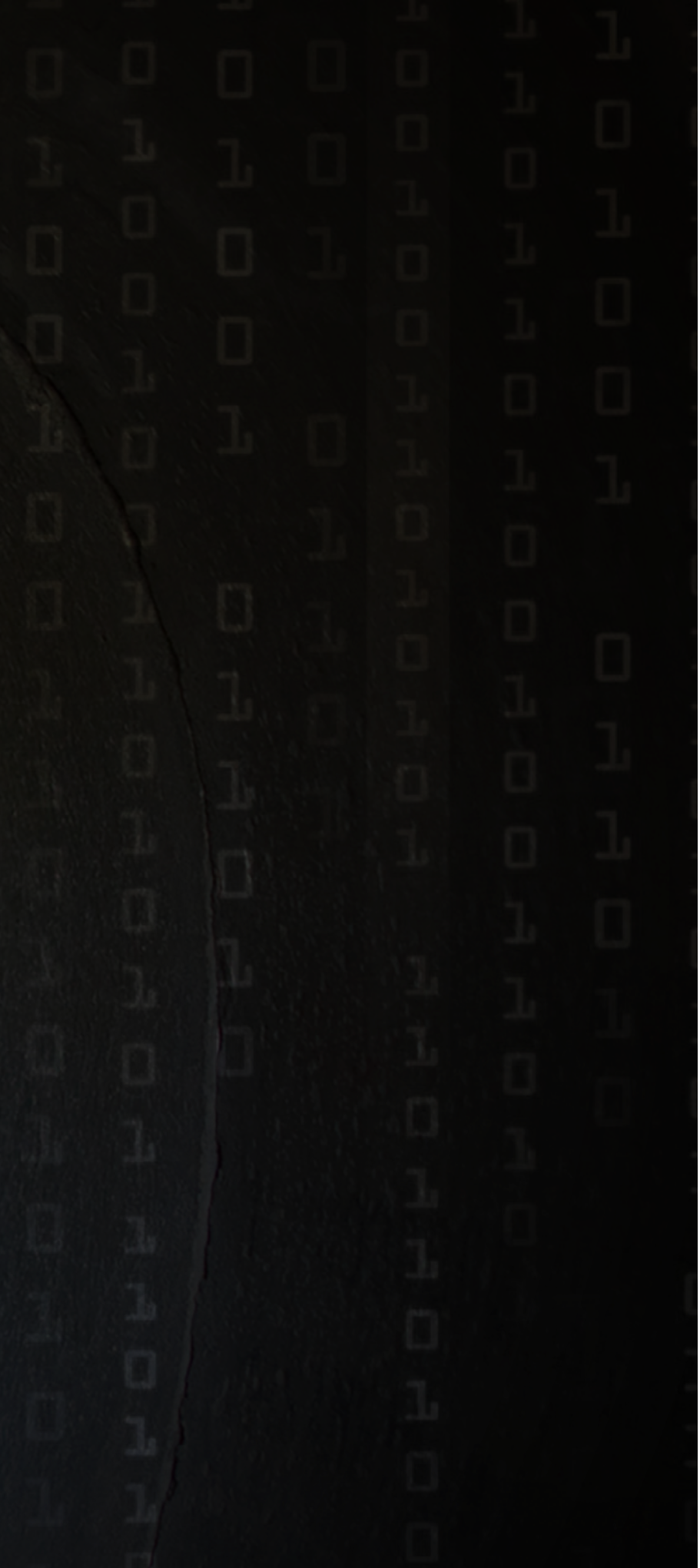
OPERATING ENVIRONMENT 2035

1st Revision

MINISTERIO DE DEFENSA



OPERATING ENVIRONMENT 2035

1st Revision

Concept Development
Joint Centre

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de Defensa
https://publicaciones.defensa.gob.es

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

publicaciones.defensa.gob.es
cpage.mpr.gob.es

Published by:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Paseo de la Castellana 109, 28046 Madrid

NIPO 083-22-187-3 (print on demand)
ISBN 978-84-9091-674-2 (print on demand)

Edition date: October 2022
Layout and Printing: Ministry of Defense

NIPO 083-22-191-2 (e-book edition)

NIPO 083-22-188-9 (online edition)

ÍNDICE

CHAPTER 3

Foreword

In 2017, the National Defence Advanced Studies Centre (CESEDEN) launched the "Futures Programme", to research and respond to the many unknowns foreseen in the 21st Century Armed Forces design. The programme produced two separate but complementary documents that have made a significant contribution to addressing these questions, and the outcome of the initiative has been a success. *Panorama of geopolitical trends. Horizon 2040*, produced by the Spanish Institute for Strategic Studies (IEEE) and the *Operating Environment 2035*, produced by the Concept Development Joint Centre (CCDC), then still at CESEDEN, have provided a glimpse of how our Armed Forces should evolve to face the challenges of the coming decades.

After a period of three years, coinciding with the start of a new military planning cycle, both documents have been revised. The result of this review is the present *Operating Environment 2035 - 1st Revision*, the main purpose of which is the operational and strategic analysis of the Armed Forces operating environments, aimed at defining the military strategic framework.

Also produced by the CCDC, now within the framework of the Joint Staff new Force Development Division, it follows the guidelines of the previous version; hence it has not been prepared by a small group of experts; rather, it is the product of a broadly collaborative and consultative process, both within the Armed Forces, the Security Forces and the Spanish academia and business sectors, so it can be said that it is an example of Spanish strategic thinking on security and defence matters.

I would therefore like to thank all those who have participated in this process, who have helped to make this document more comprehensive, realistic and probably more accurate. The evolving forms of action in cyberspace, the information environment and outer space; the new concepts of integrated operations and networked combat; the great impact of disruptive and emerging technologies; and the need to renew much of the military equipment, in a growing budget economic context, increase the degree of uncertainty in the future Operating Environment, forcing us to make a greater prospective effort to avoid mistakes as far as possible.

As a result, proper foresight and firm and decisive development of the mentality, organization, materiel tools and people that constitute the Armed Forces is becoming increasingly necessary, albeit it may be complex and even traumatic in some respects.

An environment that is constantly changing, and that at an ever-increasing pace, requires continuous adaptability for the Joint Force. After a creative debate on this change and an in-depth analysis, the purpose of this document is to guide, over the long term, the lines of action to determine the strategic framework, doctrinal reflection, capability planning, concept development and Force readiness. This document intends to be a reference point for a process of continuous reflection and adaptation towards a future that is difficult to foresee, but in which many of the main trends are already present.

It must be stressed, however, that the essence of the war has not changed, nor has the Armed Forces continued commitment to the present and future of Spain.

To this end, after describing the characteristics of the future Operating Environment and setting out the Operational Scenarios in which the action shall take place, the main characteristics that should shape the future Armed Forces are presented, as are the 10 potential areas for change in the Armed Forces identified so that they may adapt to the 2035 Operating Environment and equip themselves with these characteristics. The aim is thus to realistically achieve a Multidomain-integrated, highly-combat-capable, balanced, effective, viable, sustainable, efficient, versatile, highly-responsive, flexible, resilient, highly-available, strategically-mobile, modular, innovative, adaptable, interoperable force with strong morale.

A Force that must also be fully prepared to make a greater and more intense contribution to the National Security System, maintaining its own Defence component while strengthening the mechanisms for collaborating and coordinating with other instruments of State power. Nor should we forget that the Armed Forces shall remain the main guarantors of our sovereignty, independence, territorial integrity and constitutional order in 2035, as well as a very important element of our international significance, of our progress and well-being and, in short, of our freedom.

CHIEF OF DEFENCE

Admiral General Teodoro E. López Calderón

Madrid, on the 8th June 2022

Executive overview

In today's rapidly changing and uncertain world, identifying global trends in the various areas that shall shape the future security environment is complex. How these trends interact with national interests shall generate contexts with varying degrees of conflict, competition and cooperation that shall shape the operating environment of 2035.

In a context of ongoing competition, including among allies, generalized rearmament, of permanent friction with adversaries in what has come to be called the gray zone, and of ever closer and more likely hybrid conflicts, the Armed Forces shall remain one of the main instruments of democratic states to intervene in conflicts, guaranteeing defence, protecting national interests, contributing to international stability, and providing security and well-being for their citizens.

