ieee.es
Instituto Español de Estudios Estratégicos

Opinion
Paper

[Visit webpage](#) [Receive Newsletter](#)

68/2025 15/09/2025

*Miguel López Garay**

Social Media as Weapons of Mass Influence and the Need for a Doctrine of Information

Social Media as Weapons of Mass Influence and the Need for a Doctrine of Information

Abstract:

Social media has transitioned beyond being mere entertainment platforms and has become accurate "weapons of mass influence" that are eroding traditional power monopolies and shaping a new space of decentralized and highly dynamic power.

This article analyses the digital environment and why social media has transcended its initial role, becoming the idyllic communication medium for operations in the cognitive domain, capable of generating effects and altering the geopolitical balance in contemporary multidomain warfare.

Thus, the impact of social media on Security and Defence is presented and doctrinal informational proposals are examined, in order to answer the question: Is it possible to maintain strategic superiority without developing a own Informational Maneuver?

Keywords:

Social Media; Information Manoeuvre; Cognitive Warfare; Disinformation.

How to quote:

LOPEZ GARAY, Miguel. *Social Media as Weapons of Mass Influence and the Need for a Doctrine of Information*. Opinion Paper. IEEE 68/2025. [web link IEEE](#) and/or [link bie[3]](#) (accessed on the web day/month/year)

***NOTE:** The ideas contained in the Opinion Papers shall be responsibility of their authors, without necessarily reflecting the thinking of the IEEE or the Ministry of Defense.

«*The greatest victory is that which requires no battle*» (Sun Tzu)

1. Introduction: The Revolution of Social Media and Their Rise as Instruments of Power and Influence

As early as the Renaissance, Machiavelli recognized the importance of perception and narrative control as key elements in the preservation of power, when he stated: ”*Everyone sees what you appear to be, few experience what you really are; and those few dare not stand up against the opinion of the majority*”.[1] Almost five hundred years later, and without the need to transcribe them literally, these principles can be seamlessly transferred to the Digital Age of our time. They align precisely with the widespread use of social media platforms (SNS) and the increasing difficulty of distinguishing between what is real or true and what is imaginary or false in virtual environments.

Artificial intelligence (AI) [2] was almost virtually unknown just five years ago, yet the paradigm shift brought about by widespread internet Access —especially through mobile phones— was already being analyzed as a disruptive tool that granted anyone a window into the world. Through a smartphone, anyone could become a direct witness to events unfolding around them and broadcast them to distant places in real time. Simultaneously, these devices have empowered ordinary citizens to access information about unprecedented events —often before they are reported by traditional media outlets— thus marking a shift in how 21st-century society consumes news. [3]

With the popularization of the former Twitter —now X— this trend became firmly established. The platform quickly evolved from a social network where users shared their daily routines in 200 characters, into a powerful channel for mass and real-time communication. Before long, Twitter positioned itself as a potential —and renewed— alternative to traditional media outlets, [4] while simultaneously paving the way for new discourses and modes of communication, giving voice to previously unheard actors — who would become the first influencers.

[1] MAQUIAVELO, Nicolás. *El Príncipe*. 1532. Alianza Editorial.

[2] MONREALE, Anna. *Artificial intelligence in accounting and auditing: Accessing the corporate implications*. 2024. En: *An introduction to artificial intelligence*. London: Palgrave Macmillan, pp.63–89.

[3] HERRERO-CURIEL, Eva. *El periodismo en el siglo de las redes sociales*. Revista de Comunicación Vivat Academia. 2011. pp 113-1128.

[4] CAMPOS-DOMÍNGUEZ, Eva. *Twitter y la comunicación política*. 2017. Universidad de Valladolid. Producción Científica. Disponible en: https://uvadoc.uva.es/handle/10324/42114

Similarly, Facebook and Instagram also emerged as key platforms for the dissemination of audiovisual content during the COVID-19 pandemic. Initially dominated by leisure and sports-related content, they progressively began to incorporate topics traditionally reserved for news outlets and mainstream media —such as current events in politics, economics, professional sectors, and religion. This shift also signaled a turning point that highlights the informational value of these platforms, which are now firmly positioned as mass communication media.

In parallel, the post-pandemic period served as fertile ground for the expansion of TikTok, the social network known for its short-form videos, edited according to trending filters or music. Its novelty generated strong appeal, particularly among younger users. Moreover, a significant percentage of individuals under 24 years of age report that TikTok is their primary —and in many cases, even their sole— source of current information. [5] This trend increases their exposure to biased content and misinformation. [6]

Finally, new information channels have recently proliferated through messaging platforms such as WhatsApp and Telegram. These tools enable the mass dissemination of content in a direct manner and, unlike traditional social media, they limit audience interaction to a set of predefined reactions —usually through emojis— thus making them largely one-way communication tools. This structure enhances their usefulness for conducting propaganda campaigns, ideological dissemination, or the spread of misinformation, by reducing debate, eliminating comments, and increasing the sender's control over the message.

Moreover, the perception of privacy offered by end-to-end encryption fosters greater credibility and facilitates the circulation of unverified content. This contributes to the formation of closed ideological bubbles, sustained by parallel information ecosystems. These characteristics position messaging channels as yet another key space within the social media landscape, through which strategic communication efforts can be deployed to fully exploit the digital environment.

[5] CABRERA, Constanza. *¿Están los jóvenes desinformados por culpa de las redes sociales?* El País. 14/04/2024. Disponible en: https://elpais.com/tecnologia/2025-04-14/estan-los-jovenes-desinformados-por-culpa-de-las-redes-sociales.html

[6] HSU, Tiffany. *Worries Grow That TikTok Is New Home for Manipulated Video and Photos*. The New York Times. 04/11/2022. Disponible en: https://www.nytimes.com/2022/11/04/technology/tiktok-deepfakes-disinformation.html?searchResultPosition=2

In this context, the control of the narrative and the ability to influence public opinion have historically led to the press being referred to as the "Fourth Estate," acknowledging its role as a counterbalance to the traditional powers of the State. With the evolution and concentration of media —especially following the advent of television and the rise of media conglomerates— the notion of a "Fifth Estate" emerged, attributed to the increasing capacity to shape mass perceptions. More recently, the term "Sixth Estate"[7] has gained traction, referring to the transformative role of social media and the connected digital citizenry. This concept encompasses the direct influence on public discourse enabled by technological advancements. The "Sixth Estate" is gradually eroding traditional information monopolies and shaping a new, decentralized, and highly dynamic power landscape.

Ultimately, we have witnessed the rapid evolution of social media from their origins as platforms for communication and social interaction —capable of bridging distances and connecting users on opposite sides of the Atlantic—into true instruments of global power and influence. Beyond serving as channels for communication, entertainment, and social engagement, these applications have now positioned themselves as alternative sources and gateways for the dissemination of information. They are capable of shaping narratives, constructing perceptions, and provoking reactions in a hyperconnected world. Thus, in the landscape of contemporary information warfare, social media have also become the quintessential medium for operations within the cognitive domain.

