assassinations and terrorism, their organizing principle lay in the systematic management of perceptions abroad. In this regard, the doctrine closely paralleled the logic of PSYOPS. A central mechanism consisted of disseminating both authentic and fabricated information in foreign environments in order to deepen political cleavages, erode confidence in public institutions, and cultivate receptivity to the Soviet model (Rid, 2021; Darzewska; Żochowski, 2017; Hosaka, 2024).

Operationally, this approach relied on several recurrent techniques. These included the exposure of alleged conspiracies and hostile designs attributed to opponents in order to influence international public opinion; the strategic deployment of compromising material, whether genuine or falsified, to discredit institutions and prominent individuals; and targeted efforts to shape the attitudes of governments, political parties, and economic elites in directions compatible with Soviet interests (Hosaka, 2024).

A pivotal element of this system was the use of agents of influence, considered more persuasive than conventional media channels because of their perceived credibility and proximity to decision-making circles. Such intermediaries, including journalists, academics, political actors, and individuals with indirect access to policymakers, could operate consciously or unwittingly, thereby reinforcing Soviet narratives within foreign political and intellectual spheres (Hosaka, 2024).

During the Cold War, television gradually supplanted radio as the principal medium for the dissemination of PSYOPS, largely owing to its ability to combine image, sound, and narrative within a single communicative platform. Whereas radio relied exclusively on spoken language and the listener's imagination, television enabled the construction of more persuasive messages through the incorporation of visual elements that conveyed heightened realism, authority, and immediacy. This medium proved particularly significant for campaigns directed at both domestic and international audiences, as it facilitated the dramatization of events, the personalization of political leadership, and the framing of complex conflicts in simplified, binary, and readily recognizable terms (Taylor, 2003). Consequently, television substantially

expanded the scope and effectiveness of state-sponsored PSYOPS, reinforcing and consolidating perceptions and attitudes in a deeper and more enduring manner than traditional radio-based communication.

3 CYBER INFLUENCE OPERATIONS IN THE DIGITAL WORLD

Throughout the 1990s, rapid advances in telecommunications, driven by the expansion of the internet, the consolidation of satellite communications, and the widespread adoption of the Global Positioning System (GPS), fundamentally reshaped global patterns of communication, coordination, and decision-making. Information flows shifted away from linear, slow, and hierarchical structures toward increasingly integrated, decentralized, and continuous networks operating close to real time. In this context, these transformations gave rise to a "network society," in which the primary structures of power, production, and social interaction are organized around digital information networks rather than territorially bounded hierarchies (Castells, 2009).

Cyberspace thus transformed the foundations of human communication by compressing time and space, lowering barriers to interaction, and enabling unprecedented levels of connectivity across societies. By 2025, it is estimated that approximately 68% of the world's population has access to the internet, a level of penetration that underscores the extent to which digital networks have become a structural element of contemporary social, economic, and political life, amplifying the reach, speed, and strategic relevance of information in global affairs (International Telecommunication Union, 2024).

Within this context, the Gulf War (1990–1991) marked a decisive turning point, as digitalization assumed a central role in the conduct of armed conflict and significantly enhanced the projection of military power. The conflict demonstrated, on an unprecedented scale, the integration of advanced technologies, information networks, and military operations, thereby consolidating a new model of warfare structured around digitally enabled capabilities (Creveld, 1991; Gray, 1999).

The extensive use of satellites, GPS, secure communications, advanced sensors, and precision-guided munitions enhanced operational coordination, accelerated decision-making cycles, increased selective lethality, and reduced reliance on large-scale troop deployments. In this context, digitalization did not replace kinetic capabilities; rather, it operated as a strategic

multiplier, rendering the timely collection, processing, and dissemination of information a decisive factor in the effectiveness of military operations (Creveld, 1991; Gray, 1999).

As communication infrastructures became increasingly interconnected with the Internet and societies grew more dependent on digital networks, perceptions of cyber risk rose significantly. Computer-based attacks and economically motivated cybercrime became more frequent, affecting both businesses and individuals (Clarke; Knake, 2009). At the same time, military planners began to recognize cyberspace as an operational domain, enabling the development of strategic cyber operations. This shift is exemplified by two emblematic cases: the 2007 cyberattacks against Estonia and the Stuxnet operation targeting Iran's nuclear program.