Thus, the Armed Forces, without in any way abandoning their reason, which is the military defence of Spain, participate more and more in National Security.

However, the coming changes in the fields of security and defence are expected to be of great magnitude, largely linked to revolutionary technological development, of which we only know the beginnings at this stage. Therefore, thinking about future operating environments and, hence, the design of future Armed Forces, is becoming increasingly necessary, albeit more difficult.

The purpose of this document is to reflect on the characteristics of the Operating Environment (OE) 2035, on the possible scenarios or operational contexts in which the Armed Forces may operate and on the changes they shall have to face successfully to adapt to this environment. The OE 2035 must provide a rigorous starting point for the development of military planning, shaping a future effective Armed Forces and continuing to fulfil its mission adequately.

The document is organized into three main sections. In the first section, the characteristics of the current operating environment, the geopolitical and social environment, and the military and security environment are analysed, not only by describing the current characteristics, but also by seeking to identify the predominant trends in each.

The second section consists of an analysis of Spain's vital and strategic interests. The Operational Scenarios (OS) in which the Armed Forces shall act to safeguard these interests are then laid out. Three OS[1] have been identified:

---

1 Both the Operational Scenarios and the Military Strategic Courses of Action are framed within what the National Security Strategy calls the Strategic Axes of Integrated Strategic Planning, as shall be seen below.

- Operational Scenario (OS) 1: MILITARY DEFENCE (Deterrence, Surveillance, Prevention and Response), which is the main Operational Scenario of action[2]. This is where the Armed Forces conduct their primary mission and is their reason.
- Operational Scenario (OS) 2: PROJECTION OF STABILITY ABROAD, in which we contribute, mainly alongside our partners and allies, to international security and the defence of universal values in fulfilling our[3] commitments.
- Operational Scenario (OS) 3: PUBLIC SECURITY AND WELL-BEING, setting out the Armed Forces contribution with their capabilities to the National Security System, thus providing citizens with the necessary security environment to live their lives in peace and prosperity[4].

The third and final section is a consequence of the reflection developed in the previous two sections. By way of conclusions and proposals, it identifies the characteristics that the Armed Forces of 2035 must have, highlighting their viability, sustainability, efficiency, responsiveness, versatility, flexibility, resilience, availability, strategic mobility, modularity, capacity for innovation, adaptability, interoperability and moral firmness.

These characteristics shall be essential to be able to fight simultaneously in the five operational domains[5] and take on the missions to be conducted in the future operating environment. This entails a need to address profound changes in multiple areas, which is why, in conclusion, we propose 10 potential areas of change in the Armed Forces fully to adapt them to the Operating Environment 2035.

---

2 Although Operational Scenarios represent a broader concept than the Military Strategic Courses of Action of the Employment Concept of the Armed Forces 2021 (CEFAS 2021), there is a correspondence between Operational Scenario (OS) 1: MILITARY DEFENCE with the Military Strategic Course of Action of Deterrence and Defence.

3 Operational Scenario (OS) 2: PROJECTION OF STABILITY ABROAD corresponds to the Strategic Military Course of Action of Stability Projection.

4 Operational Scenario (OS) 3: PUBLIC SECURITY AND WELL-BEING corresponds to the Military Strategic Course of Action on other Contributions to Security.

5 Land, Maritime, Airspace, Cyber and Cognitive [PDC-01(A)].

Introduction

The choice of 2035 in the first version of this document was not accidental. It was considered a time horizon that would allow for some foresight, since most of the ideas and circumstances present here should be in place by that date, although they shall probably vary in incidence and intensity from the time of writing.

On the other hand, a forward-looking analysis period of more than 15 years falls within what our Defence Planning regulations consider the "long term" when determining the capabilities that the Armed Forces shall need in that period, depending on the foreseeable strategic and operating environments. Therefore, a look at the possible operating environment 15 years ahead is timely, since the speed of change and evolution of the operating environment, as a result of scientific and technological innovation, is of such a magnitude that it is likely to affect all areas of life, including the military, so that beyond this timeframe uncertainty is excessively accentuated.

The aim is therefore to approach the drafting of this document by considering possible changes from the reality of today towards the near future, always avoiding dogmatic assertions. If the global crisis caused by the COVID-19 pandemic, Afghanistan's withdrawal, and Ukraine's invasion has taught us anything, it is that change in different scenarios can be sudden, so that any attempt at a closed, masterly approach can be disproved and rendered obsolete at any moment.

Moreover, the publication of the National Defence Directive 2020 (DDN 2020) and the subsequent Defence Policy Directive 2020 (DPD 2020) sets in motion a renewed Defence planning cycle. Furthermore, the creation of the Force Development Division (DIVDEF) within the structure of the Joint Staff (EMACON), which includes the Concept Development Joint Centre (CCDC), makes it the body responsible for leading the cross-cutting Force Development process and the working element of EMACON on Transformation.

All these circumstances make it recommendable to approach the review of the Operating Environment 2035 (OE 2035) through a complex process of research and anticipatory reflection on the possibilities offered by the various potential futures. This process is a prospective work that aims to propose a study of the future, essentially strategic and with clear operational applicability.

It should be noted that the process has been broadly participatory, involving several rounds of consultations with experts - at all levels - in the various areas or subjects covered. Thus,

the present document reflects to a large extent the thinking of the Armed Forces in a broad and cross-cutting manner.

In addition, experts from outside them, including from industry, academia, diplomacy, etc., have also been involved. The comprehensive vision of National Security, which is a fully valid concept and shall be even more so in the years to come, has made this approach recommendable, thus enriching and improving the document with its point of view covering various angles and a much-required critical perspective. In this regard, the National Security Strategy 2021 (ESN 2021) has been a particularly relevant reference. Therefore, from the methodological point of view, the guidelines of the previous OE 2035 have been followed.

The main objective of the OE 2035 (1st Revision) is to be able to positively influence the future, effectively advise on decision-making in designing Armed Forces that contribute to the National Security architecture. Moreover, the period that begins with this publication is based on a situation of national crisis, as a consequence of COVID-19, increased by the Ukrainian conflict, which shall most likely have significant consequences for the Spanish economy. However, the Russian invasion has led to the beginning of an expansive cycle of Defence spending, foreseeably also in Spain. However, the lack of Defence culture and awareness, in which a large part of Spanish society is involved, including its elites, which makes it difficult to enjoy sufficient resources to face the undeniable challenges to Spain's security in the coming years.

Therefore, mistakes must be avoided as far as possible. It is essential to get the design of the development and adaptation towards more agile, versatile and effective Armed Forces right. An adequate dimension, organization and sustainability, will make it possible to face possible

future challenges, among which it is necessary to highlight the increase in hostile actions in the so-called grey zone and the conflicts on the eastern border of the EU, which will probably provoke a profound redefinition of the European security architecture. Otherwise, we will fall into the mistake of being prepared for the past war but not for the next one, as seems to be inferred from the poor Russian performance in Ukraine. Today's conflicts and security challenges are already posed in very different terms from those of the recent past.

A second objective of this document, which is also of great importance, is to contribute to spreading a Defence culture and awareness, presenting to society which challenges and threats could jeopardize its stability and well-being. This is done to show how to adapt the Armed Forces to guarantee the necessary, important and legitimate protection of our national interests.

As for the structure of the document, the original one has been maintained, since it is considered fully valid. Thus, the main core of the work has been structured in three chapters:

Chapter 1, "DRIVERS OF THE OPERATING ENVIRONMENT 2035", sets out the key characteristics that shall shape the operating environment in 2035. In other words, the scenario in which the actions of the Armed Forces are likely to take place. It is true that many of the factors are already present and may not seem very new, but we are, very probably, at the beginning of a cycle of change from the scenarios of the past, in which the dominant trend shall be an increase in and intensification of the factors already present. Nevertheless, the emergence or accelerated development of certain disruptive technologies is always possible, and these are seen as the main potential driver of change compared to what is envisaged in the chapter.