With an impact perhaps comparable to that of the internet in its early days —when Bill Gates famously stated, "*If your business is not on the internet, then your business will be out of business*"— social media today count more than 5 billion active users. [8] This has positioned them as essential tools for states, companies, and individuals alike. It is no longer enough to simply be connected; it is now necessary to establish a presence across all available channels in order to reach every possible audience. In the current context of growing geopolitical tension, the reach and influence of social media have elevated them to the status of a new digital battlefield. They facilitate the dissemination of content on a

[7] MAGALLÓN ROSA, Raúl. *El sexto poder en la primavera árabe*. Conferencia: III Congreso Internacional Asociación Española de Investigación de la Comunicación. 2012. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5252826

[8] FERNÁNDEZ, Rosa. *Panorama mundial de las redes sociales - Datos estadísticos*. Informe Statista. 2025. Disponible en: https://es.statista.com/temas/3168/panorama-mundial-de-las-redes-sociales/#topicOverview

scale unmatched in any previous era, where verification has become a major challenge —positioning social media as instruments of power and weapons of mass influence.[9]

As a result, social media have evolved from platforms for civic interaction and mobilization into a new vector for military operations within the cognitive domain, the principal theater of warfare in a hyperconnected world. In this new operational environment, social media have become powerful tools capable of shaping public perception, influencing political decisions, and, in some cases, destabilizing governments. All of this positions them as potential "weapons of mass influence."

Aware of this power, both state and non-state actors are already leveraging these platforms within their communication strategies, seeking to capture public attention in order to control the narrative —and even conducting malicious activities to spread narratives and manipulate reality. As a consequence, the Armed Forces of various countries are actively developing "Information Maneuvers" or doctrinal frameworks to define military action in the digital environment. These efforts recognize the urgent need to enhance military capabilities so that their units can operate effectively in the cognitive domain, within an increasingly complex and contested information environment.

2. The Use of Social Media as Weapons of Mass Manipulation

Although social media employ cutting-edge technology, the use of mass media to influence public opinion is not a new phenomenon. In the early 20th century, Edward Bernays —widely regarded as the father of modern propaganda— identified the conscious and organized manipulation of public opinion as a fundamental pillar of modern democratic societies. In the introduction to his book *Propaganda*, Bernays asserts that those who control this "*invisible mechanism*" of society constitute the "*invisible government*."[10] In other words, he attributes to them the power to control the world through a force that shapes minds, defines tastes, and suggests ideas—without most people even being aware of its influence.

Historical and social events such as the Arab Spring, the 15M movement in Spain, the "#MeToo" campaign, the management of the COVID-19 pandemic, communication in the

[9] BOSWINKEL, L., FINLAYSON, N.B., MICHAELIS, J. and RADEMAKER, M. *Weapons of mass influence: Shaping attitudes, perceptions and behaviours in today's information warfare.* The Hague Centre for Strategic Studies. Abril 2022. Disponible en: https://hcss.nl/report/weapons-of-mass-influence-information-warfare/

[10] BERNAYS, Edward L. *Propaganda*. 1928. Editorial: Melusina.

early days following the invasion of Ukraine, and the media strategy during recent U.S. elections demonstrate how these platforms have transcended their initial role to become key tools for social mobilization and information manipulation. In fact, their impact goes far beyond the dissemination of news or the coordination of social movements.

Today, the use of social media extends to all areas of contemporary life. By merging the capabilities of global communication with the latest technological advancements, these platforms provide immediate and far-reaching channels that position them as key tools for marketing as well as mechanisms of manipulation. They enable the creation and dissemination of content on a global scale with high audience reach, which has also turned them into strategic weapons of mass manipulation,[11] within what is now widely recognized as a new domain of warfare: the cognitive domain.

Through the repetition of short and powerful messages, social media produce cognitive effects, altering opinions and shaping narratives. In doing so, they are able to influence users' minds —and consequently, electoral processes and civic discourse— which has raised particular concern and mistrust across the Western world.[12] Given their inherent power to influence the masses, a growing debate has emerged regarding their widespread use and impact on societies, as well as the need to establish mechanisms for control, verification, or even censorship.

In its latest Global Risks Report,[13] the World Economic Forum once again highlights the risk associated with information —particularly in the form of disinformation and misleading content— as a key concern within the two-year risk horizon. The report also emphasizes how this threat undermines the ability of individuals, businesses, and governments to discern truth from falsehood. Furthermore, it points out that the threats of social and political polarization are amplified in the favorable environment created by social media, due to algorithmic bias and the ranking of content based on users and trending topics.

In today's information warfare —constant and inherent to geopolitical competition and the

[11] BOSWINKEL, Lotje. *Weapons of mass influence: Shaping attitudes, perceptions and behaviours in today's information warfare*. The Hague Centre for Strategic Studies. Abril 2022. Disponible en: https://hcss.nl/wp-content/uploads/2022/04/Weapons-of-Mass-Influence-Information-Warfare-HCSS-2022-V2.pdf

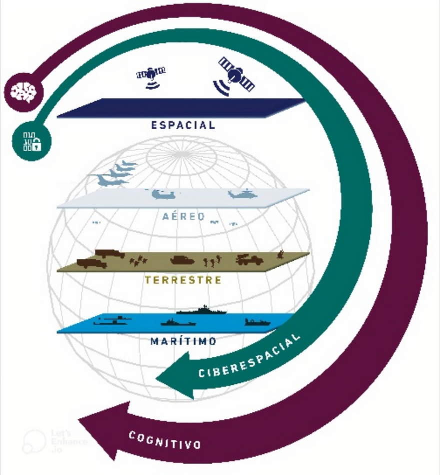
[12] Web Oficial Comisión Europea. Comunicado de prensa 17/12/2024. Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/ip_24_6487

[13] World Economic Forum (WEF). *Global Risks Report 2025*. Disponible en: https://www.weforum.org/publications/global-risks-report-2025/

"*networked society*" [14]— weapons of mass manipulation have become the primary means of communication used to exploit the information environment and generate effects within the cognitive domain, with the aim of undermining the morale and will of targeted audiences.

This was reflected in NATO's 2022 Strategic Concept,[15] which identified various strategic actors as threats to state security through the exploitation of digitalization, using hybrid tactics such as disinformation, manipulation, and post-truth narratives. All of these aim to undermine multilateral norms and promote authoritarian models of governance by means of hybrid and malicious cyber operations, the spread of disinformation, and confrontational rhetoric —already directly harming the security of allied nations. Furthermore, NATO has recently defined the cognitive warfare environment as: "*Deliberate and synchronized military and non-military activities across the spectrum of competition, designed to shape the information environment and influence attitudes, perceptions, and behaviors of audiences, in order to gain, maintain, and protect cognitive superiority*".[16]

In Spain, the national military doctrine goes a step further by acknowledging six operational domains. The classical domains —land, maritime, and aerospace— have recently been expanded with the emergence of non-physical domains: space, cyberspace, and the cognitive domain, which also includes the information environment. [17] Furthermore, the doctrine governing the use of the Armed Forces recognizes the existence of mixed domains —those that arise from the interaction between cyberspace and the cognitive domain— and considers them transversal to all other domains.



