ieee.es
Instituto Español de Estudios Estratégicos

Opinion Paper

02/2026 09/01/2026

*Ángela Navarro Paredes**

Information in Hybrid Warfare. Early Predictive Model Proposal

Information in Hybrid Warfare. Early Predictive Model Proposal

Abstract:

In the context of contemporary warfare, information becomes both an instrument of power and a destabilizing element. This article reflects on the impact of disinformation and narrative manipulation on security and institutional trust, as well as the need to implement a system capable of anticipating informational threats. Based on the analysis of narratives and emotions on social networks, the importance of integrating technological tools and human working groups to strengthen the strategic resilience of states is highlighted. In this way, the use of information as a weapon of power and an influential element in shaping the international status quo is underscored.

Keywords:

Information, Disinformation, Hybrid war, Social networks.

How to quote:

NAVARRO PAREDES, Ángela. *Information in Hybrid Warfare. Early Predictive Model Proposal*. Opinion Paper. IEEE 02/2026. 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.

Owing to the increasing prevalence of social networks, not merely as instruments of communication or interpersonal interaction, but also as vehicles for the transmission of information, recent years have witnessed significant advances in the optimization of processes and workflows. Nevertheless, this evolution has simultaneously introduced new risks that expose individuals, institutions, and even states to complex situations with potentially detrimental consequences. Consequently, the very concept of conflict has undergone a profound transformation, giving rise to new modalities such as the concept of hybrid warfare.

Over the past decades, hybrid conflicts have become a real and difficult challenge to confront. This has led to the emergence of new threats for governments, as well as battlefields that are increasingly hard to control, with information, among others, becoming a territory to be conquered or defended. Within this scenario, a new world order arises in which the most powerful actor is no longer the one with the greatest wealth, military strength, or political influence, but rather the one that controls information and the narrative, both in traditional media such as television, radio, or the press, and in digital platforms such as social networks.

In this new order, information thus becomes essential, not only to sustain the democratic principle of access to information, which fosters civic participation, but also as a weapon. Control over what is transmitted or, more precisely, how it is transmitted, has become a way to sow doubt and fear, polarize societies, and even erode public trust in institutions. All these factors today can be considered equally, or even more, effective than the occupation of a territory or the violation of national sovereignty.

Nevertheless, current responses to hybrid warfare campaigns tend to be reactive. Action is only taken once the damage has already been done and fake information has fulfilled its intended purpose, or democratic processes have been destabilized through institutional distrust. This reveals a genuine weakness, which is the lack of early warning mechanisms capable of detecting such hybrid operations in their initial stages, before they can inflict harm.

To address this problem, this article proposes the development of an early predictive model based on the analysis of narrative and emotional patterns on social media. It assumes that hybrid operations leave detectable traces in online discourse before their effects materialize in politics, economics, or society. Such traces may appear as radical

shifts in public opinion regarding certain issues, irregular surges in polarizing emotions, repetition of identical messages by fake accounts or bots, or the massive distribution of manipulated audiovisual content known as deepfakes[1].

Moreover, this analysis includes the concept of "information overload" or "infoxication", referring to the excessive flow of information injected into society, which undermines citizens' critical thinking[2]. The saturation of information, whether reliable or fake, encourages confusion and facilitates the spread of misinformation. In this sense, information overload can be viewed not only as a byproduct of active digital media use, but also as a genuine vector that amplifies the effectiveness of hybrid campaigns.

Hybrid Warfare and (Dis)Information. Predicting Hybrid Warfare through Behavioral Pattern Changes on Social Media.

Hybrid Warfare in the Contemporary Context. Information and Disinformation as Weapons.

In the contemporary understanding of hybrid warfare, information has evolved from being a mere channel for transmitting data and events to becoming a key strategic tool within the sphere of geopolitics. As a result, battles are no longer fought solely through the use of tanks, warships, or aircraft, but also through the deployment of symbolism, emotion, and the manipulation of perceived reality as offensive instruments. Many states and non-state actors have identified the potential of information as a means to destabilize the international order, undermine democratic institutions, and weaken societies from within, without resorting to direct or physical violence[3].