Its content takes reference to the document *Panorama of geopolitical trends. Horizon 2040 (2nd Edition)*, by the Spanish Institute for Strategic Studies (IEEE), as was its original version. The 1st revision of both Horizon 2040 and the Operating Environment 2035 has been approached in parallel, in continuous coordination. The aim is to achieve a synergistic and coherent transfer from the political-strategic level to the strategic-military level, to allow the conclusions obtained to be exploited in the joint operational sphere.

Chapter 2, "OPERATIONAL SCENARIOS FOR ARMED FORCES ACTION", describes those areas in which the Armed Forces shall most likely be operating in 2035 to protect and secure national interests. Three scenarios are considered:

- OS 1 Military Defence[6]: this is the Armed Forces' reason. Their mission is conducted through deterrence, surveillance, prevention and response, including through widespread high-intensity combat if necessary. This is the context for reaction operations against aggression or threats; permanent deterrent or preventative operations through multiple surveillance, security and control activities in sovereign land, maritime and airspace domains and national interests; and operations in cyberspace, outer space and the cognitive domain, which are more recent but already indispensable. They are conducted daily and on a permanent basis (24/7) and are executed in the national sovereignty space and in the nearby areas necessary to

6 Operational Scenario 1 is aligned with the First Axis (Protect) of the National Security Strategy (NSS) and with the provisions of Chapter I of LO 5/2005, of 17 November, on National Defence.

ensure their effectiveness, as well as in the common and cross-cutting spaces that new technologies have created.

This is the most demanding context as it may compromise the overall Armed Forces capability in such high-intensity, widespread combat operations, where the forces may be largely involved in a dynamic and resource-intensive operational tempo.

- OS 2 of Projection of Stability Abroad[7]: in which, through peace support and humanitarian aid operations, stabilization and development support or, if necessary, collective defence, the Armed Forces defend our national interests beyond our borders. Normally through multilateralism structured by the international organizations providing security, or through integration into temporary international coalitions or through agreements reached bilaterally with different nations.
- OS 3 Public Security and Well-Being[8]: in which the Armed Forces conduct their mandate enhancing Spain security through cooperation with other State institutions in a comprehensive manner. Its fields of action are diverse, such as the fight against international terrorism, organized crime, the protection of critical infrastructure, defence against cyber-attacks, emergency and disaster relief, whether or not arising from hostile actions, Non-combatant Evacuation Operations from locations outside national territory, etc. It also includes the contribution of the Armed Forces to State action, in areas such as civil defence, support for scientific activities, customs surveillance, etc. The COVID-19 pandemic has only reinforced the pre-existing tendency to promote a greater contribution by the Armed Forces to a comprehensive State security to act more frequently and intensively in this environment at the request of the competent authorities.

Chapter 3, "ARMED FORCES ADAPTATION TO THE OPERATING ENVIRONMENT 2035", analyses the implications of change for the Armed Forces, so that it can face the challenges of the future operating environment with a greater likelihood of success. In this rapidly changing environment, it is necessary to consider, with ambition but also realism, the necessary adaptations of military tools. This includes potential areas of change in terms of personnel, materiel, technology and infrastructure, but also in key areas such as leadership, education and training and, in short, the strategic and military thinking that must guide the future actions of the Armed Forces.

Finally, it should be noted that this OE 2035 is not a definitive product but shall be open to a continuous process of revision and updating, established periodically. For this reason, the extension of the duration of the prospective cycle that produces the OE 2035 is under study, with a possible transition from the current 3 years to a 6-year cycle, with its publication coinciding with the year prior to the start of a new military planning cycle. Therefore, the next version would extend a forward horizon beyond 2040.

---

7 Operational Scenario 2 is aligned with the Third Axis (Participate) of the NSS and with the provisions of Chapter II of LO 5/2005, of 17 November, on National Defence.

8 Operational Scenario 3 is aligned with the Second Axis (Promote) of the NSS and with the provisions of Chapter V of LO 5/2005, of 17 November, on National Defence.

However, whenever circumstances dictate or significant changes or disruptions occur in the political-military environment, further revisions shall be made to incorporate those ideas and concepts that shall determine changes in the future operating environment and thus keep the process of continuous adaptation of the Armed Forces active.


A EN TIEMPO REAL
4032940
5194789
68943
1334359
1518
21662
ERESPACIO
kaspersky
LG

CHAPTER 1

Drivers of the Operating Environment 2035

Definition of the Operating Environment

[01] Defence Planning aims to design the Joint Force and obtain the necessary capabilities to achieve the objectives set out in the defence policy and to be able to deal with future operational scenarios. This purpose involves designing effective Armed Forces and obtaining the human and materiel resources to make them real and sustainable. This design must be based on knowledge of the scenarios in which they must work and the missions they will face, as well as the capabilities provided by new technologies.

[02] The operating environment is defined as "the set of conditions, circumstances and influences, either fix or variable, affecting the employment of capabilities and decision-making, as they relate to the operation. The environment evolves with the intensity and speed with which these conditions, circumstances or influences evolve" (Joint Terminology Glossary PDC-00).

[03] It is therefore a complex set of actors, the interrelationships among them, the strategies applied by the aforementioned actors, the areas in which operations are conducted, the capabilities and resources, and the challenges and opportunities that arise due to the objectives to be achieved by the Joint Force. Moreover, there are other global, regional and local variables, such as the political context and public opinion, which influence how the Armed Forces must operate at any given time. These conditions change over time, making them difficult to analyse and understand.

Rigorous analysis of the Operating Environment provides the commander with a comprehensive and detailed understanding of the situation, facilitates accurate and timely decision-making and an understanding of its potential effects and consequences

Characteristics of the Operating Environment 2035

[04] The most recent prospective documents, both national and foreign, insist that the main characteristic of the environment is the so-called VUCA9. This trend is unanimously considered to be on the rise.

VUCA environment

[05] The following table provides a summary of the characteristics of such an environment:

Figure 1: VUCA Environments

	Characteristics:	Effects	Requirements
Volatility	• Nature of change • Rate of change • Dynamics of change	• Makes it difficult to identify trends and patterns • Creates instability	**VISION**
Uncertainty	• Unpredictability • Unawareness / awareness	Makes it difficult to anticipate: • Risks and threats • Opportunities	**UNDERSTANDING**
Complexity	• Multiplicity of causes • Interrelated factors	Makes decision-making difficult	**CLARITY**
Ambiguity	• Multiplicity of interpretations	Lack of knowledge of the situation	**AGILITY**

9 VUCA: Volatility, Uncertainty, Complexity and Ambiguity. There are currently other evolved VUCA models, such as BANI or VI2RCA2S, but in this document we shall keep the VUCA model for consistency with other strategic documents in force.

[06] If one of the main tools of foresight is analysing and projecting trends into the future, **volatility** makes this analysis extremely difficult. Continuous changes at an ever-increasing speed, together with the increasingly frequent occurrence of surprising and high-impact events and the capabilities of emerging technologies, make it difficult to identify trends or patterns. We are therefore living in times when "the *status quo*" is becoming increasingly short-lived. This trend seems to be increasing, so a proper understanding of security-relevant patterns of change, while essential, does not guarantee that the right organization or capabilities shall be in place for every future Armed Forces operation.

The increasingly frequent occurrence of surprise and high-impact events makes it difficult to identify trends or patterns

[07] On the other hand, the lack of certainty about future developments creates an environment of **uncertainty**. There are numerous situations which, because they are in their early stages of development, make it difficult to understand them to assess their future impact. They include the existential crisis of the EU and, therefore, its necessary development in the short term, new trends in NATO, the midterm impact of the Ukrainian conflict, the resurgence of populism and nationalism, the use of mass and global media as a weapon, the increase in hostile actions in the grey zone, artificial intelligence or other emerging and disruptive technologies. This reality makes the necessary anticipation in the planning and execution of operations a challenge that is not without risk.

[08] Therefore, although this anticipation is the paradigm to be pursued, it is necessary to be aware that part of the future actions of the Armed Forces shall be reactive in nature.