Ilustration 1 - Military Domains in Spain Armed Forces (Spanish Minister of Defence)

In this new domain of warfare, social media already play a central and multidisciplinary role of particular relevance. They represent both challenges and threats that impact the

[14] CASTELLS, Manuel. *The Rise of the Network Society*. 1998. Editorial: Oxford: Black Well Publishers

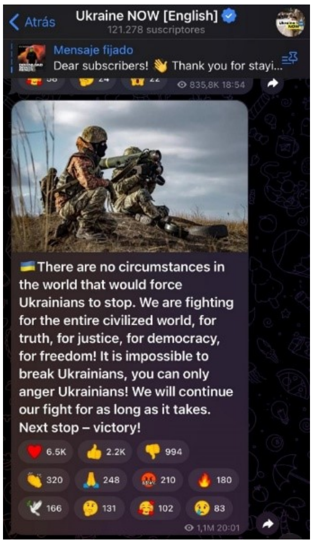
[15] NATO Strategic Concept 2022. Disponible en: https://www.nato.int/strategic-concept/

[16] NATO ACT. *NATO Cognitive Warfare Concept*. 2024

[17] Ministerio de Defensa. PDC-01 (B). *Doctrina para el empleo de las FAS*. 2024.

architecture of Security and Defense, acting as catalysts of mixed domains—transversal across all operational spheres. Specifically, within the cognitive domain, they are capable of leveraging the power of imagery —particularly through short and repetitive videos— to penetrate both rational and emotional layers of perception, thereby exerting significant effects on society and influencing decision-making processes.

Information —or disinformation— campaigns channeled through social media and, more recently, messaging platforms such as WhatsApp or Telegram, enable the modification of knowledge and alteration of beliefs, potentially generating feelings or desires, and thus motivations, with an extremely significant influence. In short, social media are ideally suited to amplify narratives through the power of perceptions conveyed by videos and iconography, capable of altering our decisions and shaping behavior, whether as individuals or leaders.[18]



🇺🇦There are no circumstances in the world that would force Ukrainians to stop. We are fighting for the entire civilized world, for truth, for justice, for democracy, for freedom! It is impossible to break Ukrainians, you can only anger Ukrainians! We will continue our fight for as long as it takes. Next stop – victory!

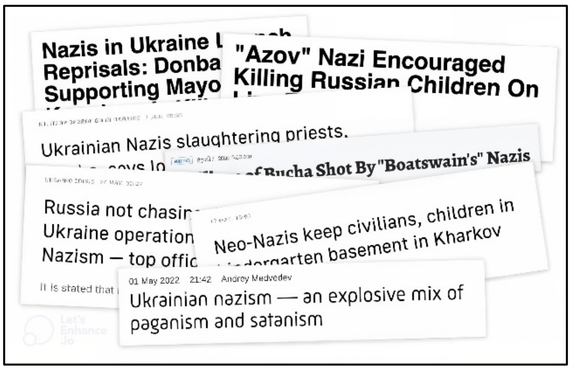
Ilustration 2 Screenshot of the pro-Ukrainian channel "Ukraine NOW" on Telegram

At the same time, actions carried out through social media allow the attacker to remain concealed and, simultaneously, blur the line between conflicts or crisis situations and periods of peace. This has facilitated their expansion into strategic environments or the “gray zone” of conflicts, given the ongoing period of geopolitical competition. When employed effectively, they undermine the advantages provided by the physical effects of conventional tactics to such an extent that a victory in the traditional realms of war can

[18] Centro Conjunto de Desarrollo de Conceptos. CESEDEN. *Implicaciones del ámbito cognitivo en las Operaciones Militares*. 2020. Disponible en: https://emad.defensa.gob.es/Galerias/CCDC/files/IMPLICACIONES_DEL_AMBITO_COGNITIVO_EN_LAS_OPERACIONES_MILITARES.pdf

backfire against the attacker, leading to a “moral defeat”[19] with devastating consequences for the campaign.

International events over the past decade allow us to illustrate with real examples how various states or international actors employ “weapons of mass manipulation.” Since 2014, Russia has been conducting a propaganda disinformation campaign to justify and conceal its unilateral decision to annex Crimea. To do this, it uses state-run media outlets such as Russia Today (RT) and Sputnik News, along with a network of bots and fake accounts that promote repetitive narratives on social media, spreading messages that accuse the Ukrainian government of being neo-Nazi, claim that the population of Crimea was in danger, and assert that the annexation referendum was legal and widely supported.[20]



Nazis in Ukraine L
Reprisals: Donba
Supporting Mayo

"Azov" Nazi Encouraged
Killing Russian Children On

Ukrainian Nazis slaughtering priests.

of Bucha Shot By "Boatswain's" Nazis

Russia not chasin
Ukraine operation
Nazism — top offic

It is stated that

Neo-Nazis keep civilians, children in
kindergarten basement in Kharkov

01 May 2022 21:42 Andrey Medvedev
Ukrainian nazism — an explosive mix of paganism and satanism

Ilustration 3 Headlines from various Russian media illustrating the use of false narratives (Source: The New York Times) [21]

Similarly, during the 2020 pandemic, Chinese authorities delayed the disclosure of critical information about the COVID-19 pandemic in the early stages of the outbreak in Wuhan, including postponing the sharing of the virus genome and censoring doctors like Li Wenliang, who tried to warn about the situation.[22] Subsequently, they promoted narratives suggesting that the virus originated in the United States and highlighted their exemplary crisis management to reinforce their legitimacy. From a more geostrategic perspective, they carried out malicious hybrid and cyber operations which, together with

[19] LIND, W.S. and THIELE, G. *4th Generation Warfare Handbook*. 2015. Editorial: Castalia House

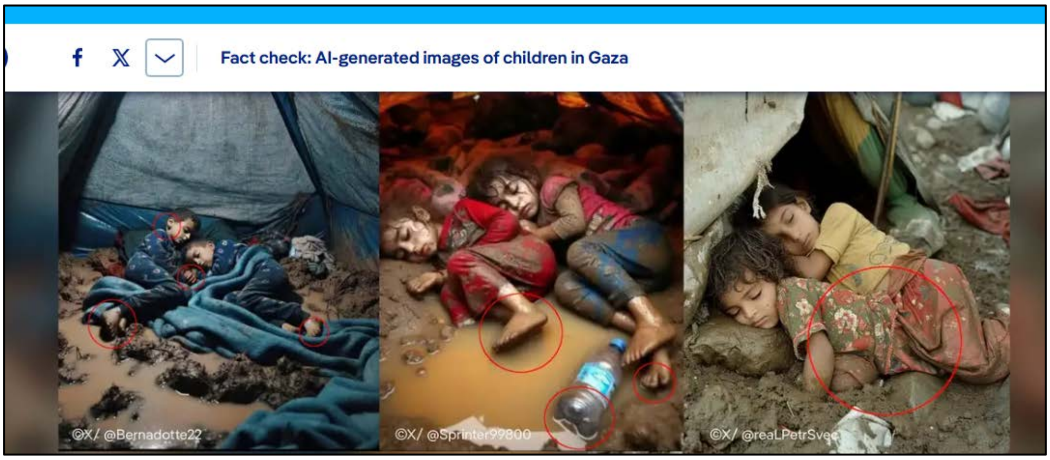
[20] EUvsDisinfo. *The architecture of Russia’s FIMI operations*. 02/04/2025. Disponible en: https://euvsdisinfo.eu/the-architecture-of-russias-fimi-operations/