In Estonia, large-scale distributed denial-of-service (DDoS) attacks disrupted government institutions, financial systems, media outlets, and communication services by overwhelming networks with massive volumes of traffic generated by compromised devices, temporarily rendering essential digital services unavailable (Mirkovic. *et al.,* 2015; Schmidt, 2014). By contrast, Stuxnet represented a more sophisticated and targeted form of cyber warfare, as a state-sponsored malware designed to infiltrate Iran's Natanz nuclear facility and covertly sabotage industrial control systems by manipulating centrifuge operations while feeding false data to operators (Zetter, 2014).

The literature in strategic studies, as well as national security and military doctrine documents, has frequently overstated the cyber threat, often invoking the specter of a future "cyber Pearl Harbor"—a large-scale cyberattack allegedly capable of bringing an entire nation to its knees at the push of a button (Clarke; Knake, 2009; Singer; Friedman, 2014). Over time, however, it has become evident that the practical use of this instrument does not sustain such an apocalyptic narrative.

Rather than serving as an instrument of instantaneous and comprehensive destruction, cyber power has demonstrated its strategic relevance primarily as a force multiplier across three principal domains (Buchanan, 2020): (1) sabotage operations, involving the temporary or permanent disruption of electronic systems and critical infrastructure; (2) espionage operations, encompassing the extraction of sensitive data from digital devices and networks; and (3) psychological activities conducted in cyberspace, commonly referred to as cyber influence operations. Following Cordey (2019), cyber influence operations can be understood as activities

conducted through cyber-related tools and techniques that exploit the structural vulnerabilities of the digital environment in order to shape perceptions, attitudes, emotions, and motivations, thereby interfering with decision-making processes.

The distinction between traditional PSYOPS and cyber influence operations lies primarily in their operational domain. Conventional PSYOPS may incorporate physical measures on the battlefield, including deception initiatives coordinated with kinetic actions, whereas cyber influence operations are executed exclusively within digital networks and platforms. Despite this environmental difference, cyber influence operations remain firmly grounded in the doctrinal foundations and conceptual logic of PSYOPS and may thus be interpreted as their adaptation to contemporary technological conditions. The expansion of psychological strategies into the digital sphere has substantially increased the capacity of both state and non-state actors to shape collective interpretations of reality and influence public debate on an unprecedented scale (Rid, 2013).

In the first two decades of the twenty-first century, cyber influence operations gained increasing prominence, emerging as a central instrument of contemporary influence campaigns. This development has been driven largely by rapid technological advances that expanded global connectivity while simultaneously deepening society's structural dependence on digital networks and information ecosystems. These transformations have not only reshaped the informational environment but also significantly reduced the economic and operational barriers to conducting influence operations.

Unlike traditional PSYOPS, which typically required substantial financial investment in printing facilities, radio and television broadcasting infrastructure, physical distribution networks, and the deployment of specialized personnel, cyber influence operations can be conducted through existing digital platforms with comparatively limited material and financial resources. Digital content can be produced rapidly, disseminated instantaneously across borders, replicated at near-zero marginal cost, and amplified through automation and algorithmic systems. As a result, both state and non-state actors are able to sustain large-scale influence campaigns with greater precision and at a fraction of the cost associated with traditional psychological operations (Stengel, 2019).

Three major innovations have decisively shaped the expansion and effectiveness of cyber influence operations: the widespread proliferation of smartphones, the advancement of big data analytics, and the consolidation of social media platforms.

First, the widespread adoption of smartphones has fundamentally transformed communication dynamics and the dissemination of cyber influence. In earlier periods, media such as pamphlets, radio broadcasts, and television programs were typically consumed in fixed, context-bound environments. In contrast, individuals now carry permanently connected devices that facilitate the continuous, real-time transmission of messages, irrespective of physical location (Levinson, 2004; Saylor, 2013).

