Instituto Español de Estudios Estratégicos

Opinion Paper

Visit webpage Receive Newsletter

70/2026 22/06/2026

*Carlos Galán Cordero**

Multi-domain conflict and hybrid warfare in the 21st century

Multi-domain conflict and hybrid warfare in the 21st century: from the case of Ukraine to the escalation between the United States, Israel, and Iran

Abstract:

Contemporary armed conflicts reveal a growing integration between conventional military operations, cyber operations, and information influence campaigns. This phenomenon falls within the paradigm of hybrid warfare, in which state and non-state actors combine military, technological, economic, and informational instruments to achieve strategic objectives across multiple operational domains. This paper analyzes the role of the digital ecosystem and the cognitive domain in the evolution of armed conflicts in the 21st century. Through a comparative analysis of the war triggered by the Russian invasion of Ukraine, the conflict between Israel and armed groups in the Gaza Strip, and the recent military escalation between the United States, Israel, and Iran, the article examines how information operations, cyber operations, and influence strategies are integrated into contemporary strategic planning.

Keywords:

Hybrid warfare; cognitive operations; strategic disinformation; armed conflicts.

How to quote:

GALÁN CORDERO, Carlos. *Multi-domain conflict and hybrid warfare in the 21st century*. Opinion Paper. IEEE 70/2026.

Introduction

The evolution of armed conflicts in the 21st century highlights a profound transformation in the nature of war and strategic competition between states. Contemporary confrontations no longer unfold exclusively on the physical battlefield but extend to other domains such as cyberspace, the information environment, and the cognitive domain. In this context, information has become a strategic resource whose management can be as decisive as territorial control or conventional military superiority.

This phenomenon is often described through the concept of hybrid warfare, which refers to the combined use of military, cyber, informational, economic, and diplomatic instruments to achieve strategic objectives. The integration of these instruments allows the actors involved to exert pressure on their adversaries across multiple operational domains, generating cumulative strategic effects without necessarily resorting to traditional forms of direct military confrontation.

The development of digital technologies and the expansion of global communication platforms have significantly amplified the scope of these dynamics. Social media and other digital communication channels enable the dissemination of strategic narratives on a global scale, the mobilization of international audiences, and the shaping of perceptions about conflicts in real time. As a result, the information environment has become a central arena of confrontation in which state and non-state actors compete to influence public perception, the political legitimacy of military operations, and decision-making processes.

Recent conflicts clearly illustrate this transformation. The war triggered by Russia's invasion of Ukraine has highlighted the importance of influence campaigns, open-source intelligence, and digital platforms in constructing strategic narratives. At the same time, the conflict between Israel and armed groups in the Gaza Strip demonstrates how the contest over the international legitimacy of military operations is increasingly playing out in the digital ecosystem. The recent escalation between the United States, Israel, and Iran further confirms that the dynamics of hybrid warfare can coexist with higher-intensity military confrontations and generate strategic effects that extend far beyond the regional sphere.

These examples suggest that informational dominance and cognitive dominance have acquired growing relevance in the conduct of contemporary armed conflicts. Operations aimed at influencing perceptions, narratives, and decision-making processes have become central instruments of global strategic competition; consequently, understanding the evolution of warfare in the 21st century requires integrating traditional military analysis with the study of the informational, technological, and cognitive dynamics that shape the current strategic environment.

The objective of this study is to analyze the role of hybrid warfare and cognitive operations in contemporary armed conflicts, paying special attention to the interaction between military operations, information campaigns, and the dynamics of the digital ecosystem. To this end, a comparative approach is adopted that examines three particularly relevan n scenarios: the war in Ukraine, the conflict in the Middle East, and the recent military escalation between the United States, Israel, and Iran.

The article is structured into several sections. First, it examines the concept of hybrid warfare and its evolution in contemporary strategic doctrine. Next, it analyzes the development of cognitive operations and their relationship to the militarization of the information environment. Subsequently, three case studies—Ukraine, the Middle East, and the escalation between the United States, Israel, and Iran—are analyzed to identify common patterns in the use of hybrid strategies and influence operations. Finally, the paper addresses the legal, strategic, and economic implications of these dynamics for international security and for the development of international law applicable to armed conflicts.