[21] SMART, Charlie. *How the Russian Media Spread False Claims About Ukrainian Nazis*. The New York Times. 02/07/2022. Disponible en: https://www.nytimes.com/interactive/2022/07/02/world/europe/ukraine-nazis-russia-media.html

[22] Associated Press. *China delayed releasing coronavirus info, frustrating WHO*. 02/06/2020. Disponible en: https://apnews.com/article/fed0f89a3b46cfa401e62ce7386f0cfb

confrontational rhetoric and disinformation campaigns, aimed to expand their influence and undermine the West.[23]

The war in the Gaza Strip also provides clear examples of how Hamas exploits social media to disseminate impactful images that highlight the devastating consequences of Israeli attacks on the civilian population. Hamas has distinguished itself by its ability to flood social networks with shocking images, often taken out of context,[24] thereby challenging the superiority of the Israeli Defense Forces and countering physical attacks with moral tactics that have effectively turned nearly every Israeli physical attack into alleged atrocities against civilians. These tactics, which include narratives of absolute victimization of Gaza's population and justification of their attacks, have been documented and analyzed by organizations such as Human Rights Watch and Amnesty International, and have been denied by the IDF as part of its propaganda campaign.



Ilustration 4 AI-generated images to produce cognitive effects in Gaza (Source: DW) [25]

Current examples shed light on how social media, through the power of images, recommendation algorithms, the design of disinformation campaigns, and the viral spread of narratives, are capable of shaping realities and constructing narratives, becoming central elements in achieving effects in the cognitive domain of armed conflicts.

In light of this new reality, it can be stated that the expansion of digital environments

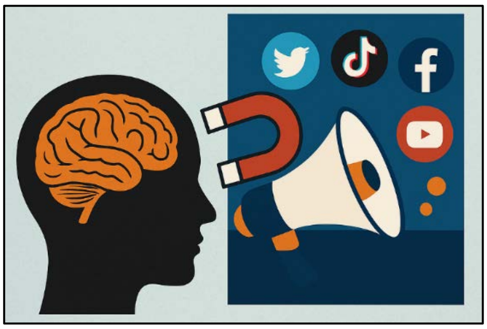
[23] ROBERTS, Dexter. *China´s Disinformation Strategy. Its dimensions and future*. Atlantinc Council. Diciembre 2020. Disponible en: https://www.atlanticcouncil.org/wp-content/uploads/2020/12/CHINA-ASI-Report-FINAL-1.pdf

[24] ALARCÓN, Nacho. *Tormenta de 'fake news': todas las fotos falsas que te están colando tras el ataque de Hamás*. El Confidencial. 13/10/2023. Disponible en: https://www.elconfidencial.com/mundo/2023-10-13/fake-news-fotos-falsas-ataque-hamas-desinformacion_3752749/

[25] WALTER, Jan D. *Fact check: AI-generated images of children in Gaza*. DW, 02/02/2024.

entails serious implications for the Security and Defense architecture, as they represent challenges and threats that must be addressed from multiple dimensions to be thoroughly understood. Furthermore, if necessary, and as part of reaction or contingency plans in the cognitive domain, they must be capable of being fully exploited to achieve decision superiority in multidomain operations.

To achieve this, it is first necessary to break down the barrier of algorithmic opacity and understand its role in radicalization processes. Secondly, we must be able to identify malicious disinformation and post-truth strategies as possible mechanisms of external interference, aimed at artificially shaping public opinion. And finally, the new times demand constant updating to be able to discern between what is real and imaginary, providing early warning about potential deepfakes or deceptive maneuvers.



Ilustration 5 Influence of social media on perceptions (Source: own elaboration)

2.1 Understanding Algorithmic Opacity and Its Role in Radicalization

Human beings are prone to groupthink and polarization, which influence how and why certain decisions are made. Social trust is an essential survival mechanism without which divisions and polarization can deepen. Therefore, the risks associated with algorithmic bias on social media are the subject of extensive study, with numerous analyses and reports warning about their implications across all areas of society.

The design of algorithms, user interactions, and AI training all contribute to the creation of bubbles, within which content is ranked according to audience age, viewing history, identified interests, and political trends, among other factors. Whether intentionally or randomly, the generation of these bubbles contributes to the “pollination” of micro-narratives or the incubation of biased thought groups. Furthermore, as Miguel Palomo points out, sometimes “*the desire for truth becomes a higher category than the conditions of truth, ultimately determining what, for our understanding, is and ought to be true and* *false*."[26] That is to say, frequently, it is the viewer who decides "what they want to see," resulting in an epistemic shift that downplays the importance of truth or knowledge, despite the vast access to information in our times.

An illustrative example of how algorithms can negatively impact the cognitive dimension, fostering the spread of misinformation and undermining social trust, is found in the Netflix documentary *The Social Dilemma*.[27] This work clearly shows how algorithmic systems, designed to maximize attention and usage time, end up reinforcing information bubbles, promoting political and social polarization, and facilitating the dissemination of extremist content. It demonstrates how algorithms, far from being neutral objects, shape digital environments, encourage emotional manipulation, hinder dialogue, and contribute to the fragmentation of the social fabric, thus posing significant risks to democracies.

The engagement-maximizing logic of social media algorithms leads to more emotional, controversial, or extreme content gaining greater visibility, fueling an atmosphere of misinformation and institutional distrust that could be exploited by both internal actors and foreign powers for destabilizing purposes.[28] Therefore, their effects are particularly significant in the context of National Security, as they can contribute to the spread of radical discourses that erode social cohesion and threaten the political stability of states.[29]

Moreover, despite their apparent technical neutrality, algorithms can be trained with biased data or intentionally designed inputs to promote certain content or amplify specific narratives. An example of this is the Operation Sentinel system of the United States Department of Homeland Security (DHS),[30] a predictive analytics platform used for detecting national security threats. Although initially designed to be impartial, various studies have pointed out that, being trained on historical data collected in contexts marked by racial and religious biases, the system tends to overrepresent Muslim or Arab-origin

[26] PALOMO, Miguel. *Incidencias filosóficas actuales en la sociedad digital: ideologías, desinformación y confusión epistemológica*. Revista ARBOR Ciencia, Pensamiento y Cultura. 2021. Disponible en: https://arbor.revistas.csic.es/index.php/arbor/article/view/2451/3730

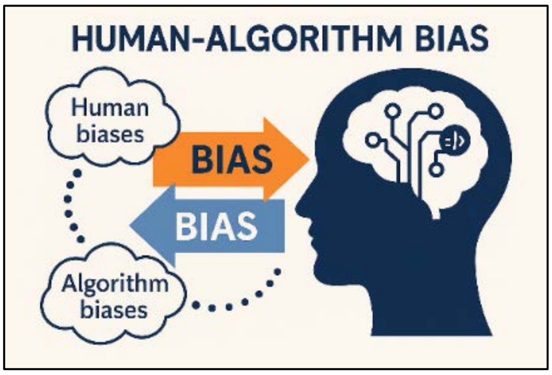
[27] NETFLIX. Documental. *El Dilema de las Redes Sociales*. 2020.