One of the most recurrent tactics in this new form of warfare is the manipulation and control of narratives through disinformation campaigns. Such campaigns are designed to confuse, polarize, and foster distrust toward corporations, public institutions, media organizations, the armed forces, and law enforcement agencies, or even among citizens themselves. In the present era, rather than keeping silent information wise, the goal is to

[1] CHESNEY, Robert & CITRON, Danielle, *Deepfakes and the New Disinformation War.* Article Foreign Affairs https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war (accessed on the web 22/05/2025).
[2] CORNELLA, Alfons, *Infoxicación. Buscando un orden en la información.* Book (accessed 22/05/2025).
[3] HOFFMAN, Frank G., *Conflict in the 21st Century: the rise of hybrid wars.* Book (accessed 24/05/2025).

make noise. This involves the deliberate injection of excessive and often contradictory messages, the falsification of data, and the dissemination of half-truths, thereby disorienting individuals and impairing their capacity for critical judgment by blurring the distinction between factual reality and dialectical fiction. Consequently, this phenomenon is amplified within the environment of information overload, not with the intention of convincing audiences that a specific statement is true, but rather of obstructing access to the truth itself[4].

In conflict scenarios such as the one waged between Russia and Ukraine in recent years, these strategies have been employed with notorious effectiveness. During the conflict, Moscow promoted numerous alternative and contradictory narratives to the Western discourse, using both aligned media outlets and social networks to justify and legitimize its intervention in Ukrainian territory, while simultaneously undermining international support for the Ukrainian government. At the same time, many European states were affected by the dissemination of conspiracy theories, manipulated images, and fake news and stories designed to erode social cohesion, generate doubts about the sanctions imposed, as well as foster Russia-leaning perceptions among specific population groups.

Social networks thus assume a decisive role within this emerging dynamic. Owing to their capacity to segment audiences and to accelerate the viral dissemination of content, they have become a privileged battlefield for cognitive warfare, defined by Daniel Iriarte in his book "*Guerras cognitivas*" as a means of influencing thought and shaping reasoning and behavior through overexposure to information, derived from psychological campaigns[5]. Today, platforms such as X (formerly known as Twitter), TikTok, Instagram, and Facebook enable the rapid and indiscriminate dissemination of messages that exploit the emotions of their recipients, particularly fear, outrage, frustration, anxiety, and confusion. This dissemination of false information is further amplified by bots and fake accounts, which operate in a fully automated manner and without the need of direct human intervention[6].

[4] PEIRANO, Marta, *El enemigo conoce el sistema: Manipulación de ideas, personas e influencias después de la economía de la atención.* Book (accessed 01/09/2025).
[5] IRIARTE, Daniel. *Guerras cognitivas.* Book (accessed 23/10/2025).
[6] LÓPEZ GARAY, Miguel, *Las redes sociales como armas de influencia masiva y la necesidad de una doctrina informativa.* Opinion Paper IEEE n. 68/2025. https://www.defensa.gob.es/ceseden/-/ieee/las_redes_sociales_como_armas_de_influencia_masiva_y_la_necesidad_de_una_doctrina_informativa#A14 (accessed on the web 23/10/2025).

In response to this paradigm, several international organizations have underscored the urgent need to develop media literacy strategies to counter disinformation. For instance, the European Union has promoted initiatives such as “EU vs. Disinfo” to monitor and neutralize foreign influence campaigns, including those orchestrated by Russia[7]. Nonetheless, the rapid and continuous evolution of technology, together with the development of increasingly sophisticated artificial intelligence software that contributes to the creation of disinformation through tools such as deepfakes, renders this domain unstable, volatile, and hard to regulate.

Ultimately, hybrid warfare in the twenty-first century finds in information its most subtle and powerful weapon. Thus, the issue is no longer who possesses the truth, but who succeeds in imposing their narrative upon the collective imagination.

The Current Problem: Delayed Reaction to Attacks. Limitations of Existing Response Models and the Risks of Acting Too Late.

Over the years, hybrid campaigns based on disinformation have revealed evident shortcomings in current response models. Acting belatedly not only entails losing control of the narrative but also fosters the erosion of public trust in government, the polarization of social debate, and the proliferation of a widespread sense of confusion and uncertainty. In a world where information is weaponized, delay in response represents yet another form of defeat. For this reason, it is key to anticipate false narratives and reinforce the capacity for early response in such contexts.

It is therefore essential to examine the limitations of current response models and, subsequently, the risks associated with delayed action. The principal weaknesses of the existing framework can be summarized as delayed and fragmented reactions, a lack of coordination among actors, insufficient media literacy among modern populations, dependence on private and opaque platforms, and vulnerability to increasingly sophisticated hybrid tactics.

