Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

José M. MARTÍNEZ CORTÉS
PhD in International Security.

Email: jmcpope@hotmail.es

The new operating environment and aerospace operations

Abstract

The strategic context and new risks and threats shape a novel operating environment to which armed forces, and air forces in particular, will need to adapt if they are to maintain their operational capability and effectiveness. The events of war and conflict over the past two decades reveal that advances in technology have radically altered the space of operations and, as a consequence, have affected the application of military power. The traditional way in which military operations are planned and conducted has therefore been clearly affected. In current and future operational scenarios, greater agility, flexibility and adaptability in the way operations are conducted will be required to maintain the strategic advantage that allows [aerospace] operations to be executed with a probability of success.

Keywords

Operating environment, hybrid strategy, multi-domain, operations space, operational agility.

Cite this article:

Martínez Cortés, J. M. (2022). The new operating environment and aerospace operations. *Spanish Institute for Strategic Studies Journal*. No. 20, pp. **415-440.**

Disclaimer: The ideas expressed in this research article are those of the author and do not reflect the official position of the Air and Space Army or the Ministry of Defence.

Conflicts in the Western hemisphere since the end of the Cold War have generally led, at the time they occurred, to a misperception of future conflicts, under the proclamation that technological superiority would be sufficient to defeat any adversary (a clear reference to the first Gulf War and Operation *Allied Force*). However, events in recent years related to different crises or conflicts have been increasingly diluting this initial perception. In addition to a complex and constantly evolving strategic context, with new threats and the influences they have on the operating environment, conflict management is fundamentally a dynamic activity due to the various factors that influence the state and its relations with society, and to the sometimes unpredictable effect of the use of the instruments of state power against an adversary. Therefore, through the synergistic and cross-cutting application of the instruments available to the government (Diplomatic, Information, Military and Economic), the success of the necessary comprehensive strategy for crisis or conflict resolution requires not only a correct knowledge of the context, risks and threats and good political-military coordination, but also an adequate understanding of the nature and evolution of conflicts. Knowledge of these and the implementation of good coordination and synchronisation will not ensure victory, but without them, it will be difficult to implement the instruments of the national strategy effectively.

Therefore, the effort of foresight on how to operate in operational environments in the short and medium terms (on an approximate horizon of 2040) must begin with a review of the strategic context and the risks and threats to help us understand how operational environments are shaped and how their characteristics affect the application of military power in what is called the *operational space*[1]. Spain, like other neighbouring nations, needs to define how to confront scenarios, not just conflicts, from the military point of view, in the short and medium terms. In line with some allied countries, all indications are that we need to evolve towards a new way of operating in what we can call a "multi-domain environment", which we will come to in due course. For now, we begin by looking at the current strategic context, the threats and the characteristics of the operational scenarios we can expect.

New strategic context

The world today seems no safer than in the past. Despite there being few conventional conflicts, there is a high level of conflict in the international strategic context (Dacoba, 2021a: 4), and very high levels in 2022 due to the conflict in Ukraine, a context that could be described as complex, dynamic and competitive.

The international panorama is in a continuous evolution which, in recent times, has accelerated and become extremely complex. But today's international context is

1 The space of operations is the portion of the physical and non-physical fields of operation where the instruments of power, particularly the military instrument, operate, actions are executed, engagements take place, and effects are produced (PDC-01A).

not only complex but also very demanding (Fojón, 2021: 3), a product both of its own complexity and of the difficulty of the different state actors to find the right place on the international "chessboard". These actors are suffering from the effects of strategic competition between the US and China and the growing pressure exerted by Russia in its quest to remain a major player which just because it is well known is no less dangerous, as current events reflect. They also face new challenges, such as the rise of China in various respects, the US administration's shift in focus towards Asia-Pacific and energy insecurity, not to mention the increasingly damaging effect on the world's population of the use of information for malicious purposes.

In an X-ray of this panorama, the following aspects can be highlighted by way of summary, defining its main characteristics:

– *Evolution to a new balance of power*. With the rise of China as a new economic and technological power with growing military capability, and with almost constant pressure from Russia in its quest to remain a major player, in many aspects the world is evolving from the unipolarity and hegemony of the US in the late 20th and early 21st centuries to a multipolarity of aggressive competition. This strategic competition drags the rest of the middle and small powers into a dynamic of growing tensions in all areas (Dacoba, 2021b: 4).

– A *struggle for hegemony and influence at the international level* with several new actors and one crucial one, China, in strong competition with the US. China's progress in different areas is worrying since official confirmation of a test of Chinese hypersonic weapons in October 2021 (due to the difficulty of detection and interception) and the development of artificial intelligence, which is of great interest to the Chinese military establishment. Both aspects are described as very worrying by the US authorities[2].

– *Increased access to technology coexisting with asymmetry in capabilities* between different actors (Operating Environment 2035, MINISDEF, 2019: 36). In recent years, there has been a proliferation of non-state actors who, although they have the capacity to access new technology, do not have the possibility or prefer not to engage in conventional confrontation with major state actors, a strategy also used by some revisionist powers. This has led to a huge increase in the use of new, so-called "non-physical" domains, which allow attempts to circumvent this asymmetry in technology and capabilities through the use of non-conventional methods. Authoritarian regimes find an ideal terrain for employing, in an unattributable way, these unconventional tools, which is one of the reasons why such regimes have proliferated (Dacoba, 2021a: 3).

2 https://www.reuters.com/business/aerospace-defense/top-us-general-confirms-very-concerning-chinese-hypersonic-weapons-test-2021-10-27/

https://www.elconfidencial.com/tecnologia/2021-11-14/eeuu-china-inteligencia-artificial-tecnologia-militar_3323119/

– All the above justifies that in the 21ST century there is a perception of *widespread and intense conflict*. The 2021 edition of the Stockholm International Peace Research Institute's (SIPRI) conflict report notes that, after a pronounced deterioration in global stability and security over the last decade to 2020, there is a mixed picture on overall trends. It highlights growing military spending, an increase in the number of armed conflicts (although the total number of casualties decreased, possibly due to the end of the Syrian conflict), and a balance between potential escalation and containment in most hotspots on a geopolitical chessboard with numerous regional rivalries.

  This conflictivity is not only identified with the existence of traditional conflicts, but also, and to an increasing extent, with non-war scenarios, included in what is known as the "grey zone", where the adversary seeks to achieve its strategic objectives without exceeding our response threshold, and where there is therefore no fully fledged or traditional conflict.

– Globalisation and new technologies have also led to the greater interdependence of the different actors. What happens in one part of the world has a direct and almost instantaneous influence in parts far away (Panorama of Geopolitical Trends, Horizon 2040, 2nd edition: 115), as evidenced by the effects on different sectors of strategic measures or actions in other areas. This huge interdependence also produces a perception of tension and conflict that is not only generalised but also ongoing, a situation that contributes to the rise of nationalism and populism as a reaction (sometimes negative) to outside influences.