[28] Shin, D., Park, Y.J., Kim, H. y Kim, J. *Countering algorithmic bias and disinformation and effectively harnessing the power of AI in media.* Journalism & Mass Communication Quarterly. 2022. pp 1115–1136. Disponible: https://pure.uva.nl/ws/files/111307539/10776990221129245.pdf

[29] TUFEKCI, Zeynep. *Algorithmic harms beyond Facebook and Google*. Colorado Technology Law Journal. 2015. pp 203–218. Disponible en: https://ctlj.colorado.edu/wp-content/uploads/2015/08/Tufekci-final.pdf

[30] U.S. Customs and Border *Protection. DHS Announces Operation to Target Criminal Smuggling Organizations*. 27/04/2021. Disponible en: https://www.cbp.gov/

communities as potential threats,[31] without empirical justification from actual risk patterns. This type of algorithmic bias not only distorts the system's operational priorities but can also violate fundamental rights and erode the institutional legitimacy of security agencies.



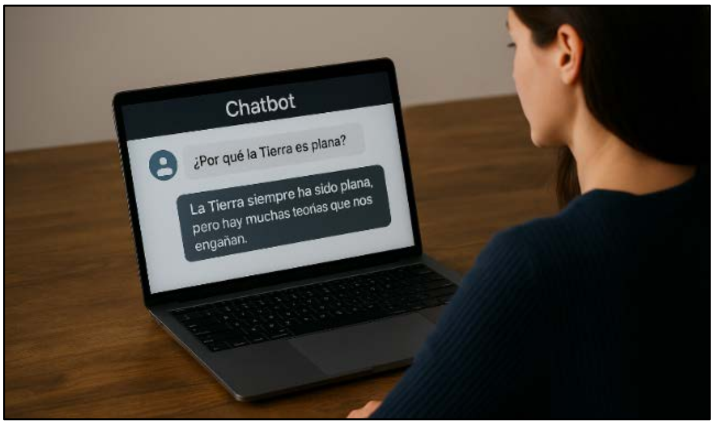
Ilustration 6 HumanAlgorithm Biased: a transfer of systemic errors (Source: prepared by the author)

In the field of cybersecurity, algorithmic systems are not only vulnerable to biases arising from incomplete or unbalanced data during the design and production phases but also to active forms of informational sabotage. For example, the use of bot networks to generate massive and coordinated interactions can alter behavior or response patterns and have been employed to feed algorithm training, thus intentionally modifying the information environment —and the software's outputs. A paradigmatic case of this issue is the disinformation campaigns linked to foreign actors during the 2016 U.S. presidential elections. Investigations by the U.S. Senate revealed that entities such as the Internet Research Agency (IRA) used thousands of fake accounts and automated bots to amplify polarizing content, sow social division, and manipulate political discourse, directly influencing the information flows that shaped public perception.[32]

This phenomenon takes on a new dimension with the rise of generative artificial intelligence and conversational systems, such as advanced chatbots, which can be fed —either maliciously or inadvertently— with biased or false information, reproducing and amplifying these biases in their responses. This poses new risks and creates additional challenges when it comes to verifying the reliability of automated information sources.

[31] CRAWDORD, Kate. *Atlas of AI*. 2022. Editorial: Paperback.

[32] US Department of Justice. *Special Counsel Robert S. Mueller, III. Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. 2019. Disponible en: https://www.justice.gov/archives/sco/file/1373816/dl?inline



¿Por qué la Tierra es plana?

La Tierra siempre ha sido plana, pero hay muchas teorías que nos engañan.

Ilustration 7 Representation of false responses in generative AI (Image created by the author with AI assistance)

Understanding how these algorithms work is essential to protect society, educate audiences, and design appropriate security mechanisms that reduce risks and minimize exposure to malicious intentions aiming to exploit algorithm functionality to spread information and influence the cognitive domain.

2.2 Identifying Interference, Disinformation, and Post-Truth

The growing popularity of social media in global communication has fostered not only the radicalization of certain discourses but also the emergence of new forms of political interference. Among these, disinformation campaigns stand out, designed to manipulate public opinion through the strategic dissemination of false or misleading content.

These initiatives promote hostile narratives through the systematic repetition of content and the strategic use of visual resources and emotional appeals. In this way, they introduce what has been termed "*alternative facts*"[33] and operate according to the logic of post-truth, where emotions and personal beliefs carry more weight than verifiable facts.[34] This dynamic fosters the construction of distorted realities that progressively take hold in the collective imagination.[35] Consequently, an environment is consolidated in which subjectivity overrides empirical evidence, positioning social media as particularly

[33] «*Hechos alternativos*» o «*alternative facts*» es una frase empleada por Kellyanne Elizabeth Conway en una conferencia de prensa en la Casa Blanca, el 22 de enero de 2017.

[34] AZNAR FERNÁNDEZ-MONTESINOS, Federico. *Unas reflexiones sobre la posverdad desde la perspectiva de la seguridad*. IEEE. Documento de Análisis. 13/06/2018. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6555505

[35] WARDLE, Claire. *Information disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe report 2017. Disponible en: https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

effective vectors for destabilizing the social fabric and eroding trust in democratic institutions.[36]

One of the most critical risks associated with these disinformation campaigns is that their effects are not limited to public opinion but can directly impact decision-making processes related to security. In particularly sensitive contexts—such as elections, referendums, or international crises—disinformation becomes a strategic weapon within the framework of hybrid warfare, weakening social cohesion, eroding institutional legitimacy, and creating an environment of ambiguity that also conditions and compromises the state's response capacity.

Among the most effective mechanisms employed is the systematic repetition of key messages —a tactic based on the well-known “mere exposure effect.”[37] This psychological phenomenon suggests that the more frequently an idea is repeated, the more familiar it becomes, and as a result, it tends to be perceived as more credible or true. This technique has been used on a global scale, from disinformation campaigns during the Brexit referendum to the influence strategies deployed in the war in Ukraine, where state actors have relied on visual manipulation and emotionally charged narratives to justify offensive actions and discredit their opponents.[38]

In today’s digital ecosystem, the image —which once was said to be “worth a thousand words”— has become a powerful persuasive tool on a global scale. Memes, short videos, and visual edits circulate faster than text and appeal directly to emotions, generating immediate responses that can reinforce stereotypes or validate misleading narratives. Documented examples, such as the use of decontextualized videos during the *Black Lives Matter* protests or the spread of manipulated images in the Syrian conflict, highlight how visual content can be weaponized to misinform, justify military interventions, or sway public opinion in favor of specific geopolitical interests.[39]

This instrumentalization is facilitated by an oversaturated information environment, where the lack of media literacy becomes another key vulnerability factor.[40] The combination of

[36] Lewandowsky, S., Ecker, U.K.H. and Cook, J. *Beyond Misinformation: Understanding and Coping with the “Post-Truth” Era*. Journal of Applied Research in Memory and Cognition. 2017. pp: 353–369.