[09] The **complexity** of the environment is caused by the number of factors involved and the relationship among them. In the past, each intervening factor was easier to locate, and it was possible to discover the origin of the threat and its possible intensity. However, this pattern has been superseded by a 360º and multidimensional spectrum, where many of the factors involved are not directional but enveloping, cross-cutting, non-linear and interrelated. Thus, the application of possible solutions to problems shall not be unique and unidirectional, but permanently integrated in the framework of multi-domain operations.

[10] Therefore, developing tools and methodologies that allow for greater clarity and a better systemic approach to problems shall be essential for decision-making.

The anticipation required in planning and executing operations is a challenge that is not without risk

[11] Difficulty identifying cause-effect chains and the perpetrator's authorship provides a great deal of ambiguity. The difficult traceability of the authorship of attacks, especially in the cyber and cognitive domains, shall make it difficult to respond to actors who shall seek to exploit this weakness. The agility needed to adapt to this type of confusing situation shall determine not only the way the Armed Forces act, but also their future organization and the optimal skills of their members, requiring agile leadership at all levels.

Geopolitical and social environment

[12] In this section, the main reference is the *Panorama of Geopolitical Trends. Horizon 2040 (2nd Edition)*[10], so the features that may most directly affect the future operating environment are shown in a simplified form.

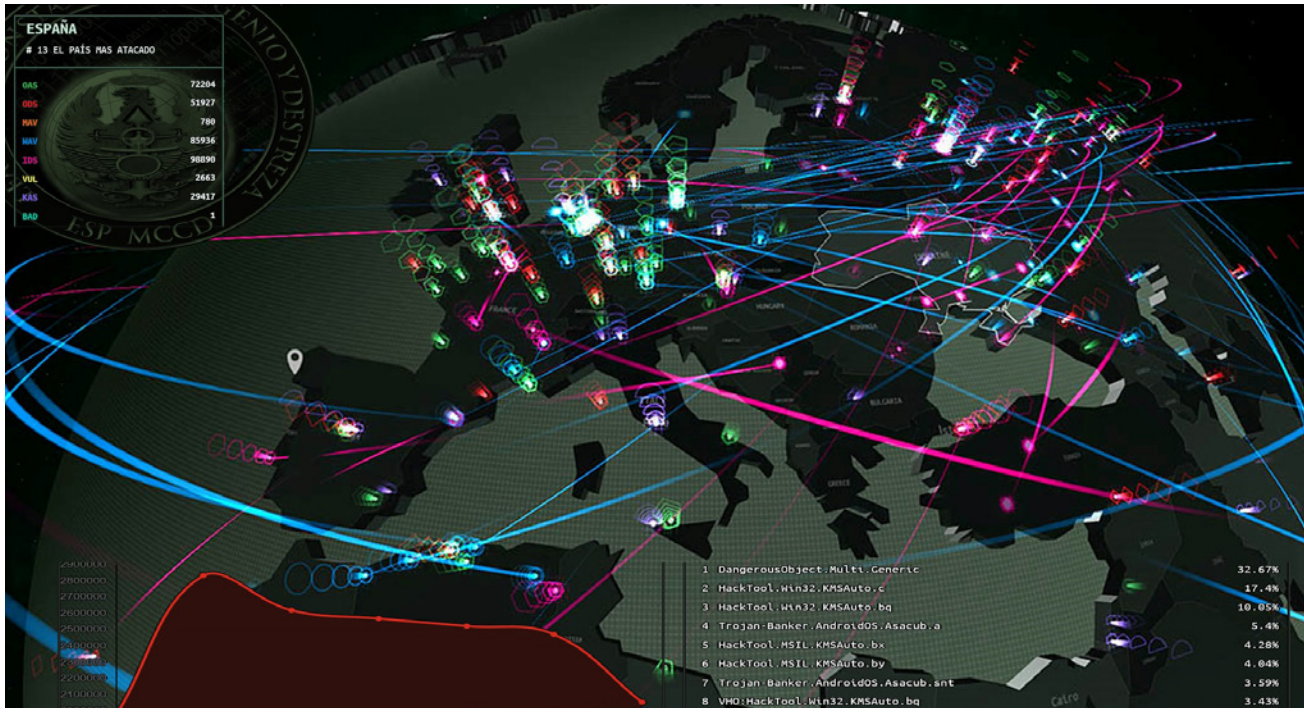
[13] After the bipolarity of the post-World War II era, the US-led unipolar world has come to an end. America's pragmatic approach to energy-related issues has allowed and promoted its strategic retreat, both because of its internal dynamics and the emergence or re-emergence of other global actors. One of its effects is the progressive reduction of its military forces outside its borders, creating relative security vacuums, which are quickly occupied by other countries or armed groups.

[14] The difference in interests between Europe and the United States is coupled with a growing American business, economic and geopolitical competition with China, while the rivalry with Russia, despite the war in Ukraine, is probably secondary. On

10 *Panorama of geopolitical trends. Horizon 2040* (2nt Edition). Madrid, Spanish Institute for Strategic Studies (IEEE), Ministry of Defense, 2021.

the other hand, US disenchantment with and mistrust of Europe's weak defence contribution is growing. Therefore, although the United States shall remain the leader of the West, its level of involvement is, from a European perspective, more uncertain, which seems to be intensified after the end of the intervention in Afghanistan, accentuated by the growing US interest in the Pacific.

While the US shall remain the undisputed leader of the West, its level of involvement is more uncertain than in the past



[15] We are therefore in a multipolar world, with some tendency again to the formation of two competing blocks, led to varying degrees by the United States, China, the European Union and Russia, which shall be joined by other poles such as India, Brazil or even Türkiye and Indonesia, provided that they are capable of evolving towards internal scenarios marked by greater stability and prosperity.

[16] Among them, the role of non-state actors cannot be discarded. After having neutralized the Daesh pseudo-jihadist state in the Middle East as the main driving force of international terrorism, Daesh remains in place in the Sahel and it is possible that it intends to expand again to other areas in Central Asia or Southeast Asia. Not to mention that the recovery of Taliban power in Afghanistan could give a new boost to the aforementioned international jihadism, led by Daesh, Al Qaeda or their multiple regional affiliates.

Daesh remains entrenched in the Sahel and may be looking to expand again to other areas in Central and Southeast Asia

[17] The dispute for leadership between the United States and China is evident, with a tendency to apply protectionist policies in times of crisis. This rivalry, centred on trade, technology and economics, increasingly encompasses security. Even if China's rise creates the conditions for a "Thucydides Trap"[11], its change of *status quo* in the international environment is unlikely to result in open conflict with the United States. In the short term, however, it is likely to influence local or regional conflicts and even the formation of two distinct technological blocs, guided respectively but each superpower.

[18] China's situation due to its economic strength and demographic potential have made the country a major global power in an astonishingly short period of time. Its economy is expected to be the world's largest in the coming decades, surpassing that of the United States. Both circumstances make China a major geopolitical actor with global security interests.

[19] China has traditionally been cautious, basing its strategy on commercial and financial expansionism. However, the current trend is towards greater assertiveness in defending its policies and interests in an environment of business-state symbiosis. This development, together with the strengthening and modernization of its military capabilities, should be closely watched, as China has become the West leading strategic competitor.

China's current trend shows greater assertiveness in defending its policies and interests

[20] For its part, Russia has been able to partially fill the strategic vacuum caused by America's voluntary withdrawal, especially in the Eastern Mediterranean, the Middle East and Africa. Moreover, it gained international prestige by contributing decisively to the defeat of international jihadism in Syria. However, its invasion of Ukraine has, at least temporarily, truncated this process, with great reputational damage to Russia. Therefore, there is great uncertainty about Russia's future role in the international security architecture, which will depend to a large extent on the outcome and the manner in which the Ukrainian war is concluded.

[21] However, despite this recent recovery in its influence capacity, Russia's economic situation, which depends mainly upon the international hydrocarbon trade, also affected by international sanctions, prevents it from being a global player. Although the possibilities presented by its influence in the Arctic could give it greater future relevance, Russia's high level of ambition regarding the reestablishment of its traditional strategic buffer, mainly Ukraine, Belarus and the Caucasus, which has even led it to unleash a major war, has triggered a deep crisis, which makes its understanding with both NATO and EU member countries very difficult.