Through this analysis, the article aims to contribute to the academic debate on the transformation of war in the 21st century and on the growing role of the information domain in strategic competition between states.

Hybrid War and Cognitive Operations: The Militarization of the Information Environment

The concept of hybrid warfare has been widely used in strategic literature to describe conflicts characterized by the integration of different instruments of power. Authors such as Frank Hoffman have noted that hybrid wars combine conventional military capabilities, irregular tactics, terrorism, and information operations within the same strategic

framework. This approach reflects the growing complexity of contemporary conflicts and the blurring of boundaries between war and strategic competition.

Contemporary military doctrine has progressively incorporated this perspective through the concept of multi-domain operations, which recognizes the need to coordinate actions across different operational domains to generate cumulative strategic effects. In this context, the information domain is becoming increasingly relevant. Information operations seek to influence perceptions, legitimize certain military actions, and erode the adversary's political or social cohesion; consequently, disinformation campaigns, the manipulation of digital content, and psychological operations have become common tools of strategic competition among state actors.

One of the most significant doctrinal developments in recent strategic literature is the concept of cognitive operations.

Indeed, these operations aim to directly influence the mental processes through which individuals interpret information and make decisions. Unlike traditional information operations, which focus on the dissemination of content, cognitive operations seek to alter the way audiences process and evaluate available information.

Various studies[1] have emphasized that the cognitive domain constitutes a new arena of strategic competition where cognitive operations may include activities such as: coordinated influence campaigns on social media, algorithmic manipulation of the visibility of certain content, exploitation of cognitive biases in specific audiences, or strategic amplification of polarizing narratives.

The digitization of the information ecosystem has multiplied the potential reach of these operations. Platforms managed by global technology companies such as Meta, X Corp., or TikTok act as critical infrastructure within the global information environment.

From a military perspective, these dynamics have driven the development of doctrines aimed at integrating cognitive domain into strategic planning[2].

---

[1] See, among others, the works of DE ESPONA, RAFAEL JOSÉ **(2023).** *Acción estratégica de la defensa sobre el ámbito cognitivo: los centros de gravedad del ámbito cognitivo*. Boletín IEEE, nº 29, o el Documento de Trabajo IEEE (2020). *Implicaciones del ámbito cognitivo en las operaciones militares*. Instituto Español de Estudios Estratégicos. (Madrid: IEEE-CESEDEN, 2020).

[2] See: NATO Allied Command Transformation. *Cognitive Warfare Concept.* Norfolk: NATO ACT, 2024 o Christoph Deppe y Johannes Schaal. *Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Concept*. Frontiers in Big Data, 2024.

Ukraine: Information Warfare and Digital Mobilization

The war triggered by Russia's invasion of Ukraine constitutes one of the clearest examples of the integration between conventional military operations and information warfare strategies in the 21st century. Since the conflict began, both Russia and Ukraine have deployed complex communication campaigns aimed at influencing national and international perceptions, reinforcing the legitimacy of their respective positions, and undermining political support for the adversary.

Unlike previous conflicts, the information environment of the current war in Ukraine is characterized by intense participation from state actors, digital platforms, and independent analysis communities. The massive dissemination of information through social media, messaging channels, and video platforms has generated a highly dynamic information ecosystem, in which strategic narratives are constructed and contested in real time.

One of the most notable elements of the Ukrainian strategy has been the systematic use of digital communication to mobilize international support. From the first weeks of the conflict, President Volodymyr Zelenskyy adopted a communication strategy based on direct messages disseminated through social media and virtual appearances before foreign parliaments. These interventions—directed at institutions such as the U.S. Congress, the European Parliament, and various national legislative bodies—were widely disseminated on digital platforms, generating a strong impact on international public opinion. This use of digital diplomacy allowed Ukraine to construct a narrative centered on the defense of national sovereignty and democratic values in the face of external aggression.

At the same time, Ukrainian authorities developed information campaigns aimed at bolstering domestic morale and mobilizing support from the civilian population. The dissemination of messages of resistance, along with images of the defense of cities such as Kyiv and Mariupol, helped consolidate a narrative of national resistance in the face of the invasion.