This transformation embodies a core principle identified by Linebarger (1954), who underscored the strategic importance of persistent and context-sensitive messaging in traditional psychological operations. Whereas radio broadcasts during the Second World War enabled sustained engagement with target audiences, smartphones now operate as omnipresent channels of influence, enabling cyber influence operations to function continuously and to embed persuasive content seamlessly within the routines of everyday life.

Second, the expanding availability of big data and advanced analytics has enabled the personalization of influence campaigns with unprecedented precision. By collecting and processing vast quantities of user data, including browsing behavior, consumption patterns, preferences, and social connections, actors are able to tailor messages to specific demographic segments or even to individual users (Zuboff, 2018).

Linebarger (1954) emphasized the centrality of audience-oriented messaging, arguing that effective PSYOPS must resonate with the concrete concerns, beliefs, and vulnerabilities of its intended targets. In the digital era, cyber influence operations extend and significantly refine this principle. Through the integration of big data analytics and artificial intelligence, influence operators can segment audiences with remarkable granularity and craft highly customized narratives aligned with distinct psychological predispositions and emotional triggers.

Third, the rapid expansion of social media platforms has reshaped the structures of information diffusion and social interaction. These platforms enable not only the large-scale, instantaneous dissemination of content but also foster horizontal communication, where users actively produce, share, and amplify narratives (Singer; Brooking, 2019). In this context,

PSYOPS are no longer reliant solely on centralized broadcasters; it now circulates through peer-to-peer networks, gaining credibility through its apparent spontaneity and organic spread.

Content may be propagated by ordinary users who unknowingly amplify manipulated material, by digital influencers with undisclosed ties to the actors behind the operation, or even by established news organizations that occasionally reproduce already viral content without sufficient verification. Furthermore, coordinated inauthentic behavior often employs fake profiles to manipulate perceptions and extend reach (Olejnik, 2024).

Within this networked architecture, cyber influence campaigns translate core principles identified by Linebarger (1954) into the digital environment, particularly the strategic coordination of multiple communication channels and the systematic use of repetition. Whereas traditional PSYOPS relied on the integrated deployment of print media, radio, and clandestine broadcasts to create a sense of ubiquity and inevitability, contemporary digital platforms reproduce and intensify these effects through algorithmic amplification and patterned user engagement. The proliferation of accounts, formats, and platforms generates an appearance of consensus, normalizes selected narratives, and produces informational saturation.

In this context, repeated exposure, now accelerated by platform logics that privilege visibility and emotional resonance, shapes perception, and influences decision making processes. By exploiting these structural features, cyber influence campaigns accelerate cognitive saturation and ensure that targeted narratives penetrate deeply and persist within specific audiences.

A central technique identified by Linebarger (1954) consists of deliberately blending accurate information with misleading interpretations, selective omissions, and contradictory narratives. By interweaving verifiable facts with distortion and mutually inconsistent claims, propagandists can erode cognitive stability, foster uncertainty, and undermine trust in authoritative sources. In digital environments, this strategy is particularly potent: the coexistence of true, false, and partially accurate information within the same informational ecosystem complicates verification processes and produces ambiguity rather than straightforward belief. The objective is not merely persuasion, but confusion, fragmentation of perception, and the weakening of coherent public judgment.

Moreover, the architecture of many social media platforms is intentionally structured to maximize user engagement through psychologically rewarding features such as intermittent

notifications, "likes," and algorithmically curated feeds, which encourage habitual and sometimes compulsive patterns of use (Alter, 2017). This design intensifies exposure to continuous flows of content while diminishing the reflective distance necessary for critical evaluation. As a result, emotionally charged or misleading narratives can be rapidly consumed and disseminated with limited scrutiny.

The creation of artificial personas to disseminate information, a practice common in Second World War PSYOPS, has reached a new level in cyberspace. Anonymity in this environment enables the easy creation of fake and inauthentic accounts, allowing both state and non-state actors to operate without clear identification, thereby weakening accountability and complicating detection (Singer; Brooking, 2019; Benkler; Faris; Roberts, 2018).