– In addition to the numerous traditional geopolitical disputes and the existence of warlike confrontations (in many cases, with great powers involved through *proxies,* generally non-state, to prevent actions from being attributed), the elements identified above also encourage new forms of competition between great powers, while avoiding head-on confrontation (Dacoba, 2021a).

– Last, technological development and the increasing emergence of disruptive technologies not only take us into a profound technological transformation, but also force us to be part of a world in which change is inexorably occurring at an accelerating pace, as the *Strategic Foresight Analysis report* 2017 (15-16) points out.

Risks and threats

In the strategic context described above, there are classic threats and risks[3], new ones and some that are only intuited, or simply not yet known. Societies in our Western environment strive to achieve the highest degree of security, which in this context

3 Threat is any circumstance that endangers the security or stability of Spain, and risk is the contingency or probability that a threat will materialise and cause harm.

is no easy task, given the complex nature of the challenges we face. In this respect, official and reference documents highlight virtually the same risks and threats, which are broadly summarised in the 2021 National Security Strategy (NSS).

Although the 2021 NSS has retained almost all the challenges and threats from the previous 2017 NSS, with a new naming of risks and threats, it has several significant nuances. First, there are the "*disinformation campaigns*" which find in cyberspace fertile ground for their propagation, targeting people and their perceptions and jeopardising the legitimacy of democratic systems, undermining, moreover, citizens' trust in institutions and social cohesion itself (Dacoba, 2022: 6). Likewise, as common and transversal elements of risks and threats, the NSS underlines technology and the prominence of the use of hybrid strategies, which is increasingly widespread and within the reach of all types of actors, state and non-state. Furthermore, the new NSS stresses the dynamic nature of risks and threats as elements of a continuum that reflect a progressive gradation, which depends on the degree of likelihood and impact because, among other things, the interaction and interconnection between the different domains is much greater than it was previously, as we will see below.

With regard to hybrid strategies, and hybrids in general, it is necessary at this point, from a security perspective, to delve into a brief analysis of the evolution of conflicts over the last two decades, focusing primarily on the concept of hybrids, which is having such an impact not only on the understanding of conflicts but also on the correct execution of optimal responses to the challenges they pose.

Evolution of conflicts. The concept of the hybrid

Since the beginning of this century, a change seems to be taking place in the characteristics of armed conflicts, but not in their root causes; from the Napoleonic-industrial model to one in which the line between war and peace has become blurred, it is an evolution that makes it very difficult to analyse present and future conflicts from a "war and peace" perspective (Martínez Cortés, 2020: 849).

In this period, much has been written about the concept of "hybrid warfare", a concept that has undergone a certain evolution; since the end of the Cold War, there has been a proliferation of articles related to the concept, provoking intense debate and analysis within the Western community. The aim of both debate and analysis has been none other than to better understand what really happens in the context of armed conflicts regarding their objectives, strategies and the means used by the actors who aspire to a change in the *status quo*.

As far as the concept of hybrid warfare is concerned, the first mention in academia is attributed to Robert G. Walker, who used it in his graduate thesis (Walker, 1998). Drawing on the *Fleet Marine Force Manual Warfighting*, Walker argues that 21st century warfare will be characterised by an intimate mix of conventional and special actions. In this regard, we must recall three relevant elements of reference. First, it was not until the publication of the article "*The War of the Future: The Coming of Hybrid*

Conflict", written in November 2005 by the then US Secretary of Defence, Lieutenant General James N. Mattis, together with Lieutenant Colonel Frank G. Hoffman, that it was given theoretical content. Second, it was in the 2006 conflict between Israel and *Hezbollah* that its first major practical manifestation seemed to take place. And third, it was the presentation of Hoffman's 2007 essay "*Conflict in the 21ST Century: The Beginning of Hybrid Warfare*" that popularised this idea in the defence community. Nevertheless, and notwithstanding these contributions, the main contributions of the leading exponent of hybrid warfare, Frank G. Hoffman, were at their most productive in the last years of the first decade of the 21ST century, when in 2009 he published several articles on the subject. In this regard, given the good reception that Hoffman's approach received from the outset, it is still a paradigm that has been much cited, worked on and in constant evolution.

But why is this concept so well received by experts? In Baqués' opinion, much of the blame lies with the difficulties the US encountered in taking control of Afghanistan and Iraq after the initial success of their respective interventions in 2001 and 2003; far from stabilising both scenarios, the situation deteriorated. The US's heavy investment in the most sophisticated weapons systems did not help much, nor did its huge defence spending. Hoffman notes that without a new paradigm adapted to post-9/11 realities, lethal operations on the ground would be doomed to failure (Hoffman, 2009a: 1).

The enemy the Western troops encountered did not correspond to the idea of a conventional army - well trained and equipped with the doctrines needed to carry out combat missions - while its funding was, at best, precarious and unstable. Furthermore, non-state armed actors of different kinds were appearing everywhere, generating synergies unfriendly to the US (local militias, often equipped with new communication technologies, collective weapons and even heavy weapons, which were rarely available to the old guerrillas of centuries ago; organised crime linked to illicit trafficking, also equipped with long arms and sometimes rocket launchers and grenades; terrorist groups, etc.). This fact made it necessary to review bibliographies and newspaper archives, and to dust off the lessons learned in long-ago conflicts such as Vietnam, to determine whether we were dealing with an insurgency or whether what was emerging was really something new. In turn, Western concern about what was happening in Afghanistan and Iraq was significantly heightened following the confrontation in southern Lebanon in the summer of 2006 between Israel and Hezbollah. At that time, Israel, with one of the most advanced armed forces in the world at all levels (technologically, but also doctrinally, and even in terms of combat motivation), was unable to defeat an enemy that neither responded exclusively to the logic of conventional armed forces nor simply acted as a guerrilla force.

Events in Afghanistan, Iraq and southern Lebanon highlighted several weaknesses of Western powers. Beyond the spectacular data in military balance sheets about their supposed superiority, the best-endowed states on the planet were incapable of winning wars that seemed —at least a priori— minor, but things had certainly taken a turn for the worse precisely when those responsible for Western strategic planning least expected it (Baqués, 2021a, 82). But what had the antagonists of the major powers

done right to create this situation? Fundamentally, knowing and understanding the adversary, a major priority, although less commonly put into practice than may seem (on many occasions due to overconfidence or complacency), but which in fact should be the sine qua non condition for facing any war adventure, as Sun Tzu expressed in his famous essay on "The Art of War" (2013: 11).

> "If you know others and know yourself, you will not be in danger in 100 battles; if you do not know others but know yourself, you will lose one battle and win another; if you do not know others and do not know yourself, you will be in danger in every battle".