In parallel with these Ukrainian defensive actions, various analyses have pointed to the use of disinformation campaigns by actors linked to Russia with the aim of influencing the

international perception of the conflict[3]. Among the most widespread narratives were claims regarding the alleged illegitimacy of the Ukrainian government, accusations of persecution against Russian-speaking minorities, or alternative interpretations of certain military events. These narratives were disseminated through state media, social media, and digital channels linked to influence campaigns.

One of the best-known cases was the controversy surrounding the so-called "Ghost of Kyiv," a purported Ukrainian fighter pilot credited with multiple shootdowns of Russian aircraft during the early days of the war. Although it was later demonstrated that the story had a significant propaganda component, the episode illustrates how quickly certain narratives can spread in the contemporary information ecosystem[4]. Other notable examples included the circulation on social media of manipulated or out-of-context images and videos, some of which actually originated from previous conflicts. The dissemination of this content caused confusion in the early stages of the conflict and highlighted the difficulties of verifying information in real time.

One of the most innovative features of the war in Ukraine has been the role played by open-source intelligence (OSINT).

Indeed, communities of independent analysts and specialized organizations have used satellite imagery, geospatial data, and audiovisual material available on social media to analyze military developments on the ground. For their part, organizations such as Bellingcat have helped verify attacks on civilian infrastructure, troop movements, and damage caused by military operations[5]. This type of analysis has made it possible to challenge official narratives and provide empirical evidence in debates regarding the conduct of hostilities.

Finally, the use of geolocation and digital analysis tools has also made it possible to reconstruct certain episodes of the conflict, such as the events that took place in the city of Bucha, where the dissemination of satellite images and videos recorded by civilians

[3] See, in this regard: PAUL, Christopher y MATTHEWS, Miriam, *The Russian "Firehose of Falsehood" Propaganda Model* (Santa Monica, CA: RAND Corporation, 2016), GEISSLER, Dominique et al., *Russian Propaganda on Social Media during the 2022 Invasion of Ukraine* **(**EPJ Data Science**,** Volume 12, Article 35 (2023), PIERRI, Francesco et al., *Propaganda and Misinformation on Facebook and Twitter during the Russian Invasion of Ukraine.* (arXiv preprint, 2022).

[4] LAURENCE, Peter. "How Ukraine's 'Ghost of Kyiv' Legendary Pilot Was Born," *BBC News*, May 1, 2022.

[5] HIGGINS, Eliot et al., "Russia's Bucha 'Facts' Versus the Evidence," *Bellingcat*, April 4, 2022; WATERS, Nick y HIGGINS, Eliot, "Russia's Kremenchuk Claims Versus the Evidence," *Bellingcat*, June 29, 2022; STRICK, Benjamin, "Over 500 Days of the Russia-Ukraine Monitor Map," *Bellingcat*, July 24, 2023.

played a significant role in documenting alleged violations of international humanitarian law[6].

On the other hand, digital platforms have played a central role in the conflict's information ecosystem. Technology companies such as Meta, X Corp., and TikTok have adopted various measures to limit the dissemination of certain content linked to disinformation campaigns; among these are the restriction of Russian state media in certain regions, the removal of coordinated networks of fake accounts, and the introduction of informational labels on content related to the conflict.

We must note, however, that these decisions also sparked debates about the role of tech companies in managing the information environment during armed conflicts, as well as the boundaries between content moderation and narrative control.

Thus, while on the one hand the experience of the war in Ukraine demonstrates that control of the information environment can significantly influence the course of an armed conflict—such that the ability to mobilize international support, maintain internal cohesion, and shape global perceptions constitutes a strategic resource of the first order—on the other hand, the conflict has highlighted the growing importance of the cognitive domain as a space for strategic competition. The interaction between military operations, information campaigns, and the dynamics of the digital ecosystem shapes a new type of multi-domain conflict in which the battle for the narrative unfolds in parallel with military operations on the ground.

In this sense, the war in Ukraine can be considered a particularly significant laboratory for the study of information warfare in the 21st century.

The Middle East: Narrative Warfare and the Digital Ecosystem

The conflict between Israel and Palestinian armed organizations—particularly Hamas—in the Gaza Strip constitutes another significant example of the growing centrality of the informational domain in contemporary conflicts. In this scenario, the narrative dimension of the conflict plays a fundamental role in the dispute over the international legitimacy of military operations.