---

11 The term refers to the possibility of war breaking out when one emerging power threatens the consolidated world leadership position of another.

[22] Russia's fragile economic situation contributes to its motivation to exploit new technologies for the defense of its interests, especially in the fields of cyberspace and cognitive operations, in which it is actively assertive. Russia's poor conventional performance in Ukraine is likely to increase this trend in the coming years, in which Russia will have to rebuild its conventional potential in the face of serious losses. In addition, its friction with the West will bring it even closer to China through a strategic alliance that will enhance the capabilities of both nations, even in scenarios where the presence of both is recent and relevant, as is the case of Africa.

[23] The progressive European diseng-agement from Russian energy products, which will have China as its main recipient, will only reinforce this trend, making Russia's future largely dependent on this alliance with China, turning it into a subsidiary power to a certain extent.

[24] For its part, three divergent trends coexist in the EU. The first is a consequence of Brexit, which shows a possible way forward for countries dissatisfied with what they see as the EU institutions' meddling in their internal sovereign affairs.

[25] The second runs contrary to the first, seeing the UK's exit as an opportunity to make decisive progress on issues that had been relegated to lower prominence by

the traditional British stance. The area of security and defense is perhaps the most relevant in this regard. Advances are to be expected in the coming years in defense matters, which are already glimpsed in the European Global Strategy of 2016 and seem to be accelerated in the "Strategic Compass" of 2022, which insists on the need for greater credibility of European Defense to guarantee the achievement of its interests, mainly in its close environment. The NATO Strategic Concept 2022 is a boost to the relationship between NATO and the EU in defense matters, deepening their complementarity. The conflict in Ukraine seems to reaffirm this option, which although it is currently imposed, it is necessary to consolidate in the longer term, given the differences between some of its members, when the Ukraine crisis has been overcome and European public opinion focuses on issues other than security.

The UK's exit from the EU is an historic opportunity to make decisive progress in the area of security and defence

[26] However, in the EU there are countries with different interests, different strategic conceptions and a different perception of the threat, some focused on the East while others are focused on the South. The war in Ukraine has focused almost exclusively on the East, although the existence of differences of criteria on how to face the Russian challenge is evident, despite the fact that the Russian threat can also materialize from the Southern flank, given its influence in Africa. Consequently, one of the great challenges in the construction of a credible and autonomous common European security will be the harmonization of both trends.

[27] An essential factor in building European security is greater involvement by the population, with the development of a more assertive mentality in defence of its interests and a greater awareness of the sacrifices entailed by effective defence, against several risks and threats.

[28] It is precisely the conflict in Ukraine that has been the main driving force for various nations to rethink the concept of their security, abandoning traditional positions of neutrality or non-participation in defense matters. One of the main factors that has

led to this situation has been the impact on public opinion of a high-intensity conflict in the heart of Europe.

[29] Finally, the third trend is the growing Euroscepticism of a large portion of their citizens. While most governments and national elites are committed to multilateralism as a strategic option, as in Spain, there is strong criticism of globalization, including its security aspect, which is accentuated in crises such as the economic crisis of 2008, the one caused by COVID-19 or the Ukrainian conflict.

Multilateralism as a strategic option is in deep crisis

[30] The frustration of part of society strengthens anti-EU political forces, tending towards the renationalization of the management of both economic and security crises. The result is a weakening of the Union that hinders greater coherence and credibility.

[31] As a specific factor, the growing existence of cultural, religious and social ghettos in many European countries is an enabler of resurgent political radicalism. These, if they increase in size or radicalization, can lead to social conflicts that threaten to overwhelm the capacities of police forces.

[32] It can be concluded that Europe, whose weight on the international stage has diminished, is in crisis, which has been defined as existential by the EU Global Strategy. Displaced from the global axis of influence, at least until the European project is consolidated, it faces the resurgence of nationalism and the growing polarization of political trends, together with a demographic development that threatens the achievements of past decades.

[33] However, European nations are aware that, in isolation, they would be increasingly irrelevant and vulnerable in the international context. The growing Russian threat has increased this perception and may lead to a strengthening of the EU's security policy. The growing Russian threat has increased this perception, which may lead to a strengthening of the EU's security policy, which is already underway but will need to maintain its momentum in the coming years.

Europe is made up of nations that, in isolation, would become increasingly irrelevant and vulnerable in the international context

[34] At the same time, the stable international system that emerged after World War II, based on international law and creating different levels of international political, judicial or security organizations, has become fragmented and lost credibility.

[35] The stagnation of the United Nations Security Council, which has maintained the same decision-making mechanisms since it was founded, is probably the main cau-

se of the UN's loss of influence. Actors of great global significance, such as the EU, Japan, India, the African Union, the Arab or Ibero-American nations, without permanent seats on the Council, feel increasingly disconnected from its decisions, which are often alien to their interests.

[36] Without substantial changes to decision-making mechanisms, the United Nations, the main source of legitimacy in international security matters, may in the future follow the same path of irrelevance as the League of Nations in the 1930s. The Ukrainian crisis has highlighted this situation.

[37] The consequence is that multilateralism, which is desirable as the main tool for conflict prevention and resolution, is giving way to regional, bilateral approaches or *ad hoc* coalitions on the margins of the international system. The trend towards a new militarization and coercive use of economic tools entails a return to using hard power in international disputes, as opposed to diplomatic action and subjection to international security institutions.

There is an unmistakable trend towards a new militarization and coercive use of economic tools as opposed to diplomatic action and subjection to international security institutions

[38] In this context, competition between states is intensifying. This is fostered by the possibility of the continued use of offensive technologies, with less potential for military escalation than traditional conventional confrontation, operating through hybrid strategies in the so-called grey zone. But besides states, there are other elements to be borne in mind in future security, due to their social and economic influence. Non-state actors, mainly terrorism and organized crime, and from another perspective, macro-corporations with large global economic interests, are clear examples.

[39] The aforementioned scenario is significantly influenced by the falling cost of offensive systems capable of causing significant damage. The exclusive capability of states to equip themselves with high-capacity military materiel has to coexist with mechanisms of aggression and influence in the cyber and cognitive domain. These mechanisms, which are simpler, cheaper and more readily available, can have a high-intensity effect.

Mechanisms of aggression and influence in the cyber and cognitive domains can cause very strong effects

[40] This possibility is reinforced by the delay in legal and regulatory adaptations to technological developments. Their pace of development is outpacing the legislative and regulatory processes that govern their actions. In the security field, this is particularly true

for hostile actions in the cyber and cognitive domains, especially given the difficulty of applying our national laws and regulations to technological actors located outside Spain. Similar legal gaps may also influence the future use of artificial intelligence and robotics.

[41] Because of these developments, the current trend is the emergence of a virtual, cross-cutting and delocalized society which, under particularly severe crises, can become anti-systemic and ungovernable. Global interconnection is a true cultural revolution, with great advances but also with undeniable risks for the stability and cohesion of societies as we know them.

[42] National values and interests directly related to security, such as patriotism, loyalty to national institutions and awareness of a common good and purpose, are challenged by being revised and replaced by others of a cross-cutting and transnational nature. Therefore, internal fractures arise, creating social bubbles around ideas that may engender friction among themselves or with society as a whole, becoming misaligned with national policies and interests.

[43] This transfer of values entails a possible weakening of social cohesion. Society, subject to offensive action by various adversaries who manipulate values or the performance of national authorities, can fall into destabilization and internal confrontation.

The emergence of a virtual, transversal and delocalized society

weakens the concept of the nation state. The transfer of values from the national to the cross-cutting and transnational increases the weakening of the cohesion of the nation

[44] Thus, authoritarian regimes or non-state actors promote the discrediting of democratic societies which, by their very nature, have a weak defence against this type of aggression.

[45] On the other hand, similarly cross-cutting international commitments achieve a broad consensus, such as the commitment made in 2015 by 193 countries to the Sustainable Development Goals (SDGs). Initiatives such as these contribute to revitalizing multilateralism, thus counteracting the tendency to renationalize global problems. Obviously, the UN's 2030 Agenda is very ambitious, but significant global progress in the coming decades on the 17 SDGs would undoubtedly mean a significant improvement in global security.