Among other things, opponents had noted that the change in values in Western societies had led them to embrace the "doctrine of the low 0s", and that the most important issues for citizens were now related to "quality of life" and "well-being", thus displacing other concerns that require greater effort or greater capacity for sacrifice. What resulted was a scenario where, as the wars generated more dead and wounded, more expenditure that failed to be spent on welfare policies and greater scepticism among the citizenry, the desires of Western political leaders to seek a graceful exit -which might include the withdrawal of their troops, operating as a servitude that would especially affect the capacity of those same Western powers to use force - would increase in proportion (*op. cit.*, p. 3. *Cit.*, 82).

Meanwhile, this reality encouraged new rivals to develop strategies that could put some of the world's most powerful states in the position of having to deal with disagreements in their own territory. Hybrid warfare would, after all, be one of the best ways to achieve this impact. For this set of reasons, the aim of those who advocate this type of conflict is to prolong the confrontation until it becomes unbearable by the standards of the most advanced societies. Above all, the new rivals sought to prevent the Western powers from concentrating large numbers of troops and firepower on the enemy, precisely to seek a rapid resolution of the conflict. In short, the aim was to prevent them from being able to implement the "American way of waging war", which consisted of overwhelming the adversary based on their military superiority (Calvo, 2011: 10).

However, regardless of the terminology used, as Baqués expresses, part of the analysis carried out in this respect is shared by different authors, in the sense that conventional wars between states are becoming less numerous (Baqués, 2021b: 1). Likewise, in this context, the role of state and non-state actors is increasing who, avoiding direct confrontation, employ a [hybrid] strategy based on the use of a combination of conventional and non-conventional techniques and/or tactics of high or low intensity, to exploit our vulnerabilities. These types of adversaries have increased the use of the domains whose effects are more difficult to attribute, the non-physical domains (cyberspace and cognitive)[4], thereby avoiding direct confrontation and possible

4 According to the Joint Doctrine for the Employment of the Armed Forces (PDC-01), there are three physical domains (land, maritime and aerospace) and two non-physical domains (cyberspace

denunciation by the international community (Colom, 2018: 39-43). Moreover, in the strategic context defined, the growing technological gap between countries, together with greater accessibility to certain types of technology with the existence of effective weapons systems and the possibility of using other spheres of action, encourages non-traditional confrontations by a greater number of actors or revisionist powers, which has led to an increase in the use of so-called hybrid or hybrid strategies.

For its part, the objective of this type of strategy is to increase its strategic options (Martínez Cortés, *op. cit.*: 851) in an unconventional and unexpected way to improve, in the case of the revisionist powers, their position in international relations. Thus, when a state actor does not possess sufficient resources to win a conventional war, it may use civilian means to a greater extent, developing a hybrid strategy that seeks to undermine the adversary's order and security system by circumventing the rules of the international system. The application of ambiguous and comprehensive strategies (with increased use of civilian and non-conventional means) is the modus operandi of this type of [hybrid] threat. In this regard, to achieve their objectives, we can expect hybrid strategy actions of all kinds, especially unconventional ones, either in open conflict or without the need to initiate one, which can seriously affect our environments, in particular the cyberspace and cognitive domains, as well as the space environment (including in the aerospace domain) and the electromagnetic spectrum, all of which are very demanding in terms of employment and need for protection.

However, we must be aware that the combination of the conventional and the irregular, what is known today as "hybrid", is nothing new (Martínez Cortés, *op. cit.*: 851). The use of a combination of conventional and irregular means in conflict is as old as the history of conflict itself. A classic war of this type is the Peloponnesian War. According to Victor Davis Hanson, as a result of the events of the Peloponnesian War (in which Athens was a naval power and Sparta a land power), it was not a war in which direct battles were the regular form of fighting but rather a war fought by unconventional means (Arauz, 2013: 61-62). Moreover, the use of all necessary means at one's disposal (military and non-military) to achieve one's stated objectives is also as old as war itself, and therefore this type of warfare, distinct from conventional warfare, is also as old as humanity itself. More than 2,500 years ago, the great Chinese strategist *Sun Tzu* wrote in his famous text "The Art of War" about the optimal expression of the strategy of "*defeating the adversary without having to face him on* the battlefield, through *spies and information management*".

The point being that hybrid warfare is not an "invention" of the late 20th century; it has always existed. So, why is there so much talk about it now, where is the real novelty in it? This question has to do with the fact that, in our times, there is a proliferation of wars that do not reach the threshold of convention (Baqués, 2021b: 2). In part, this is because some of the new technologies, those related to information, communication and artificial intelligence, can be leveraged by non-state actors to greatly increase their

and cognitive).

chances in the event of conflict against a superior power in conventional forces; systems based on such technologies are no longer the monopoly of the strongest. In addition, many actors realise that pushing for a confrontation against conventional forces at a higher level leads to rapid failure. Thus, whether by state or non-state actors, the use of a hybrid strategy opens up a range of alternative options to being defeated by militarily superior forces.

Thus, from the point of view of the states targeted by the apparent proliferation of (state and non-state) actors of hybrid strategies, what is truly worrying (Martínez Cortés, *op. cit.*: 851) is the ability, based on evolution and new technologies, to "combine and synchronise, innovatively and simultaneously, regular and irregular, military and non-military means and methods (above all, cyberspace and information), and the capacity to switch rapidly between them to create strategic effects. None of its individual components is really new; it is the combination and harmonisation of different actions that achieves a surprising effect and creates ambiguity, making it very difficult to react appropriately".

Last, in line with the need to understand how operating environments are shaped, it is important to avoid analysing what is discussed here (strategic environment or context, risks and threats, and possible adversary actions) solely from a Western perspective, because many of these and other actions, and this *hybrid* way of acting, have been extensively discussed previously in conceptual work outside the West, such as that of Chinese colonels Qiao Liang and Wang Xiangsui in their essay translated into English "*Unrestricted Warfare*" (1999: 122-123). In this essay they say:

> "However, using the combined method, a completely different scenario and situation can be set up: If the attacking party secretly raises large amounts of capital unnoticed by the enemy nation and launches an undetectable attack on its financial markets and then, after causing a financial crisis, installs a computer virus and a pre-programmed computer hack into the opponent's computer system, while also carrying out a network attack so that electricity, traffic management, financial transactions, telephone communications and media networks are completely paralysed, it will cause the enemy nation to fall into social panic, street riots and a political crisis. Eventually, the attack by the army would develop and military means would be used in gradual stages until the enemy was forced to sign a dishonourable peace treaty".