In the contemporary digital environment, anonymity is strategically operationalized through coordinated networks that integrate trolls and automated bots. Trolls, acting individually or within organized groups, operate through fabricated or semi-authentic personas and employ rhetorical manipulation, provocation, and emotional exploitation to intervene in targeted discussions. Their purpose goes beyond persuasion to intentional disruption: they aim to destabilize debates, undermine credibility, exhaust participants, redirect attention, and reinforce preferred narratives (Olejnik, 2024).

Complementing this human component, bots are software-driven automatisms designed to generate artificial traffic, inflate visibility metrics, and manufacture the illusion of consensus. They amplify selected content, target individuals with harassment, and saturate the information environment through attention flooding. When interconnected into coordinated botnets, these systems can identify target audiences, strategically select platforms, obscure their origin, and automate engagement at scale. The integration of organized trolling and botnet infrastructures enables influence actors to artificially enhance visibility and fabricate the appearance of broad and authentic public engagement (Olejnik, 2024).

These mechanisms generate manufactured perceptions of social consensus by exploiting the tendency of individuals to interpret visibility and repetition as indicators of legitimacy. In this respect, cyber influence operations represent a direct evolution of earlier clandestine practices. Just as gray and black propaganda during the Second World War relied on fabricated identities and disguised sources to conceal governmental involvement, cyber influence

operations employ synthetic digital identities and coordinated behavioral patterns to obscure authorship while constructing persuasive illusions of popular legitimacy.

This dynamic is reinforced by the clickbait economy that underpins many social media platforms, whose business models prioritize engagement and popularity over veracity, since they generate revenue from both true and false content (Stengel, 2019). Because visibility, user retention, and advertising income are closely tied to metrics such as clicks, shares, and reactions, sensationalist and emotionally provocative content tends to be algorithmically amplified (Samman; Gammon, 2025). In this attention-driven environment, accuracy and nuance frequently become subordinate to virality. Such incentive structures create fertile ground for influence actors, who can strategically craft narratives designed to trigger outrage, fear, or moral indignation—emotions long recognized in PSYOPS theory as powerful levers of persuasion.

Finally, algorithmic personalization plays a central role in consolidating echo chambers, within which individuals are predominantly exposed to information that reinforces preexisting beliefs (O'Neil, 2009; Pariser, 2012). As exposure to dissenting perspectives declines, political and social polarization tends to intensify, fostering an informational environment particularly conducive to influence strategies that mobilize identity, fear, and grievance. Under such conditions, cyber influence operations gain in effectiveness, as segmented audiences become increasingly receptive to narratives that confirm prior convictions and reduce cognitive dissonance.

Concomitantly, processes commonly described as "truth decay" deepen. The boundaries between fact and opinion grow progressively blurred; personal experience is privileged over verifiable evidence, and trust in traditional sources of information erodes.

This dynamic is accompanied by a parallel erosion of confidence in institutions and epistemic authorities, generating what may be characterized as "trust decay." The proliferation of conspiracy theories and persistent rumors further undermines institutional legitimacy, amplifies epistemological uncertainty, and reinforces demand for simplified, emotionally resonant explanatory frameworks (Buluc, 2024).

Democracies are uniquely vulnerable to cyber influence operations due to their reliance on an open and trustworthy informational environment (Stengel, 2019). Such operations exploit public trust, undermine institutional credibility, and disrupt the mechanisms of free

deliberation, thereby weakening citizens' ability to engage in informed decision-making. Through the strategic combination of algorithmic amplification, highly personalized messaging, and coordinated networks of automated and human actors, cyber influence operations can subtly shape perceptions, manipulate public opinion, and compromise the integrity of democratic processes. This susceptibility underscores a central paradox of democratic governance: the very openness that enables civic participation also creates avenues for sophisticated influence campaigns that threaten the stability and resilience of democratic institutions (Pamment; Palmertz, 2024).

Recent advances in artificial intelligence and machine learning are likely to generate a qualitative transformation in the conduct of cyber influence operations. Large language models (LLMs) enable the rapid production of coherent, contextually adaptive texts tailored to segmented audiences, while also facilitating near-instantaneous multilingual translation. This technological capacity allows transnational influence campaigns to be executed with limited human oversight, increasing the scale, plausibility, and personalization of persuasive messaging while significantly reducing operational costs.