[6] See, for example: BROWNE, Malachy, BOTTI, David y WILLIS, Haley, "Satellite Images Show Bodies Lay in Bucha for Weeks, Despite Russian Claims," *The New York Times*, April 4, 2022.

Unlike the case of Ukraine, where the conflict is primarily framed as an interstate confrontation, the Middle East conflict presents a more complex structure from a communicative standpoint. It involves multiple state and non-state actors, as well as a broad network of international organizations, global media outlets, and digital communities that help shape the information environment.

The speed with which images, videos, and testimonies circulate in the digital ecosystem has profoundly transformed the information dynamics of the conflict. Social media has become one of the main channels through which narratives— —are disseminated regarding military operations, civilian casualties, and the responsibilities of the various actors involved.

One of the most characteristic features of the conflict is the intense narrative dispute over the legitimacy of military operations. Israeli authorities have repeatedly argued that their military operations constitute the exercise of the right to self-defense against armed attacks carried out by organizations such as Hamas. In this narrative, military operations are presented as necessary actions to neutralize military infrastructure, tunnel networks, and rocket launch platforms.

For their part, Palestinian actors and various international organizations have emphasized the humanitarian impact of the conflict and the consequences of military operations on the civilian population in the Gaza Strip. In this context, the dissemination of images of urban destruction, civilian casualties, and damage to essential infrastructure plays a central role in constructing narratives critical of Israeli military actions.

This narrative dispute has a direct impact on the international diplomatic arena. Perceptions regarding the proportionality of military operations, compliance with International Humanitarian Law, or responsibility for specific attacks influence the positions adopted by governments, international organizations, and civil society actors.

As in the previous case, digital platforms have significantly amplified the informational dimension of the conflict and have become fundamental channels for the circulation of related content. During various military escalations in the region, videos recorded by civilians, journalists, or combatants have been widely disseminated on these platforms, including images of bombings, rocket launches, the destruction of buildings, and testimonies from victims.

Although the speed at which this material spreads contributes to strong emotional reactions among international audiences, it also poses significant challenges in terms of verifying and contextualizing the information.

Indeed, various analyses have shown that a significant portion of the content shared on social media during episodes of military escalation consists of manipulated, repurposed, or decontextualized material[7]. Images from previous conflicts or other geographic settings have sometimes circulated as if they were recent events , which has contributed to fueling misperceptions about certain episodes.

In addition to all this, the conflict has been accompanied by digital propaganda campaigns aimed at mobilizing political and social support. Both state actors and armed organizations have used digital platforms to disseminate messages aimed at national and international audiences, such as the communication channels linked to Hamas, which broadcast videos of rocket attacks and propaganda messages designed to reinforce their image as a resistance actor against Israel, and which sought to mobilize support among certain regional audiences and strengthen the organization's legitimacy in specific political contexts.

For their part, Israeli authorities have been developing communication strategies aimed at highlighting the defensive nature of their military operations and emphasizing the risks posed by armed organizations' use of civilian infrastructure—strategies that included the dissemination of images of rocket launches from urban areas or of military infrastructure concealed within civilian settings.

The informational component of the conflict has also been marked by the spread of disinformation. During periods of heightened military escalation, numerous false or manipulated posts circulated on social media attributing attacks or responsibility to one or another party to the conflict. Among the best-known examples are videos from previous

[7] See: Associated Press, "Fact Check: Misinformation About the Israel-Hamas War Is Flooding Social Media," 2023; DUBBERLEY, Sam y JONES, Sophia, "Real or Fake? Verifying Video Evidence in Israel and Palestine," *Human Rights Watch*, October 11, 2023; GILBERT, David, "The Israel-Hamas War Is Drowning X in Disinformation," *Wired*, October, 2023; Reuters Fact Check, "Behind-the-Scenes Footage of a Short Film Falsely Linked to the Gaza War," May 20, 2024.

conflicts that were circulated as if they depicted recent events in Gaza, as well as images generated using digital tools that simulated non-existent attacks or damage[8].