New operating environments

The new strategic context that affects us today (both internationally and in our immediate European environment) and the threats and risks that we now have to face shape, to a large extent, the operational environments in which our Armed Forces (hereinafter, SAF) must operate, considering in this regard the broad spectrum of conflicts from peace, crisis and open conflict. Therefore, what has been discussed so

far has a direct influence on the configuration of these environments, but also, and even more importantly, on the way in which the components of the armed forces, and the air forces in particular, must develop and act within them. It is therefore essential to review the effects that the new strategic context and threats have on the operating environment and, consequently, on the way of operating, but not without first highlighting the most salient characteristics of the new operating environments, of which the following are noteworthy:

a) Technological development and access to new technologies will allow potential adversaries to use non-conventional strategies, with an increased role for non-physical domains and the electromagnetic spectrum, when such adversaries cannot cope with a conventional confrontation. Moreover, based on this development and new technologies, the evolution of future scenarios reveals an increasing interaction and interdependence between the different physical and non-physical domains (Reilly, 2018: 2), which will facilitate synchronised action and the generation of effects by the adversary based on the synergy of its actions (provided it has the capacity to do so). In the new area of operations, a given area may be affected by the effects produced by an adversary in a completely different area. Both aspects, increased use of non-physical domains and domain interaction, have significantly altered the space of operations and the way we work in it.

b) New technologies and the increased use of non-physical domains are accelerating the pace of change and the consequent actions and effects that an adversary can have on our forces, and this in turn is having a major influence on the environments in which we operate. The ability to employ all domains and to carry out simultaneous, coordinated and often covert actions seeks, on the one hand, to hinder our ability to respond by entering our decision-making cycle; and, on the other hand, to operate below our threshold of action.

c) Technological advances will also transform the operational environment, expanding the space of operations and allowing for greater sensorisation of it, of automation of data processing and weapon systems, and of the range and accuracy of weapon systems, as well as logistical simplification. This will require changes in the operational art. In this regard, advances in miniaturisation and nanotechnology will make it easier for organisations, and even isolated individuals, to execute potentially destabilising lethal actions at any level, be it state, regional or international.

d) Combining technological advances with conventional and non-conventional strategies makes it possible to diminish or threaten military asymmetry, using the parts of the conflict spectrum that make it difficult to distinguish between peace and conflict. In summary, it is safe to say that the use of hybrid strategies by multiple actors, both in hybrid conflicts and in the Grey Zone, is here to stay for the long haul.

e) The greater interdependence of actors at the international level as a result of globalisation and new technologies makes states more vulnerable than before

and our vulnerabilities more transparent. In particular, in the information age, immediate access to the necessary information has a direct negative effect on the population, which becomes a target susceptible to being directly affected by adversaries (Operational Environment 2035, MINISDEF, 2019: 61), with often unpredictable effects, through an infinite number of devices and, in particular, through social networks. This effect puts the focus back on the population which, for a long period of time (basically since the end of World War II), has been a mere spectator of warfare, an aspect that forces us to increasingly focus on the cognitive domain. In addition, the civilian population is routinely present and actively interacting with military forces in areas where they are deployed. In the midst of this dynamic, combatants and non-combatants increasingly share a single operational space wherein the latter are often used as real targets.

f) Another important aspect to bear in mind is that the complexity of current scenarios in terms of the interdependence between areas, the difficulty of attribution and persistent volatility, makes it necessary to have greater knowledge and understanding of the threats that affect us or could potentially affect us, which leads to the need for better training and preparation of the personnel available or that will be available in the Armed Forces.

g) Last, based on the described characteristics of the current operational environment, and linked to the interdependence of domains and the adversary's ability to produce cross-domain effects, the new operational environments lead to the need to manoeuvre nimbly among them and the ability to produce cross-domain effects, in a scenario where connectivity becomes a key element for operating in the so-called "*combat cloud*", *a* virtual network in which the "systems of systems" will be interconnected and linked to an interoperable command and control structure (an aspect that will be expanded on later). This reality turns the network, in itself, into a critical capacity (Martínez Cortés, 2019: 158-164), thereby making it necessary to maintain a certain degree of superiority in cyberspace that allows it to be used with the necessary freedom of action.

The new operating environment and effects on the application of military power

The strategic context and the general characteristics of the new operating environments, together with other scenario-specific parameters, shape a new operational space to which it will be necessary to adapt if the SAF is to remain operational and effective. On the basis of what has already been analysed, we can affirm that the events of war and conflict in recent decades show that advances in technology have radically altered the current space of operations; and that this has had its effects on the application of military power (which we will address below) and, therefore, on the way of operating in many different aspects (also addressed below).

The high availability of non-physical domains, coupled with the sophistication of new weapon systems and the ability of the adversary to create A2/AD areas[5], may also make the achievement of [traditional] domain superiority more difficult in general terms and may not be as straightforward as in past operations[6]. In addition to having capabilities to penetrate A2AD systems where necessary, success may depend on access in a single domain that allows actions in other domains to be combined to seek new ways of producing effects (Reilly, *op. cit.*: 3). This does not mean that it is no longer necessary to fight to achieve and maintain air superiority, because it will be; however, there will be occasions when scenarios will have to be adapted to produce effects, through domains other than the traditional one, even as a matter of priority.

A widely argued point in recent years, especially in US forums, is that easy access to technology, together with an increase in highly sophisticated weapon systems (incorporating hypersonic speed) and the use of other domains of operation by potential adversaries, probably make current operational scenarios more competitive and may break the [Western] paradigm of easily achieving superiority in physical domains. The evolution to "contested and/or degraded environments", where the adversary has the ability to limit or deny our forces access and manoeuvrability through A2/AD capability (contested environment), and to disrupt or degrade our command-and-control networks and systems (degraded environment), will also increase our need for adaptation and resilience, or the ability to adapt and recover from a disruptive agent or adverse state or situation (PDC-01A: 30). This is because in complex operating environments, the adversary will most likely degrade, to varying degrees, our ability to act.

Third, the existence of a complex "*continuum of interrelated domains*", with non-physical domains and the electromagnetic spectrum playing a major role, may render ineffective the use of traditional strategies to achieve superiority in the aerospace, land and maritime domains, necessitating the use of non-traditional strategies (Reilly, *op. cit.*: 3-4). This does not mean that achieving superiority in these domains is not essential, because it probably will be, but that achieving this superiority will most likely not be sufficient since other actions in other domains may have a significant first or second order effect, or even cascading effects, which will also be very difficult to predict (Reilly, *op. cit.*: 3). This will make the ability to operate in the different domains much more uncertain. What is at stake here is not a step forward from coordinated joint action, but a very significant shift towards truly integrated joint action.

Furthermore, because of the harmful effects of potential adversaries and, in particular, the close linkage of cyberspace with traditional instruments of military power, special attention should be paid to non-physical domains. Moreover, the

5 A2/AD capability (anti-access/area denial). Ability of a potential adversary to hinder access to an area of operations and prevent/hinder own movement and action within it.