Concurrently, progress in synthetic media technologies has intensified this shift. Deepfakes, understood as AI-generated or AI-manipulated audio, video, images, or documents designed to appear authentic, have become progressively more sophisticated. These systems can produce highly realistic outputs capable of deceiving both human observers and automated detection mechanisms. By leveraging the epistemic authority traditionally attributed to audiovisual evidence, deepfakes can circulate extensively before verification processes challenge their authenticity, thereby amplifying their disruptive potential within digital information ecosystems (Venema, 2024).

In this evolving environment, the proliferation of artificial personas, voice cloning, face-swapping, and morphing techniques further expands the operational repertoire of cyber influence operations. At the same time, increasing public awareness of these capabilities produces a secondary strategic consequence. Political actors may invoke the mere possibility of fabrication to dismiss authentic evidence as manipulated, fostering informational ambiguity and progressively eroding trust in documentary verification (Venema, 2024).

In recent history, documented cases of cyber influence operations undertaken in pursuit of strategic state objectives have become increasingly evident, particularly in connection with

activities reportedly attributed to Russia. Over the past two decades, Moscow has been repeatedly associated with the coordinated deployment of conventional military force, cyber sabotage, and cyber influence campaigns. These operations extend beyond the disruption or degradation of an adversary's technical and military capabilities; they are also designed to shape domestic and international perceptions, exploit political and social cleavages, and influence strategic narratives during periods of crisis and armed conflict.

One of the earliest cases of cyber influence operations conducted alongside kinetic action occurred during the 2008 Russia–Georgia conflict. Officially framed by Moscow as an intervention to protect Abkhazia and South Ossetia, the war is widely interpreted as a response to Georgia's increasing alignment with NATO and the European Union, perceived by the Kremlin as a challenge to its regional influence. Russian ground and air forces were deployed, resulting in the rapid consolidation of control over the two territories and the withdrawal of Georgian forces (Herpen, 2014; Jankowicz, 2020).

Alongside conventional military operations, Russia conducted a coordinated cyber influence campaign. Moscow framed its intervention as a "peacekeeping" and humanitarian mission, a narrative that was rapidly amplified across the information domain. In parallel, cyberattacks targeted Georgian government websites, news portals, financial institutions, and pro-Georgian media outlets through large-scale distributed denial-of-service (DDoS) attacks, abruptly disrupting official communication efforts and even affecting international media organizations such as the BBC and CNN (Herpen, 2014; Jankowicz, 2020).

These cyber operations also included website defacements, in which original content was replaced with pro-Kremlin messages and images designed to reinforce the Russian narrative. President Mikheil Saakashvili was systematically discredited through comparisons with Adolf Hitler, while allegations of genocide, ethnic cleansing, and atrocities against civilians were widely disseminated. Simultaneously, propaganda campaigns were carried out primarily via Russian state television, digital platforms, and the recently launched Russia Today (RT), which rapidly mobilized journalists and media resources to dominate the initial information space (Jankowicz, 2020).

Despite the severe initial impact, Georgia responded in an improvised yet resilient manner. Unable to rely on its own digital infrastructure, Georgian authorities resorted to alternative communication channels, including fax lines provided by non-governmental

organizations, hosting official websites on foreign servers, and disseminating official statements through platforms such as Blogspot and even the website of the Polish presidency. Nevertheless, Russia largely succeeded in shaping early international perceptions by portraying Georgia as the aggressor and the United States as an accomplice due to its military cooperation with Tbilisi, thereby reinforcing the legitimacy of its military intervention (Jankowicz, 2020).

During the 2014 intervention in Ukraine, particularly in the annexation of Crimea, Russia conducted cyber influence operations that refined and expanded practices previously employed during the 2008 Russia–Georgia war. Although digital platforms and social media were becoming increasingly influential, this period still represented a transitional phase in which traditional mass media, especially television, remained a central instrument of influence (Lange-Ionatamišvili, 2014).

