Spanish Approach to Cognitive Warfare

Ignacio Nieto
Head of Strategic Conduct of Operations
Joint Staff
SPAIN

iniefer@fn.mde.es

ABSTRACT

This document argues for the growing interest in cognitive warfare on the international stage and emphasizes the need for the Spanish Armed Forces to develop capabilities in this field. Cognitive warfare encompasses various cognitive operations with the goal of controlling the adversary's mind, perceptions, and actions. It is increasingly considered a viable alternative to employing force or diplomacy to achieve strategic objectives. Revisionist nations employ cognitive tools, primarily targeting the three pillars of Clausewitz's trinity – people, armed forces, and government – through the information environment to attain their goals.

The document also underscores that the conventional boundary between peace and war has become increasingly blurred. This blurring complicates the development of graduated responses and the accurate identification of the conflict's end state using traditional notions of victory and defeat. While there isn't a specific legal framework governing actions in the cognitive domain, the general rules within the national and international legal frameworks of the Armed Forces apply to operations in this domain. Rules governing the use of force are particularly relevant, as they directly impact the credibility and legitimacy of operations, consequently affecting the desired support.

Understanding the operational art is crucial to grasp the intricacies of employing the military instrument in the cognitive domain. The joint function represents a cluster of interconnected capabilities and activities organized to enable the commander to integrate, synchronize, and direct them in the planning and execution of operations, including those of a cognitive nature. The primary objective is to prevent adversaries from influencing the three pillars of the decision-making process within Clausewitz's trinity.

In recent years, the international community has witnessed a growing interest in cognitive warfare, a trend accelerated by significant events such as the COVID pandemic and BREXIT. These events have heightened the attention of Western countries to this phenomenon. However, it's crucial to question whether this concept represents something genuinely new or is merely an innovative approach employed by revisionist countries to challenge the military power of Western nations. One cannot ignore the stark contrast in military budgets between countries upholding the existing international order and the revisionist countries that seek a substantial transformation of that order.

What remains beyond doubt is the substantial impact of technology on narrowing the military power gap, particularly through advancements in fields like neuroscience. For revisionist countries, the 21st Century has witnessed unprecedented and exponential technological growth, including innovations that can be applied to the battlefield. These advances are reshaping how states exert influence, employ coercion, subvert adversaries, and wage war. They have also democratized access to global means of influence, making them available to non-state actors and even individuals.

Revisionist countries are acutely aware of the traditional military superiority held by Western nations in terms of military capabilities. This awareness has compelled them to explore alternative means to achieve their strategic objectives. Cognitive warfare has emerged as the preferred arena for confronting Western

international supremacy. Cognitive warfare involves a series of cognitive operations aimed at influencing the adversary's mindset, perceptions, and actions, extending into the political sphere. It has become an increasingly viable alternative to employing traditional force or diplomatic strategies to achieve strategic goals.

When analysing the contemporary global conflicts, one quickly realizes that the traditional binary notions of war and peace are evolving into a new paradigm (Jarrod, 2020). The current conflict environment no longer aligns with these simplistic categories. In the past, war was waged more straightforwardly within traditional domains – land, maritime, and air. However, the modern battlefield is considerably more complex. While operational commanders traditionally exercised authority over tactical levels, relying on the operational art, the blurred boundaries between peace and war have rendered it challenging to devise graduated responses or pinpoint the end state of conflicts using conventional concepts of victory and defeat.

The demarcation lines separating external and internal security realms have also blurred. In this uncharted territory, low-profile adversaries coexist with ever-evolving risks and threats. Their primary instrument in this dynamic environment is the cognitive domain. In this context, revisionist countries often opt for non-kinetic subversion over kinetic coercion and exploit the lack of international governance or soft stances. Hybrid strategies have become the hallmark of these countries' approaches. A distinctive feature of the hybrid threat is its ability to pursue objectives while staying below the threshold that would trigger open conflict and the ensuing military escalation. We must understand that there is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder the decision-making processes, these hybrid threats influence and exploit vulnerabilities to incur damage below the threshold of overt aggression.

Despite the current security environment, the nature of warfare did not change in its basis at all, and it is still driven by the capstone of the Clausewitzian theory: the so-called trinity of war. Clausewitz´s trinity is comprised by three specific elements, simply put, it is about people, armed forces, and government.

- Primordial violence, hatred, and enmity, which are to be regarded as a blind natural force. This mainly concerns the people.
- Play of chance and probability within which the creative spirit is free to roam. This represents the armed forces.
- Element of subordination, as an instrument of policy, which makes it subject to reason alone. This is the third one and represents the government. (Mattox, 2008).

The Westphalian system is a principle settled in international law that states that each state has exclusive sovereignty over its territory. Everything inside the territory is directed by the state (Weatherall, 2022). Therefore, the three tendencies incarnated by Clausewitz, people, military, and government, are handled by the politicians or the governments.