6 (The) French Joint Vision of Multi-domain, Joint Concept JC-0.1.1_M2MC, French Joint Centre for Concepts, Doctrine and Experimentation (2021, 18).

increasing interdependence and interaction between physical and non-physical domains and the consequent ability of the adversary to use different domains in a rapid and synchronised manner to create cross-domain effects will not only require us to change our mindset at all levels of action, but also to operate in a more agile, flexible and interoperable manner and, even more importantly, to operate in a networked and synchronised manner. This is because it will be the only way to possess cross-domain agility to deal with the various actions and dilemmas we will be subjected to by the actions of the adversary (in line with Operating Environment 2035, 2019: 76-78). This greater agility will also be imposed by the acceleration of the pace of battle and of the changes that have taken place, which require planning, decision-making and execution cycles that are more compressed than those to which we are accustomed.

The general characteristics and effects on the application of military power outlined above constitute what has come to be known as the "multi-domain environment", *a* concept that should be defined as clearly as possible, primarily because it provides the basis for the way in which the new operational spaces must be addressed. In general terms, as set out in *Basic Aerospace Doctrine* IG-00-1, Air Force, 2nd Revision (2020: 5, 31-32), the multi-domain is envisaged as a "complex environment encompassing the physical (land, maritime and aerospace) and non-physical (cyber and cognitive) domains, as well as the interaction and interdependence between them, which is conceived as a whole for the planning and execution of military operations".

Perhaps the most important aspect of this new "multi-domain" concept is the existing interdependence and capacity for interaction between domains and their integral conception in terms of activities related to the planning and use of military power. However, although this concept is currently fashionable, it is important to be aware that simultaneous manoeuvring in different domains is nothing new (Reilly, *op. cit.*: 2). One of the earliest recorded uses of multiple domains to achieve operational objectives occurred in the 12th century BC when tribes known as the Sea Peoples were attempting to conquer Egypt. Before their invasion attempt, they attacked and destroyed numerous civilisations in coastal areas along the Mediterranean in Anatolia, Cyprus, Syria and Canaan. The Sea Peoples' plan to invade Egypt envisaged a land assault, through southern Lebanon, and a sea attack. The Egyptian Pharaoh Ramses III met and defeated the land assault of the Sea Peoples in southern Lebanon around 1178 BC; however, Egypt was still under threat from a maritime invasion. In 1175 BC, that threat emerged in the vicinity of what some historians believe was the Pelusian branch of the Nile River. The Sea Peoples' ships were technologically superior to those of the Egyptians, and Rameses knew that he could not defeat their fleet on the open sea. He therefore allowed the Sea Peoples to enter the Delta unopposed. Once they were inside the confines of the Delta, Rameses simultaneously attacked the fleet with the Egyptian fleet and with Egyptian archers from land. Unable to manoeuvre to avoid such a trap, Rameses annihilated the Sea Peoples' fleet. In this respect, it is certain that increased access to non-physical domains and growing technological progress in sectors such as cybernetics, directed energy, nanotechnology, robotics, biotechnology and *Bigdata* will drastically increase the complexity of the interrelationships between domains.

Last, technology has also given more actors the ability to challenge the *status quo*, providing them with tools whose harmful effects, consequences and implications are still largely unknown. The very possible degradation of the electromagnetic spectrum and communications, coupled with the increasing use of non-physical domains, may not only make access and freedom of movement of own forces in the operational space more difficult, as mentioned above, but may also force greater independence of tactical commanders in the execution of their missions, thus causing the need for changes to the standard system of command and control of the own forces involved. This is because, even with satellite communications (SATCOM), the capacity to secure communications for a traditional command and control process will not always be available (Priebe, *et. al*, 2019: 49).

Aerospace operations in the new operating environment

The different aspects outlined above on the new operating environments and the consequent effects on the application of military power lead us to the need to evolve towards a new way of operating, an evolution that must go beyond a mere adaptation of procedures. The traditional conduct of joint operations will not be sufficient to cope with the complexity of today's operational scenarios and threats and requires evolution or adaptation in several respects, a point developed further below.

As mentioned above, the only way to possess cross-domain agility to deal with the various actions and dilemmas we will be subjected to by the adversary's actions (in line with Operating Environment 2035, 2019: 76-78) will be to operate in a networked and synchronised manner. This will require adaptation and improvement in what has come to be called "operational agility" (a term already used in reflection and analysis documents such as the Operational Environment 2035), understood as the ability to quickly generate multiple solutions to a given challenge, being able to switch between them, allowing for rapid adaptation to any situation or action by the adversary. It is not so much a matter of responding faster but of generating multiple solutions quickly, with the capacity to saturate the adversary[7]. This operational agility must go hand in hand with greater agility in the decision-making cycle. The standard format established in these processes will not be valid in environments where the interconnection of domains greatly accelerates the speed of events, and this will affect all levels. This forces us to respond and move towards a new model of [multi-domain] operational scenario with a higher degree of interdependence, interaction and synchrony, and with the consequent need for a new model of multi-domain command and control, and a new way of applying military power.

One of the important implications mentioned will be the need to operate in a network that allows for the necessary synchrony. Superiority in multi-domain

7 NATO JADO: A Comprehensive Approach to Joint All-Domain Operations in a Combined Environment, Joint Air Power Competence Centre (2021) and Joint Concept Note 1/20, Multi-Domain Integration, UK Ministry of Defence, MOD (2020).

environments will only be achieved through data-driven *situational* awareness and advanced analytics systems to support faster and more accurate decision-making (Saur, 2021: 112). As a result, this new way of operating will require a much higher degree of processing, automation and integration throughout the mission cycle from planning to execution and subsequent assessment than is currently the case. And this is where the need for networking, connectivity and the so-called *combat cloud* arises, on which we now focus our attention because of its importance.

The *combat cloud* is basically a connection network of nodes integrated in a cloud environment (an environment in which its elements have the capacity to access information from any device and location), in which they can store and manage data, run applications and deliver content, each with a specific function. To implement the 'system of systems' concept, the *combat cloud* would ideally include a combination of manned and unmanned elements constituting the parts of a comprehensive combat system based on an interoperable network of command and control elements, including platforms, sensors and weapons [a range of effect producers that can execute different orchestrated and synchronised actions]; operators; information (and the ability to process, prioritise and distribute it); and interfaces to convert information into execution (Sanchez-Horneros, 2019: 665-666). Through secure and resilient connectivity to attacks in cyberspace, this concept aims to progressively connect manned and unmanned platforms by incorporating new digital technologies, such as artificial intelligence, *Big Data* management and quantum computing for decision support and systematic execution of the chain of actions and activities included in the mission cycle in military operations.