Military and security environment

[46] The history of Armed Forces has undergone many ups and downs. Today and in the projection of the near future, regular forces that exercise the monopoly of force, as a

continuation of state policy, may partially lose that role to non-state armed groups, organized crime or even private security agencies.

[47] Firstly, because these states, influenced by the development of their populations' thinking, are increasingly renouncing the use of the lethal capabilities that their Armed Forces provide them with to achieve their objectives. On the other hand, the use of different tools to resolve international disputes, such as economic sanctions, armament procurement to others, restrictions on movement or the prosecution of members of certain regimes, is on the rise.

[48] Therefore, the dialogue-deterrence combination is today an essential pillar in the construction of stability and international relations. However, evident in the Ukrainian-Russian war, some states still view the use of the military tool within a classical conception of geopolitics and geostrategic, even leading to high intensity warfare, while the rest view it with great reservations and limitations.

Some states still view the use of military tools within a classical conception of geopolitics and geostrategic

[49] On the other hand, it is necessary to bear in mind what some authors have defined as lawfare, which consists of using the laws, uses and customs of the most protective countries against them; this is done by actors who do not respect these laws in any way. This can be a weakness in the dialogue-deterrence combination.

[50] Many nations build and sustain strong and capable Armed Forces for effective deterrence. But if their state legislation were to excessively limit their use and the political will to use military capabilities were too reluctant, it would constitute a structural weakness that could weaken their deterrence capacity.

Deterrence can be weakened by overly protective legislation and too reluctant political a will to use military capabilities

[51] It should also be taken into account that certain non-state actors, outside international laws and customs, have been filling the strategic gaps left by the non-use, or limitation, of military tools. Thus, many of the recent and current conflicts feature entities such as tribal militias, narco-guerrillas, terrorist groups, private military or security companies, etc., as leading participants.

[52] Nevertheless, the conventional military balance remains a determining factor internationally. Western conventional superiority still holds, although the gap between its military capabilities and those of other global or regional actors is narrowing.

[53] This disadvantage leads these actors to focus intensely on asymmetric mechanisms of confrontation, to offset this gap through alternative methods. Thus, alongside tra-

ditional non-state actors, new forms of action are emerging that can be used both by states and by groups or even lone wolves. These forms of action, supported by global interconnectedness and the use of emerging technologies, shall play a major role in conflict in the coming decades.

[54] Actions in cyberspace, outer space and in the cognitive domain, along with the use of emerging and disrupting technologies such as robotics, artificial intelligence, 5G and massive data management, do not change the nature of warfare, but they are already changing how it is waged.

[55] Unwillingness to or delay in equipping ourselves with these emerging security and defence technologies can lead to a lack of interoperability with our allies in military operations, affect deterrence and state-to-state competition, and even cause strategic surprise and defeat in conflict.

New forms of action based on global interconnectedness and the use of emerging technologies shall play a major role in conflict in the coming decades

[56] These new ways of fighting increase the need for highly specialist personnel, both operational and technical, which will lead to a major qualitative leap and substantial

changes in the means, procedures, specialities, readiness and even the understanding of leadership or the working culture of the military forces. This all takes place while maintaining conventional capabilities. To achieve this, military forces must strike the necessary balance between their technological development, their critical mass of personnel and interoperability with their partners and allies.

[57] Indeed, while conventional high-intensity confrontations seem less likely - although they cannot be ruled out, as has recently been evidenced in Ukraine, - the new forms of action described are more likely and are already occurring daily at present.

[58] The pursuit of strategic goals through actions in the so-called grey zone, which are openly hostile but kept below the threshold of armed conflict, leads to an ambiguous situation, which can be seen as a continuous absence of peace without being what it is understood as a full-fledged war. Moreover, success supports the continued and increasing use of such conflicts, as demonstrated by Russia's annexation of Crimea in 2014, or the 2022 Ukraine conflict, in which, in addition to the traditional combat on the ground between Russia and Ukraine, the confrontation in the grey zone between Russia and the West has been exacerbated. It can therefore be argued that our security environment is now permanently in this grey zone, although temporarily high intensity combat episodes can happen.

[59] In this scenario of continuous and technological confrontation, a decreasing trend can be seen in the number of weapon systems of each type that enter service, with quality taking precedence while maintaining the minimum quantity to cover the spaces in possible theatres of operations. One of the main consequences is that by using cheap and more readily available hostile means, the number of actors that can cause serious damage to national interests multiplies, which will harm security.

[60] In this context, the ability to access common spaces and their denial to the adversary remains decisive in the conflict.

The pursuit of strategic objectives through actions in the grey zone leads to an ambiguous situation featuring a continued absence of peace without a full-fledged war

[61] Specifically, actions in the cognitive operating domain, boosted by the use of cyberspace in developing them, make the new primary target of warfare as the public, whether the adversary's, our own or a neutral public. The aim is to alter their perceptions in such a way that they can make the interests of the opponent their own rather than their own. Although this is nothing new, today's tools for disseminating information greatly enhance these actions.

[62] In this scenario, questioning the decision-making legitimacy of authorities and the actions of one's own forces can become pervasive, making it possible for actors of lesser power and capacity to defeat powerful nations or coalitions.

[63] Even security breaches by own forces through unintentional, inadvertent and uncontrolled distribution of information about military actions or other security activities can easily occur. In a hyper-connected world, where the provision of global connectivity is increasingly seen as a fundamental right, the systems' security is a challenge.

Actions in the cognitive domain, enhanced by the use of cyberspace, primarily target the public, both opponents' and their own

[64] In short, it does not seem possible to aspire to a prolonged situation of stability, since a permanent pattern of struggle, strategic competition and conflict emerges, on which extraordinary circumstances can occasionally be superimposed, leading to crises situations. A kind of chronic stress applied to international relations and global geostrategic, alternating between high and low moments. In this environment, the autonomous capacity for self-defence becomes highly significant.

[65] We may infer from all this that the nature of the parties to the conflict, together with the emergence of new types of combatants, is indeterminate. On the one hand, the citizen, who needs to have an adequate security culture and awareness to be sufficiently resilient to the attacks that he or she shall inadvertently and frequently suffer.

[66] On the other hand, personnel specialized in the management, both defensive and offensive, of new tools and forms of action in conflict. Whether civilian or military, they fight from a computer, a television set, transmitting powerful ideas in the framework of strategic communication, commanding a drone or analysing information in a system of indicators and alerts assisted by applications equipped with artificial intelligence, among many other possibilities.

[67] The geographical positioning of the operations shall be dealt with in Chapter 2, but it is necessary to underline that new possible scenarios of confrontation are opening up, developed totally or partially in virtual spaces, without forgetting outer space as an increasingly feasible and disputed field of action.

New virtual scenarios of confrontation are opening up, not forgetting outer space as an increasingly feasible and contested field of action

[68] By way of conclusion, it can be summarized that the military environment is articulated around a multi-domain conflict, in which the tenuous separation between conventional and non-conventional conflict, between regular and irregular warfare, between combat zone and rear-guard, as well as between combatant and non-combatant shall blur.

[69] A constant, uninterrupted and technology-driven conflict, in which low-intensity phases predominate but which can reach peaks of high intensity and lethality; in

which conventional actions converge with an increasing role played by the urban environment and unconventional actions; with a greater demand for speed in decision-making and response; undertaken largely in the cyber and cognitive operating domains; taking place in physical and intangible geographical spaces simultaneously; whose main objective is to exploit weaknesses, often linked to the inherent guarantees of democratic societies, and to manipulate their citizens' perceptions, to violate their security.

A technology-driven multi-domain conflict with increased demands for speed of decision-making and response

Challenges of the Operating Environment 2035

[70] This document broadly follows the outline of the highest strategic level document, the National Security Strategy (NSS), contextualizing the various challenges that the Joint Force shall face in terms of the trends observed.

Risks and Threats

[71] **Strategic and regional tension** and its ultimate expression, **armed conflict**, remain one of the most significant threats to national security. While the likelihood of classi-

cal state-to-state confrontation is considered lower than in the past, it cannot be ruled out, as has been displayed in Ukraine, and it is especially important to maintain the appropriate margin of deterrence. Neglecting the provision of credible and sufficient conventional Armed Forces would make it easier for a potential adversary, who might be tempted to mount a conventional armed conflict to its advantage, to exploit surprise.