The information age changed some of these rules and introduced the chance of making modifications that might materially affect the balance among the three tendencies established by the Clausewitz trinity, people, armed forces, and governments. In this current battlefield, external actors can exert influence in our societies and govern their desires and preferences. Modelling the information space makes the audiences vulnerable, notably in open and democratic spaces and countries. It is even possible to change the common opinion of the people.

It is well known that one of the factors exerting a growing influence in Spanish society is the disinformation phenomena. Disinformation erodes trust in institutions and can be part of hybrid threats not only in internal security but also external secutiry and one of the best examples is Mali. The people element is, therefore, in danger since the spread of disinformation also affects the policy-making processes by skewing public opinion.

Open and democratic societies are vulnerable to disinformation and can also attack everyone's personal cognition. External influence disrupts ordinary understandings and drives the people to believe in false information producing harmful effects over time. This is also true when it comes to the second pillar of the trinity, the armed forces. In current battlefields a panoply of different actors come together, which are subject to the ubiquity of information; an information which they generate but also receive from a multiplicity of sources and channels, and which can condition their perceptions by modelling the reality itself, both armed forces and people. Clausewitz repeatedly emphasized the importance of moral factors as well as the mental, including emotional, life of the commander in war (Milevski, 2020).

This also applies when it comes to the main political decision makers that are subject to the people´s approach to the conflicts. The adversary or competitor's decision-making processes can be altered through specific actions in the cognitive domain that change their perceptions or emotions without having to act on reality; they can also be modified through actions in other domains that, acting upon the real-life, achieve the same effects.

Revisionist powers have fundamentally rejected the geopolitical settlement that emerged in the aftermath of the Cold War. Instead, they have meticulously studied and adapted military strategies, employing innovative tools to mount increasingly assertive challenges to the established international order. It's worth noting that these nations, while challenging the existing order, also find ways to derive benefits from it, employing military power in unconventional ways.

The military's role within a state's actions is manifested through the government's utilization of the military instrument. This utilization occurs both in the broader realm of security and in the more specific domain of defence. Typically, these objectives are achieved through a series of operations. This concept is straightforward when dealing with traditional military domains. However, applying this notion to the cognitive domain proves far more intricate.

Understanding the complexity of employing the military instrument in the cognitive domain necessitates a grasp of operational art. The effectiveness of the military instrument depends on operational art and the application of critical and creative thinking. These tools are employed to harness both military and civilian capabilities and leverage them to achieve strategic and operational objectives. Operational art involves the design, organization, integration, and execution of campaigns and operations. It enables the resolution of multifaceted operational challenges, often characterized by their multidisciplinary and unstructured nature, within a dynamic and evolving environment. Operational art provides the framework that offers coherence, clarity, and a logical approach to addressing these intricate issues. In essence, operational art is linked to military capabilities and runs the business within the operational level. Operational art resorts to joint function to be effective. The joint function is the cluster of related capabilities and activities grouped together that allow the commander to integrate, synchronize and direct them during the planning and execution of operations.

Knowing that, the military capabilities must evolve to the pace of operational requirements. To adapt constantly, and even anticipate changes in the current operational environment (uncertain, global, and changing) the Armed Forces must maintain an attitude of continuous innovation and Spanish armed forces have taken the approach to build up capabilities in the cognitive domain.

Unfortunately, there is no specific legal framework to regulate actions in the cognitive domain, we are working on that, both at national and international level. However, this does not mean that there are no applicable regulations since the general rules of the national and international Armed Forces legal frameworks for operations in other domains are also applicable.

In the national context, the Spanish Constitution legitimises the actions of the Armed Forces to guarantee the sovereignty and independence of Spain and to defend its territorial integrity and the constitutional order.

Likewise, the Armed Forces, together with the national law Enforcement Forces, have the mission to protect the free exercise of rights and liberties and guarantee citizen security. Some of them are especially related to the cognitive domain, such as the right to privacy, the secrecy of communications, the freedom of expression or the protection of personal data, to name a few. Military actions in the cognitive domain are - to all intents and purposes - within this sphere of law.

As for the legal factors, the rules governing the use of force are particularly relevant since they can directly affect the credibility and legitimacy of operations and, consequently, the desirable support. This factor has turned into a vulnerability for western countries since the military are not used to fighting in these environments and the legal statecraft is not yet well defined. It becomes of paramount importance that every action of the Armed Forces and the conditions in which their operations are performed abide by the legal framework to ensure the lawfulness and legitimacy of their employment. We should not assume that the adversary will behave in the same way, though.