Ideally, in this environment, increasingly networked ground, naval and air assets should be seen not only as producers of effects but also as sensors and data relays of a true joint command-and control-network, in which all the component commands (or established commands) are integrated and from which they benefit. The importance and effectiveness of weapon systems operating in this *combat cloud* will not be based on what they can do in isolation but more on what they are able to contribute to the other elements of the overall combat system. The priority of the network will therefore be connectivity, the free flow of information and data transfer between airborne platforms, and the command-and-control system to other component commands, which will increase decision making at all levels and tactical options for weapon and sensor employment.

This environment, the development of which is a highly ambitious project, will henceforth be the enabler of how to fight collaboratively. Although it has already taken its first steps in the industry and in the Spanish FAS at a conceptual and planning level [the future FCAS system[8] will have to operate in environments of this

8 The Future Combat Air System (FCAS) project involves air assets and technologically advanced liaison satellites. It is based on two pillars: the Next Generation Weapon System (NGWS) and the so-called cooperators, a group composed of data link satellites, the A400M (operational-tactical transport aircraft), the MRTT (strategic transport and in-flight refuelling aircraft), the Eurofighter and the UCAV (Unmanned Combat Aerial Vehicle), unmanned combat air assets. Sánchez-Horneros J. (2019, 664-673).

type alongside previous systems, the so-called *legacy* systems], its implementation is a long road where adequate operational requirements and a new Concept of Operations must be defined, all harmonised at a joint level because a progressively greater number of systems, platforms and operators of all types will work in the combat cloud in a collaborative manner.

To this effect, operating will therefore increasingly mean doing so in a network, and connectivity is a key element in this. Only a robust and secure connection will allow the commander to make the rapid decisions that this way of operating demands, and also for the systems used, which are capable of operating in a multi-domain environment, to produce the effects at the right time and in the right place. However, this network environment must be clear and well-structured, otherwise it will hard for it to achieve the necessary agility and efficiency. It must be based on properly established standards, rules and procedures, on the existence and acceptance of a shared code, and on the willingness to exchange information between its components, which implies sufficient bandwidth.

This makes the network a critical capability and therefore a vulnerability, making it necessary to maintain a certain degree of superiority in cyberspace and in the use of the electromagnetic spectrum. The interaction of the two domains, aerospace and cyberspace, and the dependence of the former on the latter, further underlines the need for an alternative mode of operation based on positive and procedural control, which can be accessed by automated reversal procedures in case of the degradation of cyberspace and its own data and communication networks.

Based on the possible difficulties of accessing different zones and maintaining "conventional" [traditional] superiority in the domains, in this environment the key to countering the adversaries will be to manoeuvre with agility between domains and to obtain multiple opportunities to produce harmful effects on their vulnerabilities through what are called "windows of opportunity"[9]. This can be via actions in any of the domains, saturating them with multiple dilemmas at different points in time and space (Martínez Cortés, *op. cit.*: 160), while complementing or abandoning [depending on the circumstances] the classical concept of planning and execution in phases, as well as the traditional criterion that effects in one domain must be primarily achieved by forces operating in that same domain. To this end, in terms of cross-domain integration, and in addition to the step forward that must be made with the integration of the traditional domains (supposedly coordinated to some degree at present), progress will have to be made progressively with the effective integration of the cyberspace and cognitive domains with the aerospace domain in the case of the Air Force, adjusting the concept and planning of operations accordingly in parallel with progressive understanding of the form of integration and operational implications.

As far as command and control is concerned, this should undergo a process of evolution. This joint function includes tasks such as establishing command

9 Joint Concept Note 1/20, Multi-Domain Integration, UK Ministry of Defence, MOD (2020, 43-45).

relationships, planning, allocating tasks and resources, and evaluating progress towards objectives. For decades, the communications network on which the Armed Forces, and particularly the Air Force, have been based to conduct these activities has been largely uncontested, in an operational environment that has allowed for a highly centralised approach to air command and control. In turn, the centralisation of aerospace operations planning in a *Joint Air Operations Centre* (JAOC) has allowed the joint force to maximise planning efficiency, ensuring that commanders could weigh sensitive issues and reallocate resources flexibly as priorities changed.

However, and depending on the circumstances, this approach in a potentially "contested" environment can create a great vulnerability in aerospace operations (Priebe, *et.al.*, *op. cit.*: 47-54): an attack on the JAOC or significant disruptions in long-range communications may leave certain forces without the ability to plan and coordinate air operations. In addition, even when communication links between the JAOC and other locations may be available, bandwidth may limit the size of files, making it difficult to share images and videos. The joint force should therefore evolve the model via which it establishes authorities and responsibilities among subordinate commanders, prepares plans, prioritises and allocates resources, and communicates orders.

As outlined above, the very likely degradation of the electromagnetic spectrum and communications, coupled with the increasing use of non-physical domains, requires greater independence of tactical commanders in the execution of their missions. In particular, the fundamental principle established in aerospace operations of "centralised control and decentralised execution" should be complemented, depending on the circumstances, by a distributed control[10] that should adapt to operational changes and needs (Reilly, 2016: 70-71), allowing for delegated action based on windows of opportunity rather than on traditional methods in the physical domain. Basically, we are talking about a delegation of authority in the search for effectiveness, but in a restricted, limited and progressive manner. The allocation of this distributed (delegated) control should be made according to different parameters such as the nature of the operation and its priority, available means and geographical range of the desired effects, in addition to who has the best knowledge of the situation, which thereby acquires greater importance than previously. However, based on the terms of delegation of authority and the strict protocols to be established, this complement to distributed control must never be abstracted from the action of centralised command and control (personalised in the commander and his executive delegation of authority structure), so as not to hinder the implementation of the principle of unity of command. It is important to bear in mind that distributed control should be able to be applied only

10 Distributed control constitutes "a pyramidal structure in which certain responsibilities and competencies are delegated from higher levels, limited in time and/or place, and according to pre-established criteria. This delegation of authority is a function of several factors, in particular the nature and scope of the mission and tactical situational awareness...". Basic Aerospace Doctrine IG-00-1, Air Force, 2nd Revision (2020, 32).

to certain missions, and should be combined with centralised control of all other activities.

In this regard, and in the light of communications threats, some air forces (such as the US and the French ones)[11] are developing new concepts for greater decentralisation of air operations control, "shifting the doctrinal reliance on large and vulnerable centralised command and control nodes to more agile networked solutions, evolving towards distributed control and the decentralised execution of multi-domain operations". It is important to note, however, that this major change should not be seen as an all-or-nothing event, and will most likely not only be implemented in a restricted way but also progressively, as technology and proprietary systems allow for its implementation.