[72] Competition between states is more likely in what is known as the grey zone. Limited conflicts, in which unconventional strategies and actions are supported and complemented by ad hoc conventional actions, are more likely to occur. In this hybrid conflict dynamic, the ability and efficiency of the Armed Forces to achieve their assigned objectives shall remain critical.

The proliferation of limited conflicts with hybrid dynamics is highly likely

[73] Possibly, the greatest conventional threat comes from the implosion of fragile states, which are on the path to destabilization as a result of internal social conflicts of an ethnic, religious, political or economic nature. Such situations shall not normally evolve into direct aggression against neighbouring states, but they can lead to situations that, enhanced by criminal and terrorist activities, shall result in a regional deterioration of security. They may also lead to multinational interventions with the deployment of forces to limit or resolve the conflict.

[74] The limited capabilities of some actors in these internal conflicts shall mean that, alongside actions corresponding to non-conventional strategies, asymmetric conventional confrontations shall play a major role, in which terrorist actions, guerrilla warfare and various forms of insurgency shall continue to be used.

[75] On the other hand, these actors shall increasingly aim to equip themselves with anti-access/area denial (A2/AD) systems, which may force them to rethink their strategies in future conflicts, where deployment bases, infrastructure and communications may be more vulnerable than in the past.

[76] The experiences of recent conflicts show they tend to drag on and cannot be considered to be over. Therefore, the international community shall try to avoid prolonged massive deployments on the ground in protracted conflicts. Preference will be given to measures that lead to conflict isolation and surgical interventions with rapid entry and exit of own forces, as well as the use of so-called proxy or remote warfare, through intervening actors.

[77] As populations tend to shift towards cities, it is quite possible that some of these conflicts will be due to the emergence not only of states but also of failed cities. If their size, population, economic and social inequalities become ungovernable, con-

flict may be inevitable. The trend towards the world's population being concentrated in cities leads to conflict scenarios developing mainly in densely populated urban areas, with major constraints on operation, the need to prevent collateral damage and to avoid affecting critical infrastructure.

[78] In these circumstances, the future land environment shall be characterized by the increasing depth of the adversary's actions, the disappearance of conventional fronts, the amplification of the battle space, the increasing use of technology even by asymmetric adversaries and the preponderance of urban space.

[79] Taken together, the foregoing seems to indicate a decline in the strategic autonomy and freedom of action of Western countries, which may see their forms of action and their contribution to international stability constrained.

Surgical interventions to limit and contain conflicts shall predominate, without taking the risks of large contingents deployed permanently on the ground as often

[80] As far as Spain is concerned, the foreseeable development of some nations in our immediate security environment is not optimistic. Demographic growth far outstripping economic growth, as well as climate change, is causing social tensions in these countries because of the lack of opportunities. Consequently, citizens can easily be attracted by the possibilities offered by irregular migration, organized crime or political and religious radicalism.

[81] However, this is not incompatible with a rapid build-up of their weapons capabilities and an increase in their levels of education and training, which is an aspect to which those responsible for our security ought to bear in mind.

[82] Given the seriousness of the consequences of the conventional or hybrid conflicts in the near European security environment, coupled with Spain's responsibility as Europe's southern border, credible deterrence in this area shall remain essential, both from an international perspective - the EU and NATO - and from an exclusively national perspective.

Spain's geographical situation calls for credible comprehensive deterrence

[83] Terrorism and violent radicalization have found in new technologies a space in which to diversify their actions. Besides direct actions against organizations, infrastructure and individuals, proselytizing, recruiting, organising and financing activities are added to the command and control of their actions. It should even be borne in mind that current information technologies facilitate the availability of real online terrorism courses, which are much more sophisticated and training than in the past.

[84] Thus, cyberterrorism is a credible, real and persistent threat. Although its intentions and capabilities have been limited so far, the increasing availability of technological tools raises the prospect of more dangerous cyber-attacks on critical facilities and systems in the future.

[85] In short, alongside the traditional dimension of terrorism, we must consider the possibility of increasingly sophisticated and effective actions in the cyber and cognitive operating domains. Unlike traditional terrorism, the magnitude of the effects they can have on factors closely linked to our way of life and well-being state can create a sense of vulnerability and constant threat for citizens.

[86] In any case, previous experience with the self-styled Islamic State (Daesh) indicates that the availability of large, densely populated and infrastructurally equipped territorial bases for terrorist organizations enhances the phenomenon on a global scale, endowing them with prestige and resources. It is possible that, with this aim in mind, different groups shall once again attempt to take control of territorial and urban areas in the framework of intrastate conflicts linked to the aforementioned failed states or cities.

Terrorism has found in new technologies a space in which to diversify its actions

[87] On the other hand, it is not out of the question that some states may use terrorist tactics or elements as a line of action in their hybrid strategies.

[88] The influence of international **serious and organized crime** networks on the international scene has increased through the diversification of their activities, the sophistication of their capabilities facilitated by the ample funding available and, above all, their interrelationship with terrorism.

[89] However, it exists at the greatest scale in the context of weak or failed states, where the absence of state action facilitates freedom of action and impunity, even controlling *de facto* portions of their territory.

[90] It engages in activities such as illicit trafficking of people, drugs, weapons, works of art or historical heritage and piracy. Because the optimal conditions for carrying them out overlap to a large extent with those for the emergence of terrorist activities, there is a growing interrelation between the two phenomena.

[91] Terrorism and organized crime thus tend towards symbiosis. Profits from illegal trafficking finance terrorism, while terrorist groups create the conditions for illegal mafia activity. Although narcoterrorist groups exist, it is more common for both types of organizations to co-exist separately but collaboratively.

[92] The level of financing these networks enjoy means that they are have great capabilities, both conventional and non-conventional, which in certain scenarios may be superior to those of police forces, hence the involvement of military forces could be essential. Moreover, as with terrorism, these criminal networks can be used by third states, as a form of aggression to their adversaries.

[93] Once again, Spain's location, at a geographical crossroads between continents, seas and oceans, makes it particularly vulnerable to criminal organizations based in the Americas and Africa, especially in the Maghreb, Sahel and Gulf of Guinea, while highlighting and enhancing its role in supporting the affected nations.

Like terrorism, criminal networks can be used by hostile states

[94] Although less likely to occur than other threats, the great danger of **weapons of mass destruction** (WMD) **proliferation** makes it very important. They provide an opportunity for various actors to be able to achieve their objectives, despite their conventional and technological inferiority.

[95] The mere suspicion that states or organizations have these weapons gives them a certain *de facto* impunity, since they are capable of provoking highly lethal responses. They are therefore empowering for their possessor and incapacitating for the opponent, which makes them undeniably cost-effective.

[96] The current trend suggests an increase in the WMD threat in three distinct senses. On the one hand, the inclusion of a greater number of countries into the "nuclear club". Although the stated motives are linked to the peaceful use of nuclear energy, it is no less true that they put these countries in a better position to develop military nuclear programmes within a short time. For nations with abundant sources of energy resources, it may indicate a dual intention, increasing their ability to develop military programmes. The limited effectiveness demonstrated by counter-proliferation treaties may fuel this nuclear expansion.

[97] The second trend is the growing number of countries with delivery vehicles for WMD weaponry, which could fall into the hands of terrorist organizations in the event of internal conflict and destroy already weak state structures.

[98] Moreover, the rapid development of drones and other types of robots makes delivery vehicles that can carry chemical or biological payloads with significant effects readily available to hostile groups, even if they are not particularly well trained or funded.

Drones and other types of robots are accessible delivery vehicles that can carry chemical or biological payloads with significant effects

[99] The third trend is the increase in the technological know-how required manufacture WMD weaponry, in its different variants. It is increasingly credible that terrorist organizations may have the materiel and know-how to acquire some of these weapons, especially biological, chemical or radiological weapons.