First, regarding delayed and fragmented reaction, current detection systems rarely anticipate disinformation attacks; rather, they tend to respond only once false narratives

[7] EUvsDisinfo, *The architecture of Russia’s FIMI operations.* https://euvsdisinfo.eu/the-architecture-of-russias-fimi-operations/ (accessed on the web 23/10/2025).

have already spread. Second, the absence of coordination among key stakeholders, that include governments, media organizations, civil society, and social networks, results in uneven and disjointed responses, significantly reducing overall effectiveness. Third, inadequate media literacy prevents citizens from accessing the necessary tools to distinguish reliable information from fake facts. This limitation weakens institutional communication campaigns, leaving the public exposed to viral hoaxes, deepfakes, and other disinformation instruments that form part of potential hybrid operations on social media.

Fourth, states rely heavily on platforms such as X, Telegram, Instagram, or Facebook to counter disinformation. However, these networks are not always transparent and often fail to provide timely responses, as their algorithms tend to promote emotionally-charged or extreme content. Finally, the combined use of tools such as bots and deepfakes, along with attacks on institutional credibility and the coordination of targeted campaigns, surpasses the capacities of governments and verification mechanisms, which are generally designed to counter isolated disinformation incidents rather than structured hybrid campaigns that have already made a significant impact.

Delayed action also entails a range of serious risks. These include the loss of control over the narrative and the creation of an environment contrary to national interests, the emergence of widespread social and institutional distrust, the exploitation of vulnerabilities by hostile powers, the induction of emotional and psychological instability, and even the legitimization of aggressors. Regarding the loss of narrative control, when reliable information arrives too late, fake statements are allowed to penetrate public opinion. As a result, it becomes increasingly difficult for the truth to regain ground, given the reluctance of certain social sectors to believe official versions of events or follow institutional recommendations during crises.

In the case of growing social and institutional distrust, the constant exposure of the public to disinformation can generate skepticism toward official narratives presented by governments, the media, or even scholars and scientists. Such erosion of trust may lead to disobedient behavior, social polarization, and, consequently, the weakening of institutional structures. These feelings can create a state of vulnerability and chaos that foreign powers may exploit to destabilize democratic regimes from within, as it happened

in Ukraine, where information exerted greater influence over collective thought than military offensives themselves.

Moreover, the saturation of information, also known as “infodemic”, which goes hand in hand with the confusion and fear produced by disinformation, may result in emotional and psychological destabilization, reducing citizens’ ability to respond effectively during situations of emergency or crises. When disinformation prevails over factual content, the aggressor may even appear as a victim or as a defender of a just cause

It is therefore evident that disinformation is not merely a communication problem but a strategic threat that demands coordinated, preemptive, and well-structured responses. A delayed reaction, consequently, becomes yet another way of losing a war without ever setting foot on the battlefield.

Proposal for an Early Predictive Model of Hybrid Warfare through the Analysis of Narratives and Behaviors on Social Media.

Taking as a point of departure the negative effects derived from the lack of anticipation toward information-related campaigns that constitute hybrid operations on social media, it becomes evident that there is a pressing need to formulate an early prediction model based on the analysis of both narratives and user behaviors within these platforms. The aim of this model is to move beyond the current reactive approach, that responds only after the information operation has achieved its intended objectives. This pattern is, in fact, easily identifiable as narratives are established well before the attacks themselves take place[8].

Accordingly, the design of this early predictive model is grounded in the observation of certain activity patterns, fluctuations in the popularity or virality of specific narratives, and alterations in user behavior on social networks that may precede more visible actions. The analysis of behavior on social media can be optimized through the use of artificial intelligence and data analysis tools such as Pulsar, CrowdTangle, and Meltwater, which enable the identification of behavioral patterns and changes in narrative dynamics. However, these technological instruments must be employed along with the human

[8] POMERANTSEV, Peter, *This is not propaganda: Adventures in the war against reality.* Book (accessed 11/06/2025).

factor, responsible for interpreting the extracted data, assessing whether a genuine informational threat exists, and determining its origin, onset, and potential impact.

The aforementioned programs are used for different purposes. First, Pulsar aims to analyze how users think and communicate across online platforms. It does so through artificial intelligence that studies opinions, emotions, and the topics discussed in both social networks and news media. This tool is particularly useful for understanding the discourses of specific communities or social groups. Second, CrowdTangle allows the monitoring of viral posts on platforms such as Facebook and Instagram. Rather than analyzing individuals, it focuses on the most widely shared content, an asset for detecting fake news or identifying trending topics on social media at any given time. Finally, Meltwater combines monitoring capabilities for both social networks and other media formats, including blogs, the news, and podcasts. It is therefore employed to ascertain what is being said about a given institution or topic and how it is perceived by the public.