To this effect, in these new environments, the principle of centralised control and decentralised execution, which is deeply rooted in aerospace operations, will be complemented and its execution enhanced by distributed control (Priebe, *et al., op. cit.:* 47-55) to different subordinate levels of responsibility (where appropriate and under the terms of delegation of authority to be determined). By means of data sharing and based on a delegation of authority protocols, this add-on, which will increase operational efficiency across domains, will also allow commanders to focus more on realignment and redirection of capabilities to complete objectives and on decision issues, rather than on the actual execution of [aerospace] operations. However, an appropriate balance between centralisation (command and control) and decentralisation (execution) will need to be sought because connecting tactical operations with operational and strategic objectives will become more common.

In the other hand, in terms of the new way of operating, the big difference will be that in many cases, instead of looking at the forces he has in the particular domain or component, the operation commander will have to look at the overall force mix to determine which forces or elements are best able to achieve the desired effect, whatever their original domain. However, this statement should not lead us to think that in the future all available forces will be able to have an impact in all domains, which would lead to an inappropriate distribution of resources. On the contrary, and considering the roles and missions of each force adapted to the needs of the future, from among the elements of the force capable of performing effects in the relevant situation, the commander will have to choose the option that is most advisable. What is certain is that in this context the operational commander's intention and the overall operational situation (provided in the *Common Operational Picture* (COP), a representation of the overall operational situation pieced together on the basis of data and information provided by more than one component command) must be well known and updated in real time at all levels, including at the lowest level of the operator (MINISDEF, 2019: 36-37).

11 Summary of the Joint All-domain Command and Control Strategy, Department of Defense, USA (2022) and Concept d'Emploi des Forces CEF, État-Major des Armées, France (2020).

Likewise, the new way of operating should provide for the decoupling, as appropriate, of dominance and component command. The complexity of the operating environment is evolving in such a way that the interdependence and interaction of the different domains, and the possible cascading effects, will force a change in the comfortable spaces of the operational domains linked to the different component commands (land, maritime, aerospace and cyberspace), which will basically require a change of mindset as well as strategies to be able to influence, in particular, the non-physical domains from other domains. The shift from operating each component (land, maritime, aerospace and cyberspace) primarily in its respective domain [with varying degrees of effective coordination] towards a new synergistic way of acting across domains, but selecting the component or elements that are best placed (MINISDEF, 2019: 36), spatially or temporally speaking, will need to break many mindset barriers as it is a radical departure from the format learned by most SAF commanders.

Moreover, although it may seem merely a matter of semantics, the difference between operating in a multi-domain environment and producing effects in different domains in a cross-domain way (which has already been done for years) is substantial, as they differ in objectives, strategy and means (Bott, 2017: 24), a scheme known as "ends-ways-means" in its English terminology. In terms of objectives, there should be a move from coordination of objectives by separate component commands to "complementary objectives with a single purpose". In terms of strategies, when circumstances and capacities allow, there should be an evolution towards the search for and achievement of windows of "temporary advantage" and the "projection of power and production of effects in all domains", allowing freedom of action for actors in other domains to produce the necessary effects. And last, in terms of available means, the evolution will probably consist of a shift from a concept of massed forces (located in large forward operating bases) with constant communication and regular supplies, towards a type of "flexible forces operating in a dispersed way and following the commander's intentions in a rapid and autonomous manner", operating in line with the "mission-command" concept[12].

Furthermore, the pace of battle and its acceleration will make it impossible to address conflicts through standardised tasking and execution of operations in a traditional format; the processes of planning and executing military operations, aerospace in this case, will need to be reviewed. The cyclical-linear system of selecting and assigning targets, executing the appropriate effects, checking damage and reassigning targets is likely to be maintained, but should be revised and evolve to a more agile and dynamic

12 As set out in the Framework for Future Alliance Operations, NATO (2018), future C3 (command, control and communications) requires the Alliance to possess resilience, adaptability and interoperable C3 systems. Due to the complex and dynamic battlespace [operations space] of the future, commanders will increasingly need to exercise their authority and issue instructions using a philosophy referred to as "mission-command" in which disciplined initiative is allowed within the framework of the commander's intent. Forces will also need the ability to observe, guide, decide and act across domains to conduct fully integrated operations using a holistic approach to achieve the desired effect.

approach *(Air Force Future Operating Concept*, USAF, 2015: 7-8) imposed by the tempo of a new [multi-domain] operating environment with much a faster pace than is usual.

Human resources have always been a critical element in the military operations environment, and even more so when it comes to stages or phases of evolution. Technology alone will not maintain the strategic advantage; the complexity of current and future scenarios demands not only mental agility and a change of mindset but also an adequate preparation of staff, harnessing their full potential. Achieving the right level of individual and teamwork skills will require adequate education and training in line with the needs of modern scenarios. Both training and coaching should shift their focus towards greater complexity and integrity. As a pivotal element in this evolution, aspects related to the mental agility demanded by this evolution and way of operating should be addressed and improved, as should the training itself, basically in terms of the holistic vision of problems and the capacity for analysis and interest in knowledge. Furthermore, in addition to leadership skills, critical thinking (the ability to analyse incoming information) and strategic thinking (the ability to focus on a forward-looking approach and strategies to achieve something concrete and a plan of action to achieve the desired objectives) should be encouraged, both of which are areas that need to be emphasised as they are generally neglected in staff training.

Last, with regard to the way in which aerospace power roles should be implemented[13], they should generally not change significantly in this new space of operations *(Air Force Future Operating Concept, USAF*, 2015: 11); what will change will be the way in which they are implemented and, above all, the command-and-control scheme in which they will be immersed. Likewise, in the short to medium terms, cyberspace capabilities will be progressively integrated into all aerospace power roles in general, as they will be in other instruments of military power. In this way, aerospace systems, likewise suitably integrated in the multi-domain environment, should be able to contribute to maintaining superiority and producing certain effects in other domains and to general situational awareness to continue to be the primary tool of National Security that it is today.

In summary, we can say that operating in the new operational environments will require a significant change in the way we operate, performing networked missions and integrating the ability to produce cross-domain effects, with faster decision-making and [real] combat agility that incapacitate an adversary who simultaneously applies traditional and non-traditional methods. The only way to achieve integration in this scheme will be to have a single set of information about the adversary and its movements by connecting to a single *combat cloud*. This new way of operating is, without exception, a challenge to all those operating in the aerospace domain; it will not only directly affect the way we operate [as has been widely seen], but also the

13 As set out in Basic Aerospace Doctrine (IG-00-1, 2nd revision, 2020) and NATO Aerospace Doctrine Document AJP-3.3. (Allied Joint Doctrine for Air and Space Operations, Edition B Version 1, April 2016), and in addition to the necessary command and control, the four fundamental roles of aerospace power are air-space control, lethal/non-lethal strike, air mobility and ISR.

design of future military capabilities. However, technology is not everything; as in other policy areas, aerospace power operators will need to achieve their systems skills, capabilities and processes in high-intensity environments by learning the necessary knowledge, analytical skills training and training in, among others, next-generation LVC (*Live, Virtual and Constructive*) scenarios[14]. Of course, while the concepts of "fog and friction", in *Clausewitz*' s terms (representing uncertainty and friction), continue to exist, rigorous training and demanding process training should help to quickly understand and overcome emerging impediments to mission achievement.