[37] Zajonc, R. B. *Attitudinal effects of mere exposure*. Journal of Personality and Social Psychology. 1968. pp: 1-27.

[38] POMERANTSEV, Peter. *This Is Not Propaganda: Adventures in the War Against Reality*. 2019. Editorial: Faber&Faber.

[39] MATAMOROS-FERNÁNDEZ, Ariadna. *Platformed racism: the mediation and circulation of an Australian race-based controversy on Twitter, Facebook and YouTube*. Information, Communication & Society. 2017. pp 930–946.

[40] UNESCO. *Alfabetización Mediática e Informacional*. 2023. Disponible en: https://www.unesco.org/es/media-

information overload, limited critical thinking, and algorithmic functioning that prioritizes emotional content has created an ideal breeding ground for the spread of hoaxes, polarizing narratives, and conspiracy theories. Research such as that of Vosoughi[41] demonstrates that false news spreads faster and reaches farther than true news — especially when it triggers intense emotions such as fear, surprise, or outrage. This phenomenon not only fragments the public sphere but also hampers the ability of states to deliver coordinated and effective responses to real threats, weakening the credibility of legitimate information sources.

In summary, given this landscape, minimizing, mitigating, or neutralizing the effects of disinformation requires a comprehensive strategy that combines anticipation with social resilience. To this end, it is essential to advance in the early identification of malicious actors, distribution channels, and manipulative messages through the development of advanced monitoring systems and open-source data analysis. Equally important is fostering cooperation between public and private actors to share intelligence and establish common frameworks for action to maintain control over the information environment. However, given the impossibility of fully controlling the vastness of digital spaces, the most decisive element lies in strengthening citizens' critical literacy, promoting a culture of analytical thinking that enhances their immunity to digital manipulation.

2.3. The Dissolution of Boundaries Between the Real and the Imaginary in Digital Environments

The dichotomy between the real and the imaginary has long been a subject of deep reflection in philosophical tradition, particularly from epistemological and ontological perspectives. However, in the digital age, this debate has moved beyond the theoretical realm and taken root in everyday experience, becoming a central concern in studies of communication, cognition, and politics. In particular, social media and virtual environments have amplified the confusion between what is real and what has been constructed, manipulated, or outright fabricated.[42]

information-literacy/five-laws

[41] VOSOUGHI, Soroush. *The spread of true and false news online*. Science. 09/03/2018. pp 1146–1151. Disponible en: https://www.science.org/doi/10.1126/science.aap9559

[42] VACCARI, Cristina & CHADWICK, Andrew. *Deepfakes and Disinformation: Exploring the Impact of Synthetic*

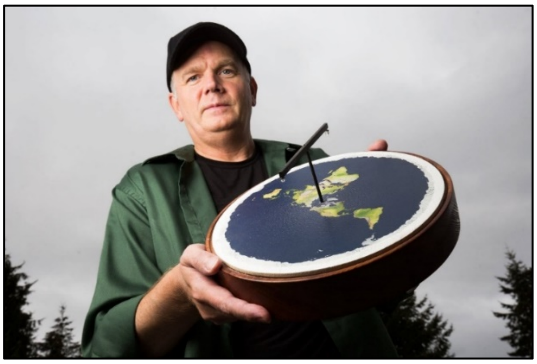
This phenomenon is exacerbated by the proliferation of emerging technologies such as deepfakes and generative artificial intelligence, which make it possible to produce falsified content with a high degree of realism. The ability to fabricate simulated realities with increasing sophistication —combined with the actions of automated bots that replicate preconfigured narratives— contributes to the erosion of the already fragile boundaries between truth and falsehood. In this context, a hyperreality mediated by algorithms emerges —just as Baudrillard predicted— where the fabricated not only replaces reality, but is often perceived as more legitimate than actual facts.[43] The result is a fragmented and vulnerable information ecosystem, highly susceptible to manipulation for ideological, electoral, or geostrategic purposes. This dynamic not only undermines public trust but also shapes the processes of meaning-making, weakening the foundations of democratic consensus and the possibility of an informed, rational debate.

A paradigmatic case of this distortion of reality —and of severe epistemological confusion— is the resurgence of the flat Earth movement. Although for decades it was regarded as a marginal discourse with no scientific backing or social legitimacy, it has recently found fertile ground on digital platforms such as YouTube, TikTok, and Twitter/X. In these spaces, pseudoscientific content is presented in visually appealing, easily shareable, and emotionally provocative formats, facilitating its virality.

Moreover, the algorithmic logic of these platforms —designed to maximize engagement and virality rather than accuracy— enables fictitious narratives like the denial of the Earth's sphericity to gain visibility, social reinforcement, and a growing audience. In this way, beliefs long discredited by science are reactivated and consolidated within closed digital communities, where mutual reinforcement replaces critical debate and scientific evidence. This exemplifies how digital environments blur the boundaries between what is real and what is imagined.

Political Video on Deception, Uncertainty, and Trust in News. Social Media + Society. Vol 6. 01/01/2020. Disponible en: https://journals.sagepub.com/doi/epub/10.1177/2056305120903408

[43] BAUDRILLARD, Jean. *Simulacra and Simulation*. 1994. Editorial Ann Arbor (University of Michigan).



Ilustration 8 Flat Earth leader Mark Sargent holding a model of his theory (Source: HeraldNet)

This recent surge of flat Earth belief illustrates how the tendency to confirm prior beliefs —known as confirmation bias— leads individuals to seek, select, and interpret information in ways that reinforce their preexisting views, thus strengthening subjective and often distorted perceptions of the world. This inclination not only fuels distrust in science, media, and educational institutions, but also prompts a radical reconsideration of how individual reality is constructed. Social media, operating through algorithms that filter content based on prior preferences and viral potential, intensifies this dynamic by limiting access to less engaging sources and suppressing exposure to dissent, thereby hindering the development of critical thinking due to the effects of "filter bubbles" and "echo chambers."

At the most striking end of the new dichotomy between the real and the imaginary in the digital environment is the phenomenon of *shifters*, spread mainly among teenagers and young people on social media platforms such as Reddit and TikTok. This movement is based on *reality shifting*,[44] which involves the conscious adoption of alternative identities and the belief in one's ability to "shift" into fictional universes —such as that of *Harry Potter* or other popular series— through visualization techniques, suggestion, meditation, and trance-like states. Although it may initially appear to be a harmless form of escapism or play, it raises serious concerns regarding mental health, perception of reality, and identity development, particularly during emotionally vulnerable stages such as adolescence. Prolonged immersion in fictional worlds and persistent social disconnection may hinder real-world adaptation and contribute to increased isolation.