In addition, to optimize data extraction, it would be necessary to codify narratives. That is, to establish themed and emotional categories that ease the detection of potential changes within them. The predictive model would also rely on alert systems based on quantitative thresholds. In practical terms, this means that once certain signals surpass pre-established limits, human analysts would intervene. For instance, if the use of narratives containing polarizing or sensitive topics were to increase by thirty percent, the human analysis working group would assess whether an informational threat exists. Should an operation or campaign be detected in advance, a warning would automatically be issued to the authorities responsible for social communication within the ministry of defense, or corrective messages would be disseminated.

Accordingly, several risk indicators may be identified. First, alterations in emotional discourse and lexical patterns, such as the substitution of neutral terms with more emphatic ones or with stronger connotations. For example, replacing “war” or “conflict” with “invasion,” or “affected” with “victim.” Second, attention must be paid to shifts in discussion topics, particularly those of polarizing or sensitive nature, such as immigration, national identity, the armed forces, the public healthcare system, or national education. Third, an atypical surge in activity among bot accounts or fake profiles disseminating false news on a massive scale, promoting certain hashtags, or sharing nearly identical

arguments in unison on specific issues.

Fourth, the emergence of discourses directly or indirectly attacking the institutional guarantors of democracy and constitutional order, such as the armed forces, judges, or the media, serves as a relevant indicator for detecting agents seeking to destabilize society. Last, the widespread distribution of deepfakes, manipulated videos, and memes, as opposed to authentic videos or well-written texts, together with an increase in the presence of emotionally charged or extreme content related to specific topics.

To illustrate the functioning of the proposed predictive model in the face of information-related operations on social media, a hypothetical scenario could be considered within a state referred to as “X.” A few weeks before general elections take place, a system of semantic and emotional monitoring applied to social networks detects anomalous activity concerning the potential role of the armed forces in the electing process. New anonymous and coordinated accounts appear on platforms such as Telegram, TikTok, and X, disseminating fear-based messages regarding an alleged covert military intervention intended to alter election results. Within less than 48 hours, these emotionally-charged videos, photographs, and publications reach massive audiences.

Through the proposed early prediction model, several indicators are identified: ani increase by 30% in posts containing the expressions “electoral fraud” and “covert coup d’état”, the repeated use of identical hashtags by newly created accounts, and the predominance of negative emotions such as fear or anger in user discourse. Upon surpassing the pre-established 30% threshold of terms considered conducive to public polarization, an automatic alert would be issued to the Informational Cyber Defense Coordination Center, composed of government technicians, intelligence analysts, fact-checking agencies, and specialists in strategic communication.

Once the alert is received, the corresponding protocol would be activated, and a qualitative analysis would confirm that the disseminated narrative forms part of an attack orchestrated by a foreign power. The institutional response would then focus on three fronts. First, the ministry of defense would issue a public statement refuting the accusations. Second, collaboration would be established with fact-checking agencies, such as Newtral and Agencia EFE, to discredit the harmful viral content. Finally, the government of state “X” would contact Telegram, TikTok, and X to report the dialectics

employed and expose those accounts that violate platform policies or constitute a national security risk.

Furthermore, the government would launch an information campaign aimed at reinforcing, on one hand, the essential role of the armed forces as defenders of constitutional order, and on the other hand, the guarantee of transparency in national electoral processes. Through these preventive measures, the information campaign would lose momentum and credibility before the disseminated narrative could solidify in the collective imagination, thereby preserving public trust and ensuring the normal organization of general elections in state “X.”

Finally, a SWOT analysis (Strengths, Weaknesses, Opportunities, and Threats) is proposed to evaluate the key elements that could influence the development and implementation of the predictive model.