Conclusion

On the basis of what has been discussed in this article, it can be stated that the operational space of the operating environments that await us today and in the medium-term future (up to 2040) are being significantly altered by the different aspects mentioned above. To maintain effectiveness as an essential tool of National Security, the Air Forces, and the Air and Space Forces in particular, should evolve and adapt the way they act and operate in this operational space. Failure to do so would mean losing the relevance of the Air Force as an instrument at the disposal of the government to fulfil its mission.

Among the key elements in addressing these developments, the following can be highlighted. First, greater knowledge and understanding of hazards and environments will be required, as well as the necessary adaptation and resilience to withstand and recover functions adequately. Second, it should be possible to operate with greater agility across domains, which will only be possible by operating in a network via robust and secure connectivity that allows for agile cross-domain effects, for which it will also be necessary to enjoy the desired superiority in cyberspace.

In addition, a more agile configuration of command and control should be progressively implemented to facilitate the application of the fundamental principles of the command-and-control function, evolving towards greater decentralisation under the "*mission-command*" philosophy. This should allow subordinate commanders more disciplined initiative within the framework of the commander's intent. Third, greater agility and flexibility, in addition to a huge capacity to adapt the way of operating, will be necessary to maintain the strategic advantage that allows [aerospace] operations in

14 The Armed Forces will need to be supported by highly capable operational training systems focused on innovation, adaptation and responsiveness, and that are capable of incorporating the complex, increasingly contested and degraded operating environment. By creating complex, customised training events and leveraging existing technological capabilities to integrate real and artificial (synthetic) elements and performances, these systems enable training in highly dynamic, high-intensity environments in which decision-making under pressure can be improved, both in the command function and in the execution of operations, while allowing for a decreasing use of real platforms.

a multi-domain environment to be tackled with probability of success, producing the necessary effects across domains. Last, given that human resources, like cyberspace, are a cross-cutting element, superiority in the cognitive domain will also be necessary, although this will be difficult to achieve in all its aspects.

Bibliography

Books

Baqués, J. (2021a). *De las guerras híbridas a la zona gris: la metamorfosis de los conflictos en el siglo XXI*. UNED.

MINISDEF. (2019). *Challenges for Allied Air Forces in future multi-domain scenarios*. MINISDEF.

Qiao, L. and Xiangsui's, W. (essay, 1999). *Unrestricted Warfare*. Translated and published (2015) in the West by Echo Point Books & Media.

Articles

Arauz, J. (2013). Asymmetric warfare and proportionality. *UCM*.

Baqués, J. (2017). Towards a definition of the "Grey Zone" (GZ) concept.

— (2021b). From hybrid wars to the grey zone. *Global Strategy*.

Bott, J. W. (2017). What's After Joint? Multi-Domain Operations as the Next Evolution in Warfare. *School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth.* Kansas.

Colom, G. (2018). Hybrid wars. When context is everything. *Army Review* (June).

Dacoba, F. (2021a). Conflictividad s. XXI; los grandes suben la apuesta. *IEEE.*

— (2021b). Pero…¿todavía hay guerras? *IEEE*.

— (2022). Una nueva ESN para una nueva realidad. *IEEE.*

Fojón, E. (2021). A grand illusion? The European Union and Geopolitics. *IEEE*.

Hoffman, F. (2007). Conflict in the 21st Century. The Rise of Hybrid Wars, *Potomac Institute for Policy Studies.* Arlington.

Hoffman, F. (2009a). Further thoughts on Hybrid Threats. *Small Wars Journal.*

— (2009b). Hybrid vs. Compound War. *Armed Forces Journal* (October, 1).

— (2009c). Hybrid Warfare and Challenges. *Joint Forces Quarterly* (issue 52).

— (2009d). Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict. *Strategic Forum.* No. 240 (April). Institute for National Strategic Studies.

Huber, T. (2002). Compound Warfare: The Fatal Knot. *U.S. Army Command and General Staff College Press.* Kansas, Fort Leavenworth.

Martínez Cortés, J. M. (2019). Las fuerzas aéreas aliadas ante los futuros escenarios multidominio. *Aeronautics and Astronautics Journal.* Issue 402.

— (2020). La relevancia del poder aeroespacial en escenarios de amenaza híbrida. *Revista Aeronáutica y Astronáutica* (November).

Priebe, M. *et al.* (2019). Distributed Operations in a contested environment. *RAND Project*.

Reilly, J. (2016). Multidomain Operations, A Subtle but Significant Transition in Military Thought. *Air & Space Power Journal* (Spring).

— (2018). Over the Horizon: The Multidomain Operational Strategist. *OTH journal.*

Sánchez-Horneros, J. (2019). The Next Generation Fighter in the FCAS concept. *Aeronautics and Astronautics Journal* (September).

Saur, H. (2021). Multi-domain Combat Cloud. A vision for the Future Battlefield. *JAPCC*.

Walker, R. (1998). SPEC FI: The United States Marine Corps and Special Operations. *Naval Postgraduate School.* Monterey, CA.

Official documents (national and foreign)

Air Force Future Operating Concept, USAF. (2015).

Allied Joint Doctrine for Air and Space Operations AJP-3.3, Edition B Version 1. (NATO, 2016).

Concept d'Emploi des Forces CEF, État-Major des Armées, France. (2020).

National Defence Directive. (2020).

Basic Aerospace Doctrine IG-00-1. Air Force, 2nd Revision. (2020).

Operational Environment 2035. MINISDEF. (2019).

National Security Strategy. (2021).

Framework for Future Alliance Operations, NATO. (2018).

(The) French Joint Vision of Multi-domain, Joint Concept JC-0.1.1_M2MC, French Joint Centre for Concepts, Doctrine and Experimentation. (2021).

Joint Concept Note 1/20. Multi-Domain Integration. UK Ministry of Defence, MOD (2020).

"NATO JADO": A Comprehensive Approach to Joint All-Domain Operations in a Combined Environment. Joint Air Power Competence Centre. (2021).

(The) NATO Warfighting Capstone Concept: Key insights from the global expert symposium summer 2020. Hague Centre for Strategic Studies. (2021).

Panorama of Geopolitical Trends Horizon 2040. Second Edition. MINISDEF. (2021).

Strategic panorama. IEEE. (2021).

SIPRI Yearbook 2021. Stockholm International Peace Research Institute.

Strategic Foresight Analysis 2017 report. Allied Command Transformation ACT-NATO. (2017).

USAF Role in Joint All-Domain Operations. AFDP 3-99. (2021).

Article received: 19 August 2022
Article accepted: 15 December 2022