The spread of this content illustrates the difficulty of maintaining effective control over the information environment in conflicts characterized by high media intensity and strong political polarization.

The experience of the conflict in the Middle East demonstrates that the informational dimension can play a decisive role in the evolution of contemporary armed conflicts. The battle for the narrative unfolds in parallel with military operations on the ground and can significantly influence the international perception of the conflict, with the result that the ability to shape perceptions, mobilize audiences, and legitimize certain military actions constitutes a strategic resource of the first order.

The U.S.-Israel-Iran Conflict: Convergence of Conventional and Hybrid Warfare

The recent military escalation between the United States, Israel, and Iran constitutes a particularly significant example of the convergence between hybrid warfare dynamics and higher-intensity military confrontations. Although the conflict continues to evolve, recent events clearly illustrate how the involved actors— —combine conventional military operations, cyber operations, and information strategies within a single strategic framework.

Unlike previous conflicts in the region, this escalation is distinctly multi-domain in nature, with military operations unfolding simultaneously in airspace, the maritime domain, cyberspace, and the information environment. In this context, the narrative dimension of the conflict becomes a central element in legitimizing certain military actions and influencing the international perception of events.

One of the most visible features of the escalation has been the use of precision airstrikes targeting military infrastructure and strategic objectives on Iranian territory, particularly facilities linked to its nuclear program, military command centers, and air defense systems. From a strategic perspective, this type of operation follows a logic of preventive neutralization of strategic capabilities, based on the understanding that the destruction of

[8] See: CHOPRA, Anuj y MCCARTHY, Bill, “War of Narratives: Syrian Imagery Falsely Illustrates Gaza,” *AFP Fact Check*, Dec 29, 2023; Reuters Fact Check, “Behind-the-Scenes Footage of 2022 Short Film Falsely Linked to Gaza War,” May 20, 2024.

radars, anti-aircraft systems, or logistical facilities can help ensure air superiority in later phases of the conflict.

At the same time, these attacks have been accompanied by intense public relations campaigns aimed at justifying their defensive or preemptive nature. Israeli and U.S. authorities have presented these operations as necessary responses to perceived strategic threats, while Iranian authorities—and those of other countries—have denounced them as acts of aggression contrary to international law.

The Iranian response has included various forms of indirect and asymmetric action. Rather than limiting itself to direct military confrontation, Tehran has also relied on networks of allied actors in the region, which have played a significant role in the escalation of the conflict. Among these actors, Hezbollah stands out—an armed organization with a strong presence in southern Lebanon that has been involved in significant exchanges of fire with Israeli forces along Israel's northern border. Such clashes illustrate the regionalized nature of the conflict and the role played by so-called proxy actors in Iran's strategy.

The use of networks of allied actors allows Iran to exert military pressure on Israel and on U.S. interests in the region without necessarily resorting to large-scale direct confrontation; an approach that is part of a broader strategy of projecting regional influence that combines military, political, and communication tools.

Another significant element of the escalation has been the growing tension surrounding control of strategic maritime routes, particularly in the vicinity of the Strait of Hormuz. As is well known, this geographical enclave constitutes one of the world's main energy transport corridors, and its security is of fundamental strategic importance to the global economy. Various recent incidents have included attacks on commercial vessels, naval incidents, and threats to disrupt maritime traffic in the region[9]. Such actions are part of strategies aimed at exerting economic and geopolitical pressure by disrupting critical trade routes.

[9] See: Reuters, "Malta-Flagged Container Ship Hit by Projectile Near the Strait of Hormuz," March 4, 2026; Reuters, "Iran Conflict Disrupts Global Shipping as Tankers Are Stranded or Damaged," March 3, 2026; Reuters, "Iran Vows to Attack Any Ship Trying to Pass Through the Strait of Hormuz," March 2, 2026.

From the perspective of hybrid warfare, the exploitation of economic and energy infrastructure constitutes an effective mechanism for amplifying the strategic impact of regional conflicts.