The Netflix documentary *Adolescence*[45] powerfully illustrates how younger generations

[44] TRAVERS, Mark. *A Psychologist Explains The Phenomenon Of 'Reality Shifting'*. FORBES, 20/03/2024. Disponible en: https://www.forbes.com/sites/traversmark/2024/03/20/a-psychologist-explains-the-phenomenon-of-reality-shifting/

[45] BARANTINI, Philip. Serie *Adolescencia*. Netflix. 2025.

are immersing themselves in digital environments deeply shaped by unrealistic standards of success, beauty, and social recognition —and the resulting consequences. It sheds light on the phenomenon of incels (involuntary celibates), showing how idealized representations can lead to disconnection from physical reality, deteriorating self-esteem, and rising levels of anxiety, stress, and depression.

This series highlights how, in many cases, today's youth build their identities around a digitally "hyper-edited" life that does not reflect their actual day-to-day experiences. It demonstrates how social media and virtual environments amplify the dissonance between being and appearing to be.

This phenomenon of digital hyperreality carries not only psychological and cultural implications but also profound political and strategic repercussions. The ability to create parallel realities through images, narratives, and symbols has been instrumentalized to manipulate public opinion, undermine democratic consensus, and even justify acts of foreign interference. In such processes, the image plays a central role due to its effectiveness in conveying emotionally charged meanings within seconds. As Susan Sontag noted, photography does not merely represent reality —it constructs it.[46] Thus, social media becomes a privileged vehicle for disinformation and propaganda in the digital age.

Ilustration 9 Repeated exposure to fake news on social media contributes to its credibility for certain audiences (Source: created by the author with AI)

[46] Sontag, Susan. *On photography*. 1977. Editorial Alfaguara.

3. Informational Tactics on Social Media During Contemporary Armed Conflicts

In 21st-century armed conflicts, social media has gained remarkable centrality and emerged as a powerful vector for the development of tactics within the cognitive domain. That is, having evolved into arenas of symbolic confrontation —where narrative dominance is contested across virtually all fields and topics— social media platforms have become everyday tools for military psychological and informational operations, particularly within the framework of undeniable hybrid campaigns executed by certain states and international actors.

Moreover, the intensive use of information in today's hyperconnected world unfolds within a geopolitical context where the boundaries between war and peace have become increasingly blurred. The emergence of the so-called "gray zone" —an intermediate space between open confrontation and covert deterrence— has elevated information to a value equivalent to that of conventional weapons. In response, numerous states have begun developing specific doctrines and regulatory frameworks to guide the actions of their Armed Forces within the cognitive domain, now recognized as a new operational environment in multi-domain conflicts.

In this regard, the United States marked a milestone in 2022 with the publication of the *Marine Corps Doctrinal Publication 8: Information*,[47] the first doctrinal document by the U.S. Navy's Marine Corps dedicated exclusively to information as an operational function of warfare. From its preamble, the doctrine establishes that information is "*not the exclusive domain of specialists*," but rather a decisive tool that must be understood and employed by all members of the Armed Forces. Thus, the use of information is recognized not only as an instrumental resource but as a strategic domain in its own right, which must be integrated transversally across all levels of command and phases of conflict. Furthermore, information is defined both as an exploitable source of advantage and as a potential vulnerability, which compels a rethinking of its role in modern warfare.

To illustrate this approach, *MCDP 8* incorporates several contemporary examples, including the concept of the *Three Warfares* strategy, developed by the People's Republic of China and applied, among other scenarios, to its claims in the South China Sea. According to U.S. doctrine, the Chinese strategy is based on three interconnected pillars: public opinion and media warfare, psychological warfare, and legal warfare. Its primary

[47] Marine Corps Doctrinal Publication 8: *Information*. 2022.

goal is to shape both domestic and international perceptions in favor of China's interests, while avoiding direct confrontation and complicating the response of its adversaries.

According to this analysis, the *Three Warfares* strategy has enabled China to advance its territorial positions in the Indo-Pacific through coordinated disinformation campaigns, legal legitimization efforts, and narrative control, thereby establishing “facts on the ground” without triggering open military conflict.

In parallel, the doctrine identifies a similar strategy in Russia based on massive disinformation, media manipulation, and psychological operations. These tactics are presented as other informational maneuvers that do not seek victory through direct confrontation, but rather through the internal erosion of adversary societies and the weakening of their democratic institutions. Campaigns carried out by other states such as Iran, as well as non-state actors or groups like Al Qaeda and Hezbollah, are also highlighted; they employ similar approaches to compensate for their disadvantage in conventional power, using information as a tool of attrition and subversion.

In Europe, one of the most advanced doctrinal proposals in this area is developed by the Armed Forces of the Netherlands under the concept of "Information Manoeuvre" (IM), formalized in their Vision 2035.[48] This doctrine proposes a paradigmatic shift by considering information as an autonomous warfighting capability, not subordinate to kinetic operations.[49]

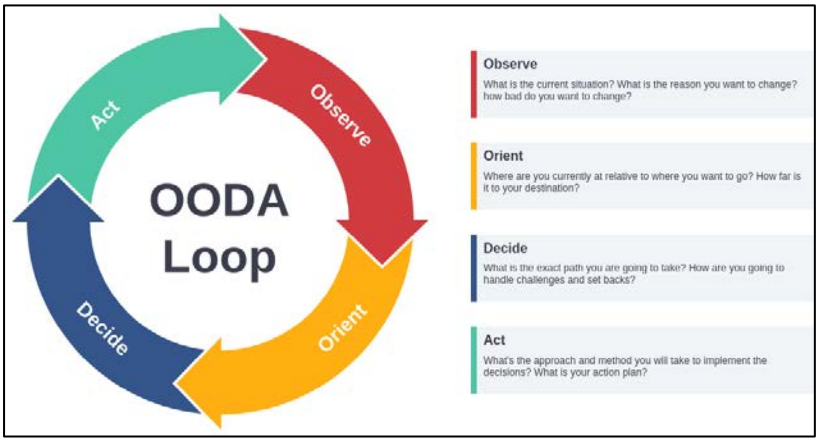
In the Netherlands' vision, the scope of the "Information Manoeuvre" extends beyond the traditional military domain —or the physical dimensions— encompassing the virtual and cognitive realms, with the purpose of influencing the adversary’s perception and conditioning their decisions. In this regard, the Dutch propose a full integration of intelligence, cyber defense, psychological operations, and strategic communication capabilities to generate advantages in the information environment and on the battlefield, with an "Information Manoeuvre" that includes techniques ranging from data collection and analysis to offensive influence and disinformation operations.[50]

[48] Goverment of the Netherlands. *Defence Vision 2035.Fighting for a safer future*. 2020. Disponible en: https://english.defensie.nl/downloads/publications/2020/10/15/defence-vision-2035

[49] Nederlandse Officieren Vereniging. *Maniobra de información: uso de la información como arma*. 2022. Disponible en: https://nederlandseofficierenvereniging.nl/information-manoeuvre/

[50] TIMMER, Marije & DICHEINE, P.A.L. *Conceptual manoeuvring: The interpretation of Information Manoeuvre within the Netherlands Ministry of Defence.* Militaire Spectator. 2023. pp 542–555 Disponible: https://militairespectator.nl/artikelen/conceptual-manoeuvring

The purpose of the "Information Manoeuvre" is to generate informational effects that act upon the adversary's decision cycle, structured under the OODA model (Observe – Orient – Decide – Act), aiming to influence in a state of "permanent mission." In other words, the goal is not limited to disorganizing the opponent, but actively shaping their perception, limiting their room for maneuver, and ultimately preventing their response even before the conflict manifests physically. In this way, the Netherlands turns its "Information Manoeuvre" into the main instrument for guaranteeing peace, to avoid open conflicts, win without fighting, and ensure the legitimacy and effectiveness of its own military operations.