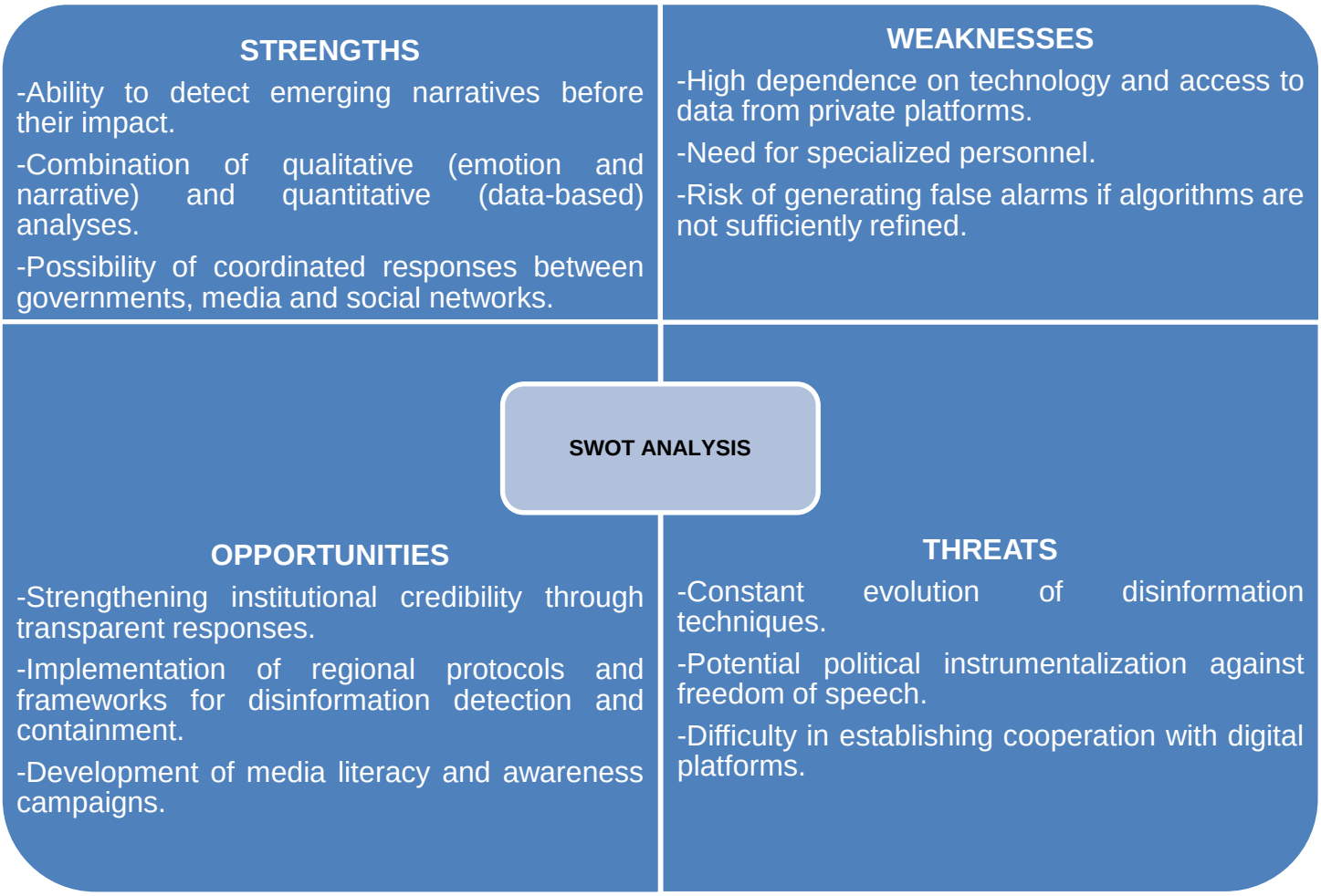

Figure 1: SWOT Analysis on the early predictive model for hybrid campaigns based on information (developed by the author).

Conclusion

Throughout this article, it has been shown that the design of hybrid campaigns through the use of information and disinformation represents a tangible threat to both the security and the stability of contemporary democratic societies. The analysis of the impact of information on users has clearly shown that current responses tend to be reactive and delayed.

Taking this limitation as a point of departure, the need and potential effectiveness of an early predictive model emerge as key elements for the prevention of the possible effects of operations that take information as a weapon. Based on the narrative and emotional analysis of social network activity, it has been verified that it is possible to identify signals that precede the deployment of such campaigns. Implementing this model, therefore, not only enhances informational resilience, but also constitutes an essential strategy to

safeguard the right to truthful information, institutional and democratic stability, and national security within the current global context.

Angela Navarro Paredes

Lieutenant Junior Grade in the Spanish Navy Supply Corps with a double degree in International Relations and Business Administration.