In summary, Spain recognizes the cognitive domain in its doctrine and procedures. And, recently, the Chief of Defence of Spain has approved the Spanish Concept to act in the Cognitive Domain. In this regard, the cognitive domain is an intangible environment inherent to the human being –considered in an individual, social, or organizationally manner– and to its judgement and ability to make decisions. Decision making process is key to understand the Spanish approach to cognitive domain.

This domain encompasses the will of every person involved in the conflict and every artificial intelligence system, thus permeating all other domains. Its main drawback is that it implies several intangible aspects difficult to appraise like values, perceptions, conscience, attitudes, and prejudices. This domain permits the Armed Forces to achieve goals, not feasible in other domains, through the employment of communication techniques, psychology, and other social sciences.

But cognitive warfare is not just another name for information warfare. As Spain understands cognitive warfare, it is a war on our individual processor, the brain. Currently, there is no agreement on the scope and implications of what is understood by cognitive operating domain, which directly points to human reasoning and emotions as the potential target of aggression in the context of a confrontation. Nowadays it is commonly accepted that the cognitive domain brings a major combat dimension to the modern battlefield and creates a new space of competition, beyond the land, maritime, air, cyber and space domains. Its field of action not only brings to the space of the battlefield the information environment but also the control of ideas, psychology, especially behavioural and thoughts.

This new domain of operations seeps into human belief systems, emotions, and motivation, and affects people's behaviour, impacting the effects on other domains, which highlights its cross-cutting nature. It is an operating domain, which permeates by its very nature operations in the three physical domains - land, maritime and aerospace - and the other non-physical domain, i.e., cyberspace. In this sense, the cognitive domain is closely related to the cyberspace domain, since cyberspace is the priority vector by which information from all domains is transmitted (emitted and received), and by which the message is sent towards different audiences.

From an operations point of view, the decision-making processes generated during the Joint Force operation, both in the chain of command and at individual or group level, are the main element of reference in the cognitive domain, the first and second pillar of the trinity. These are processes in which a decision maker chooses between two or more options, in each context and situation, based on information and knowledge that are considered unbiased, as well as on his own emotional factors.

Considering the above, our own decision-making processes shall be considered as an element of special protection, bearing in mind the threats and risks to which they are exposed. This protection, together with the

actions taken to disrupt the adversaries' and competitors' decision-making processes, will help to achieve the long-pursued goal of decision superiority. We are again referring to influence in the elements of the trinity.

By undertaking actions to reduce threats, but also the vulnerability of the Joint Force to their potential impact, it will be possible to reduce the spin-off effects, or in other words, the probability that the decision-making processes are altered by influence. This is the main goal of Spanish armed forces for the cognitive domain; to protect the decision-making process from external information activities driven by the adversary and at the same time, be able to influence the adversary decision making process to achieve the strategic goals.

REFERENCES

[1] Brook, J. (2020). Clausewitz, the Trinity, and the Utility of Hybrid War. thestrategybridge.org. Available at: https://thestrategybridge.org/the-bridge/2020/9/15/clausewitz-the-trinity-and-the-utility-of-hybrid-war

[2] Chan, S. (2021). Challenging the liberal order: the US hegemon as a revisionist power. International Affairs, 97(5), 1335-1352.

[3] Clausewitz, C (1989). On War, trans. Michael Howard and Peter Paret. Princeton: Princeton University Press

[4] Claverie, B., & Du Cluzel, F. (2022). "Cognitive Warfare": The Advent of the Concept of "Cognitics" in the Field of Warfare.

[5] European Commission (2018), "Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the regions- Action Plan against Disinformation", 5 December 2018, Brussels, JOIN(2018) 36 final, available at: https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation

[6] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy (2018), "Joint Communication to the European Parliament, the European Council and the Council- Increasing resilience and bolstering capabilities to address hybrid threats", Brussels, 13 June 2018, JOIN(2018) 16 final, available at: https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering _capabilities_to_address_hybrid_threats.pdf

[7] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy (2016), "Joint Communication to the European Parliament and the Council- Joint Framework on countering hybrid threats- a European Union response", Brussels, 6 April 2016, JOIN(2016) 18 final, p. 1-6.

[8] European Parliament (2019), "Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States", February 2019, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf

[9] Mattox, J.M. (2008), The Clausewitzian Trinity in the Information Age: A Just War Approach, Journal of Military Ethics, 7:3, 202-214. DOI: 10.1080/15027570802277755

[10] Milevski, L. (2020), Battle and its emotional effect in war termination, Comparative Strategy, 39:6, 535-548. DOI: 10.1080/01495933.2020.1826844

[11] Spanish Ministry of Defence. Joint Staff. Concept for the use of the Joint Force in the cognitive domain.

[12] Spanish Ministry of Defence. Joint Staff. Exploratory concept for the Cognitive Domain.

[13] Weatherall, T. (2022). Subjects of Responsibility under International Law. In Duality of Responsibility in International Law (pp. 11-35). Brill Nijhoff.