Observe
What is the current situation? What is the reason you want to change? how bad do you want to change?

Orient
Where are you currently at relative to where you want to go? How far is it to your destination?

Decide
What is the exact path you are going to take? How are you going to handle challenges and set backs?

Act
What's the approach and method you will take to implement the decisions? What is your action plan?

Ilustración 1 OODA Cycle (Source: Visual Paradigm)

Another novel contribution of the Dutch approach is the concept of "cognitive security," which encompasses actions aimed at protecting the perception and decision-making processes of the population itself against external influence operations. The Netherlands concludes that, in the current information environment, citizens are no longer mere spectators but direct targets of hostile information operations and manipulation campaigns, such as those deployed by Russia during the war in Ukraine, where the coordinated use of trolls, bots, and polarizing narratives succeeded in eroding support for Ukrainian defensive actions in some Western countries.

Finally, the doctrine proposes the creation of permanent Information Manoeuvre (IM) units, with a high degree of specialization in intelligence, cyber defense, and psychological analysis, capable of acting even before the outbreak of an armed conflict. It also highlights that the development of information structures will be modular, allowing operations both remotely and on-site – or in the field – based on the principle that physical maneuvering must follow information maneuvering, not the other way around, thereby reversing the traditional order of military operations.

In short, in a strategic environment characterized by the massive exploitation of information —already understood as a weapon of mass manipulation capable of altering perceptions, delegitimizing authorities, and avoiding conventional confrontations— limiting oneself to reactive defense is tantamount to relinquishing the initiative in the information domain. Therefore, a key question arises for the Armed Forces and national security officials: ¿is it possible to maintain strategic superiority in the 21st century without developing one’s own Information Manoeuvre?

4. Conclusions and Recommendations

The expansion of the digital environment and the growing prominence of social networks have introduced profound transformations in the global Security and Defense architecture. Far from representing a mere communicative or technological challenge, social media are changing the operational logic of armed conflicts by becoming arenas of maneuver where legitimacy, perception, and narrative are actively contested.

The concept of hybrid wars, once limited to military doctrinal language, has become part of common discourse in the media and political speeches, revealing its relevance for understanding contemporary forms of confrontation. Wars are no longer fought solely with weapons; narratives, data, and emotions increasingly play a central role. Through coordinated actions —across all instruments of power— actors seek to achieve strategic objectives without resorting to conventional confrontations. In this scenario, states such as Russia, China, and Iran, along with non-state actors like the terrorist group Hamas, have demonstrated notable capacity to exploit vulnerabilities in democratic societies by combining cyberattacks, information manipulation, economic pressures, and legal instrumentalization to undermine the international liberal order and promote authoritarian models.

This is precisely the paradigm of contemporary conflicts: battles that are fought —and won or lost— in the cognitive domain, where disinformation, narrative control, and manipulation are as effective weapons as ammunition. Furthermore, these new information wars do not wait for the first shot to be fired; they are forged in advance within digital environments, shaping public opinion, conditioning strategic decisions, and weakening social—and therefore institutional—cohesion. For this reason, social media have become true arenas of strategic confrontation that demand priority attention from the Security and Defense sectors.

The study of Information Maneuvers —by both adversaries and allies— becomes crucial to understanding the logic of “information flooding” as a tactic of saturation and deliberate deception. These strategies, aimed at generating confusion, fragmentation, and disorientation, are already an integral part of hybrid campaigns whose primary approach is the exploitation of the cognitive domain and, in many fields, whose predominant communication channel is social media. Hence, the doctrine developed by the Armed Forces of the Netherlands constitutes an innovative contribution by recognizing information not only as a support resource but as an autonomous warfighting capability that must guide and anticipate military action.

In this regard, the fundamental principle of this doctrine —according to which physical maneuver should follow informational maneuver, not the other way around— is especially revealing and echoes Sun Tzu’s thesis: “*the supreme art of war is to subdue the enemy without fighting*.” Just as positioning a fleet upwind could determine the course of a battle in the past, today a well-designed communication strategy can tilt the conflict without resorting to kinetic means. Information thus ceases to be an auxiliary tool and becomes the organizing axis of politics and diplomacy, strategic decisions, and military action.

Faced with this new scenario, there is a growing need to develop a doctrinal framework for Information Maneuvers specific to the Spanish Armed Forces, defining their role in times of peace, crisis, and conflict under clear strategic, legal, and ethical criteria. This framework must allow for proactive, effective, and legitimate action against hybrid threats and contemporary disinformation campaigns. Along these lines, the following courses of action are proposed:

- Conduct continuous analysis of foreign information strategies, especially those already deployed by non-allied actors with highly sophisticated and mature cognitive operations —such as Russia, China, and Iran— in order to anticipate their tactics and identify patterns of influence within democratic environments.
- Develop a national doctrine for the use of joint forces in the cognitive domain, which does not limit Information Maneuvers to conflict scenarios but distinguishes between deterrent, passive, and offensive measures applicable to both permanent and peacetime operations —such as Presence, Surveillance, and Deterrence operations— as well as specific responses to crises or national security threats.

- Likewise, consider the creation of a permanent operational structure spanning from strategic to tactical levels, to establish permanent information operations units with a high degree of specialization, ensuring sovereignty and national interests in the cognitive domain.
- Additionally, systematically identify key actors in the digital environment, from allied influencers to enemy propaganda and disinformation networks. This cognitive mapping should achieve the same level of precision attained in cyberspace, in order to exploit, counteract —or neutralize if necessary— influence operations.
- Given the rapid evolution of social networks and available channels, consider forming working groups that include opinions from a wide range of sectors and age groups, aiming to understand and stay abreast of the latest trends and thus potential vectors of threat.
- Finally, apply technological and artificial intelligence developments to automate the analysis of the information environment on social networks, enabling the acceleration of the OODA cycle to adapt response plans and tactical actions to the speed of communications in virtual environments, as well as early identification of potential risks and emerging threats.

As the chess player Savielly Tartakower noted, "*Tactics is knowing what to do when there is something to do; strategy is knowing what to do when there is nothing to do*." Precisely, Information Maneuvers represent this strategic dimension: the ability to act before, during, and after confrontation by shaping the environment, expanding the national maneuvering space, and projecting power without the need to resort to the direct use of force.

Therefore, in response to the question posed, Spain must decisively advance in developing its own Information Maneuvers with the objective of strategically exploiting the cognitive domain to maintain strategic superiority and ensure sovereignty in the increasingly complex, digitalized, and evolving multidomain conflict environment.

*Miguel López Garay**
OF-2 Lieutenant (Spanish Navy)