The cyber dimension has also gained increasing relevance among the actors involved in the conflict. Various specialized reports have noted an increase in cyberattacks targeting critical infrastructure, media outlets, and government systems in the countries involved[10]. These attacks have included attempts to infiltrate computer networks, digital sabotage campaigns, and operations aimed at spreading manipulated information or propaganda in the digital environment, demonstrating once again how the use of cyberspace as a battlefield highlights the importance of this domain in contemporary conflicts, with the certainty that cyber operations can generate significant strategic effects without necessarily resorting to conventional military force, making them a particularly attractive instrument in contexts of prolonged strategic competition.

For its part, the informational dimension of the conflict has been particularly intense. The various actors involved have launched narrative campaigns aimed at influencing the international perception of events.

Thus, Iranian authorities have portrayed the attacks they suffered as external aggression threatening regional stability, while the governments of Israel and the United States have defended the preventive or defensive nature of their military operations.

These narratives, disseminated through traditional media, social media, and diplomatic channels, have sparked intense international debate over the legality and legitimacy of the military operations, causing the narrative battle to unfold in parallel with these operations and creating a highly polarized informational environment in which different actors attempt to shape global perceptions of the conflict.

Legal and Strategic Implications: From "Multidomain Conflict" to Global Systemic Impact

The rise of hybrid warfare and cognitive dominance in contemporary armed conflicts has implications that extend beyond the strictly military realm. In scenarios such as Ukraine

[10] See: Reuters, "U.S. Banks on High Alert for Cyberattacks as Iran War Escalates," March 3, 2026; Reuters, "Hackers Hit Iranian Apps and Websites After U.S.–Israeli Strikes," March 1st, 2026; SC Media, "Cyber Operations Escalated by Iran Following U.S.–Israel Attacks," 2026.

and the Middle East, and particularly evident in the ongoing escalation between the U.S., Israel, and Iran, the interaction between kinetic operations, cyber , economic coercion, and information warfare is shaping a pattern of multi-domain conflict with strategic and legal implications of global scope.

The U.S.–Israel–Iran conflict features a combination of precision strikes, maritime tension, and cyber risk, with a classic strategic objective: to degrade the adversary's capabilities and influence its decision-making, significantly intensifying military actions that expand the operational theater (including a high-impact naval incident and the interception of a missile with implications for NATO)[11].

A structural feature of the Middle East—and one crucial to hybrid analysis—is the tendency toward expansion across theaters: main front + secondary fronts (Lebanon/Hezbollah, Gulf, Red Sea) and pressure on regional partners, alluding to the spread of the conflict and its destabilizing regional effect[12].

From a doctrinal standpoint, this fits into strategies of deterrence through punishment and denial, but also into "gray zone" logic, in which the aim is to maintain ambiguity and modulate response thresholds.

In the ongoing conflict, the Strait of Hormuz functions as global strategic infrastructure: it is not merely a maritime space but a multiplier of economic effects. Journalistic and market sources describe severe disruptions to traffic and the resulting strain on prices, insurance, alternative routes, and energy policy decisions in third countries (for example, the search for alternative supply routes).

Finally, in escalating environments, cyberactivity increases friction: it raises doubts about system integrity, service continuity, and the credibility of information. Recent "threat intelligence" reports warn of increased cyber risk associated with the conflict with Iran[13].

Comparative experience (Ukraine / Middle East) suggests that polarizing foreign audiences is a useful objective: it erodes social cohesion, increases the political cost of supporting one side, and fragments international consensus. The European conceptual framework of FIMI (Foreign Information Manipulation and Interference) is useful here

[11] See: Reuters, "US sinks Iranian warship far from Gulf, NATO downs Iranian missile heading for Turkey", March 4, 2026.
[12] See: Reuters, "Middle East conflict widens as Israeli, US strikes again hit Iran; oil soars, shares slide", March 3, 2026.
[13] See: UNIT42, "Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran", March 2, 2026

because it describes patterns of coordinated information manipulation, often by state actors or proxies, that seek to influence political processes and democratic values[14].

Regarding the economic implications, the most direct channel is energy: the Strait of Hormuz is a "choke point," and when transit is disrupted or halted, it triggers effects on prices, markets, and expectations. Coverage of transit disruptions, falling exports, and the response of importing states illustrates the almost instantaneous transmission to the international economy. Furthermore, in maritime conflicts, insurance serves as a barometer. When insurers withdraw or raise the cost of coverage, the shock is amplified: fewer ships, higher costs, longer transit times, and indirect inflationary pressure. The crisis described around the Strait of Hormuz incorporates precisely these elements.