One of the initial measures in Crimea involved replacing local television broadcasters with Russian state-controlled channels, thereby securing immediate dominance over the information environment. These televised narratives were subsequently amplified through digital platforms, enabling Russia to frame the intervention as a protective action aimed at safeguarding Russian-speaking populations while simultaneously undermining the legitimacy of Ukrainian authorities. Leveraging the increasing penetration of smartphones and the development of more robust online ecosystems, these operations achieved broader reach, enhanced persistence, and greater resonance among both domestic and international audiences (Lange-Ionatamišvili, 2014).

Several studies indicate that, in the context of the 2022 invasion of Ukraine, Russia may have employed automated social media accounts as components of coordinated cyber influence campaigns aimed at shaping international public opinion. Empirical analyses suggest that bots played a disproportionately influential role in disseminating pro-Russian content on platforms such as Twitter, accelerating the diffusion of misleading narratives and extending their reach to millions during critical phases of the conflict (Geissler. *et al*., 2023). Complementary network and natural language processing studies show that these operations relied on coordinated online communities and strategically framed narratives, often using emotionally charged themes, such as allegations of “fascism,” to manipulate discourse and legitimize military actions (Alieva; Kloo; Carley, 2024).

The use of cyber influence operations is not limited to states. Non-state actors such as Al-Qaeda and Islamic State have integrated these tactics into their media strategies, adopting increasingly refined and sophisticated forms of disinformation. Instead of relying exclusively on overt extremist rhetoric, they capitalize on political polarization, promote selective interpretations of factual events, and employ layered communication channels to preserve credibility and mobilize support. By deliberately blurring the boundary between legitimate reporting and propaganda, they hinder detection efforts and broaden the scope of their influence (Ammar, 2024).

4 CONCLUSION

The historical trajectory of PSYOPS demonstrates their enduring role as instruments of strategic influence, designed to shape perceptions, attitudes, and behaviors in alignment with political and military objectives. From their early use during World War I, when mass media was employed for propaganda, to their professionalization in World War II, PSYOPS have adapted to the evolving geopolitical landscape.

The Cold War reinforced PSYOPS as a central strategic tool, with theorists such as Paul M. A. Linebarger making seminal contributions. His emphasis on audience-specific messaging, cultural sensitivity, and integration with political and military objectives provides a theoretical and practical foundation that continues to inform contemporary influence operations. Soviet doctrine, particularly active measures, applied similar principles, while the expansion of television and mass media enabled more immediate and compelling influence over target audiences.

In the digital era, cyber influence operations represent a direct evolution of these practices. Unlike traditional PSYOPS, which relied on centralized media, cyber operations leverage social media platforms, algorithmic targeting, and big data analytics to reach segmented audiences with unprecedented speed and precision. They extend principles of audience analysis, message tailoring, and strategic integration into digital environments while employing technologies such as artificial intelligence to produce adaptive and persuasive content. Cases including Russian operations in Georgia, Crimea, and Ukraine illustrate how cyber influence campaigns can be coordinated with conventional military and political strategies, demonstrating both their effectiveness and operational challenges.

Cyber influence operations should therefore be understood as a continuation and amplification of PSYOPS principles in the digital age. Linebarger's insights remain central: careful audience analysis, culturally informed messaging, and alignment with broader objectives are as relevant in cyberspace as they were in earlier eras of PSYOPS. Emerging technologies, including large language models and deepfakes, offer new opportunities for influence but also heighten challenges in detection, verification, and resilience, making the strategic environment increasingly complex. This evolution underscores that the value of influence lies not in immediate destruction, but in the subtle and persistent shaping of perceptions and informational ecosystems, highlighting both the enduring relevance of PSYOPS and the transformative potential of their cyber-enabled successors.

REFERENCES

ALTER, Adam. **Irresistible**: the rise of addictive technology and the business of keeping us hooked. New York: Penguin Press, 2017.

ALIEVA, Iuliia; KLOO, Ian; CARLEY, Kathleen M. Analyzing Russia's propaganda tactics on Twitter using mixed methods network analysis and natural language processing: a case study of the 2022 invasion of Ukraine. **EPJ Data Science**, v. 13, art. 42, 2024.

AMMAR, Jamil. Disinformation: the Jihadits' new religion. *In*: ARCOS, Rubén; CHIRU, Irena; IVAN, Cristina (orgs.). **Routledge handbook of disinformation and national security**. New York: Routledge, 2024. p. 111–121.

BENKLER, Yochai; FARIS, Robert; ROBERTS, Hal**. Network propaganda:** manipulation, disinformation, and radicalization in American politics. Oxford: Oxford University Press, 2018.

BROWN, Anthony Cave. **Bodyguard of lies: the extraordinary true story behind d-day**. 1. ed. New York: Harper & Row, 1975.

BUCHANAN, Ben. **The hacker and the state: cyber attacks and the new normal of geopolitics**. Cambridge: Harvard University Press, 2020.

BULUC, Ruxandra. Conspiracy theories and unfounded rumors in contemporary democracies: beyond truth and trust. *In:* ARCOS, Rubén; CHIRU, Irena; IVAN, Cristina (orgs.). **Routledge handbook of disinformation and national security**. New York: Routledge, 2024. p. 208–220.

CASTELLS, Manuel. **The rise of the network society**. 2. ed. West Sussex: Wiley-Blackwell, 2009.

CLARKE, Richard A.; KNAKE, Robert K**. Cyber War:** the next threat to national security and what to do about it. New York: Ecco, 2010.

CORDEY, Sean**. Cyber influence operations:** an overview and comparative analysis. Zurich: Center for Security Studies (CSS), ETH Zürich, 2019.

CREVELD, Martin van. **The transformation of war**. New York: Free Press, 1991.

DARZEWSKA, Jolanta; ŻOCHOWSKI, Piotr. **Active measures:** Russia's key export. Warsaw: Ośrodek Studiów Wschodnich im. Marka Karpia / Centre for Eastern Studies, 2017.

GEISSLER, Dominique. *et al.* Russian propaganda on social media during the 2022 invasion of Ukraine. **EPJ Data Science,** v. 12, 35, 2023.

GOLDMAN, Jan. Influence operations and the role of intelligence. *In*: ARCOS, Rubén; CHIRU, Irena; IVAN, Cristina (orgs.). **Routledge handbook of disinformation and national security**. New York: Routledge, 2024. p. 84–94.

GRAY, Colin S. **Modern strategy**. New York: Oxford University Press, 1999.

HERPEN, Marcel H. van. **Putin's wars:** the rise of Russia's new imperialism. London: Bloomsbury Publishing, 2014.

HOSAKA, Sanshiro. Cold War active measures. *In:* ARCOS, Rubén; CHIRU, Irena; IVAN, Cristina (orgs.). **Routledge handbook of disinformation and national security**. New York: Routledge, 2024. p. 45–58.

INTERNATIONAL TELECOMMUNICATION UNION. Internet use continues to grow, but universality remains elusive, especially in low-income regions. **Facts and figures 2024**. 2024. Disponível em: https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-internet-use/. Acesso em: 23 fev. 2026.

JANKOWICZ, Nina. **How to lose the information war: Russia, fake news, and the future of conflict.** New Haven: Yale University Press, 2020.

LANGE-IONATAMIŠVILI, Elīna (Org.). **Analysis of Russia's information campaign against ukraine.** Riga: NATO Strategic Communications Centre of Excellence, 2015.

LEVINSON, Paul. **Cellphone:** the story of the world's most mobile medium and how it has transformed everything! New York: St. Martin's Press, 2004.

LINEBARGER, Paul M. A**. Psychological warfare.** 2. ed. New York: Duell, Sloan and Pearce, 1954.

MAY, Timothy. **The Mongol art of war:** Chinggis Khan and the Mongol military system. Barnsley: Pen & Sword Military, 2007.

MIRKOVIC, Jelena. *et al.* **Internet denial of service**: attack and defense mechanisms. Upper Saddle River: Prentice Hall Professional Technical Reference, 2005.