On the other hand, we must not forget the asymmetric impact on third countries. Indeed, states highly dependent on energy imports (or with concentrated supply routes) suffer disproportionate impacts and seek alternative diplomatic/logistical solutions.

Finally, regarding the legal implications, in escalations such as the current one, the legal debate quickly shifts to (i) whether there was an "armed attack" or a sufficient imminent threat to invoke self-defense, (ii) how necessity and proportionality are assessed in preventive/preemptive operations, and (iii) the role of attribution when harm stems from proxies or non-kinetic operations.

As is well known, once an armed conflict has broken out, IHL imposes classic obligations (distinction, proportionality, and precautions) that are strained by two factors: the use of dual-use infrastructure (civilian-military), and media and operational pressure to "prove" conduct to global audiences.

In this sense, the information environment influences the conduct of hostilities because it increases the operational value of perception and legitimization.

In a conflict such as that between the U.S., Israel, and Iran, where there are signs of escalating cyber risk, the key legal problem is twofold: attribution (technical and political), and the characterization of the damage (does it amount to the use of force? Does it permit countermeasures? does it enable self-defense?), especially given that much of transnational information manipulation operates in a "mostly non-illegal" zone (in EEAS

[14] European Union External Action. *2nd EEAS Report on Foreign Information Manipulation and Interference Threats*. (2024)

terminology[15]) where the response is not classical criminal law but rather resilience, transparency, platform governance, and coordinated strategic response. Furthermore, from a military doctrinal perspective, the conceptualization of "cognitive warfare" within the NATO framework helps justify why this matters operationally (not just communicatively).

Given all of the above, and based on the comparative pattern of Ukraine–Middle East–U.S./Israel/Iran, we can put forward a robust thesis: contemporary conflict tends to be multi-domain and systemic, and its "center of gravity" can shift from the physical battlefield to critical infrastructure, the energy market, social cohesion, and international legitimacy—all mediated by the digital ecosystem.

Conclusiones

The comparative analysis of recent conflicts—from the Russian invasion of Ukraine to the dynamics of confrontation in the Middle East and the escalation between the United States, Israel, and Iran—allows us to draw a series of doctrinal conclusions regarding the evolution of armed conflict in the 21st century.

First, hybrid warfare must be understood as a structural model of conflict and not as an exceptional or transitory category. The cases analyzed show that state actors systematically integrate military, cyber, informational, and economic instruments into a single strategy of confrontation. Conventional military operations remain relevant, but their effectiveness increasingly depends on their integration with actions aimed at influencing the information environment and the strategic perceptions of domestic and international audiences.

Second, the cognitive domain has established itself as a new central arena of strategic competition. Operations aimed at influencing perceptions, narratives, and decision-making processes have become an essential component of contemporary strategic planning. The digitization of the information ecosystem and the expansion of global communication platforms have significantly broadened the scope of these operations, allowing narratives associated with regional conflicts to rapidly project onto the international stage.

[15] European External Action Service.

Third, multi-domain conflicts tend to generate strategic effects that transcend the strictly military sphere. Tensions surrounding critical infrastructure, energy routes, or digital systems show that contemporary wars can produce systemic impacts on the global economy and on international political stability. The recurring crisis surrounding the Strait of Hormuz illustrates how regional conflicts can have direct repercussions on energy markets, trade routes, and global geopolitical dynamics.

Finally, the transformations in armed conflict pose significant challenges to the existing international legal framework. International Humanitarian Law and the rules governing the use of force were primarily designed to regulate conventional military confrontations between states. However, the growing importance of cyber operations, disinformation campaigns, and cognitive operations raises questions about the applicability and adequacy of current regulatory frameworks.

In this context, the study of hybrid warfare and the cognitive domain should not be viewed solely as an analytical or doctrinal issue. Rather, it constitutes a fundamental element for understanding the evolution of global strategic competition and for designing security policies capable of responding to the emerging challenges of conflict in the 21st century.

*Carlos Galán Cordero**
Director of the Master's Program in Intelligence Analysis and Cyber Intelligence
Nebrija University