NEWITZ, Annalee. **Stories are weapons:** psychological warfare and the American mind. New York: W. W. Norton & Company, 2018.

NORTH ATLANTIC TREATY ORGANIZATION. **Allied joint doctrine for psychological operations: AJP 3.10.1(A)**. October 2007. Disponível em: https://info.publicintelligence.net/NATO-PSYOPS.pdf. Acesso em: 23 fev. 2026.

OLEJNIK, Łukasz. **Propaganda:** from disinformation and influence to operations and information warfare. Boca Raton: CRC Press, 2024.

O'NEIL, Cathy**. Weapons of math destruction**: how big data increases inequality and threatens democracy. New York: Crown, 2016.

PAMMENT, James; PALMERTZ, Bjorn. Deterrence by denial and resilience building. *In:* CHIRU, Irena; IVAN, Cristina (orgs.). **Routledge handbook of disinformation and national security**. New York: Routledge, 2024. p. 20–30.

PARISER, Eli. **The filter bubble:** how the new personalized web is changing what we read and how we think. London: Penguin Books, 2012.

RID, Thomas. **Active measures**: the secret history of disinformation and political warfare. New York: Picador, 2021.

RID, Thomas**. Cyber war will not take place.** London: C. Hurst & Co Publishers Ltd, 2013.

SAMMAN, Amin; GAMMON, Earl (Eds.). **Clickbait capitalism:** economies of desire in the twenty first century. Manchester: Manchester University Press, 2023.

SAYLOR, Michael J. **The mobile wave**: how mobile intelligence will change everything. New York: Vanguard Press, 2013.

SCHMIDT, Andreas. The Estonian cyberattacks. *In:* HEALEY, Jason (org.). **The fierce domain: conflicts in cyberspace, 1986–2012**. Washington, D.C.: Atlantic Council, 2013.

SINGER, P. W.; BROOKING, Emerson. **LikeWar**: the weaponization of social media. Boston: Mariner Books, 2019.

SINGER, P. W.; FRIEDMAN, A. **Cybersecurity and cyberwar**: what everyone needs to know. Oxford: Oxford University Press, 2014.

STENGEL, Richard. **Information wars:** how we lost the global battle against disinformation and what we can do about it. UK: Grove Press UK, 2019.

STIMPSON, Ashley; IRTENKAUF, Jeffrey. Throngs of himself: Paul Linebarger wrote science fiction as Cordwainer Smith. **Johns Hopkins magazine,** Fall 2018. Disponível em: https://hub.jhu.edu/magazine/2018/fall/cordwainer-smith-paul-linebarger/. Acesso em: 23 fev. 2026.

SUN TZU. **The art of war**. [S.l.]: Pax Librorum Publishing House, 2009.

TAYLOR, Philip M. **Munitions of the mind:** a history of propaganda from the ancient world to the present day. Manchester: Manchester University Press, 2003.

VENEMA, Agnes E. Deepfake disinformation: how digital deception and synthetic media threaten national security. *In:* ARCOS, Rubén; CHIRU, Irena; IVAN, Cristina (orgs.). **Routledge handbook of disinformation and national security.** New York: Routledge, 2024. p. 175–191.

ZETTER, Kim. **Countdown to zero day:** Stuxnet and the launch of the world's first digital weapon. New York: Crown Publishers, 2014.

ZUBOFF, Shoshana. **The age of surveillance capitalism:** the fight for a human future at the new frontier of power. London: Profile Books Ltd, 2018.

Sobre a autoria

Luciano Vaz Ferreira
Doutor em Estudos Estratégicos Internacionais pela Universidade Federal do Rio Grande do Sul (UFRGS). Professor no Centro de Ciências Sócio-Organizacionais da Universidade Federal de Pelotas (UFPEL)
lvazferreira@gmail.com

Contribuição de autoria
Luciano Vaz Ferreira: concepção, coleta de dados, análise de dados, elaboração do manuscrito, redação, discussão dos resultados.

Financiamento
Não se aplica.

Consentimento de Uso de Imagem
Não se aplica.