[100] The sum of the three foregoing trends indicates that, while the nuclear threat remains unlikely to result in nuclear weapons being used too, the threat posed by biological, chemical or radiological weapons shall become more diversified and more likely. The disastrous global effects of the COVID-19 pandemic only serve to demonstrate the cost-effectiveness of voluntary and hostile actions of this nature and may serve as a source of inspiration for hostile actors. It should be noted, however, that the biological threat is less likely to occur. Biological agents are difficult to produce and manage and the scope of their action is uncontrollable.

[101] Covert data and intelligence collection shall remain a major threat, since data has become a greatly important strategic asset. As we move towards a holistic view of security, **espionage and interference from abroad** has an increasingly comprehensive dimension acting against national interests. Cases such as the recent illicit acquisition of data concerning pandemic vaccines show how industrial and commercial espionage fully impinges on the security of citizens.

[102] Beyond awareness of information security and empowerment at all levels, it is clear that our multicultural and multi-ethnic societies foster the covert presence of individuals and organizations dedicated to obtaining information for the benefit of third parties.

[103] The Armed Forces which also face a multicultural and multi-ethnic future, shall have to find solutions to provide the necessary personnel in the face of Spain's demographic decline. Elements of these personnel may maintain links with outside organizations that use them for intelligence-gathering and espionage activities

[104] Although the classic forms of espionage will continue to exist, cyber-espionage has opened up infinite scope for information theft and is currently the most common form of espionage. This mode affects not only institutions and companies, but can also be aimed at individuals, placing the most significant members of the Armed Forces as a target in this space.

The development of the cyber domain has opened up almost infinite scope for espionage

[105] **Cyberspace** has been a technological revolution with consequences that are difficult to envisage, since it is evolving and developing at a very high pace. It is an area of conflict that has changed the dynamics of warfare.

[106] Its accessibility and the relatively limited means necessary to operate within it have opened the playing field to numerous actors; even lone wolves can acquire highly damaging capabilities and challenge previously invulnerable states or organizations.

The so-called IT Army of Ukraine[12] is a significant example of growing private conflict intervention capabilities.

Small organizations or lone wolves can acquire highly damaging capacities

[107] The centrality and cross-cutting nature of cyberspace makes us more vulnerable. No complex activity takes place without the essential involvement of cyberspace. Areas that are, in turn, central to a nation's survival, such as energy security and food security, depend on its cybersecurity. This vulnerability is also particularly sensitive in the area of defence.

[108] Threats in cyberspace are, by their nature, complex and diversified, including campaigns of narrative manipulation and disinformation. Thus, cyberspace is the main enabler of a relatively new field of action: the cognitive arena. Indeed, operations in the cognitive domain do not take place exclusively in cyberspace, but that is where they have the greatest capacity for action and reach.

[109] **Manipulation and disinformation campaigns** target citizens' psyche, directly targeting opinions, attitudes, wills, beliefs, feelings, etc., to shape and use them, by distorting perceptions, according to their interests. When applied to democratic societies, they are particularly dangerous, since they can have a decisive influence on them, for example, if they are associated with electoral processes.

[110] In the area of security, they may call into question matter such as the state's own reputation and credibility, the cohesion of alliances or coalitions, the legitimacy of military operations, morale in the face of own losses, the funding and motivation of the Armed Forces, etc. Even members of the Armed Forces can be easily influenced, undermining their performance, morale, availability or commitment.

[111] Operations leading to reflexive control, the imposition of narratives on social networks, disinformation campaigns, fake news and memetic warfare are already a daily reality. They are difficult to counter due to their constant development, sophistication and complex attribution.

Manipulation and disinformation campaigns are particularly dangerous when associated with electoral processes

[112] It is to be expected that this threat shall grow, which could make cyberspace a priority arena for confrontation in the coming decades, given its multiple implications for other areas.

---

12 A group of private volunteers organized to fight in the field of cyberspace operations against Russian actions during the war in Ukraine.

[113] Land space, where life takes place and where commercial, industrial, social and political activities are concentrated, is essential to the nation. It is the location of the vast majority of critical infrastructure and state agencies or companies that are essential for the functioning of the country. Therefore, it is the target of most threats and can be expected to be the target of hostile actions by both state and non-state actors. Moreover, because it is where people's lives are lived, it is the area where crises, major disasters or those of hostile origin can have the most serious consequences for the population.

[114] In this area, there has been a gradual population shift towards urban areas and the coastal periphery, to the detriment of the large inland and rural areas.

[115] The maritime space is highly important to Spain. Its geographical location and the arrangement of insular and extra-peninsular territories make controlling the sea a priority objective, on which a large part of its energy and commercial resources depend.

[116] Threats to maritime security come both from hostile actions and from nature. Piracy, encroachment on areas of the Exclusive Economic Zone or territorial waters, illicit trafficking, illegal immigration networks and terrorism are the most obvious threats, but other actions harmful to our interests must also be borne in mind. Underwater historical heritage, the sustainability of the exploitation of marine resources or marine infrastructure, such as ports or submarine cables, must be safeguarded.

[117] Some of the world's busiest shipping routes cross Spanish waters. Furthermore, extracting resources from the sea is becoming increasingly feasible with the advance of technology that makes it possible to exploit energy resources and the sea's subsoil. Similarly, global food security can rely more heavily on the sea, which requires the preservation of marine ecosystems.

Control of the sea is a priority objective for Spain

[118] **Airspace and outer space is** an area of multiple activities of great economic and technological importance, and important for the effective operation of Armed Forces and security forces. Rapidly advancing technology presents a wide range of vulnerabilities associated with the use of both airspace and outer space.

[119] Moreover, the proliferation of actors capable of operating in airspace and outer space, both in terms of companies and states, increases the risk of illicit activities.

[120] Vulnerabilities in outer space are twofold. The first is the possible actions aimed at denying its use by our own forces, given the aforementioned importance of the resources and capabilities deployed. The second, the result of possible hostile actions from space towards our interests. In the near future, denial-of-use actions will be more likely.

[121] Conflicts can be expected to arise over the occupation of the most suitable orbits and the disposition of adversarial means in space, leading to a certain militarization of space, with concepts that shall not differ much from those used in airspace. A space arms race cannot be ruled out, including both satellite weapons and anti-satellite weapons operated from the Earth's surface, orbit disabling, cyber-attacks or denial-of-use attacks.

[122] The high commercial value and strategic potential of space-based assets also makes them a profitable target for terrorist or organized crime organizations, mainly through non-physical attacks that diminish or deny their use.

The militarization of space shall be based on concepts similar to those used in terrestrial airspace

[123] Moreover, besides the well-known harmful use of commercial or general aviation by non-state actors, there is the hostile use of drones. They constitute one of the greatest

security risks due to their easy accessibility and handling, low detectability, increasing payload capacities and the possibility of use in swarms capable of saturating defence systems. Apart from their use as an ISTAR platform, they are valid for a wide range of actions, from targeted attacks on authorities, collisions with conventional aircraft, the use of explosives against critical infrastructure and even the dispersion of chemical or biological agents.

[124] Moreover, their main vulnerability, which is the need for the operator to be close by, shall be reduced by 5G technology, which makes remote operation possible. Nor can their autonomous use by means of programmable systems and artificial intelligence be ruled out.

[125] Advanced societies depend for their security and normal functioning on a wide range of **critical infrastructure** that are essential and difficult to replace. As a result, they are priority targets for potential adversaries, both state and non-state, as well as being sensitive to extreme natural events.

[126] The sectors affected are varied: transport, food, health, banking, industry, etc., but critical energy and communications infrastructure are considered particularly sensitive, as they are the basic support for the other sectors.

[127] While actions against critical infrastructure may consist of conventional attacks, cyber-attacks aimed at preventing and hindering their operation or even physically damaging them are more likely. As most of these facilities are operated by the private sector, close coordination and cooperation between the private sector and the public security sector is key to achieving comprehensive security.

Significant damage to energy infrastructure has a ripple effect across multiple critical sectors

[128] Numerous risks and threats can seriously affect **economic and financial stability**, both nationally and internationally. Actions conducted against critical infrastructure, cyber-attacks, irregular flows of people, catastrophes, pandemics, etc., can significantly damage the economy, affect the public and have a negative impact on security, and even diminish the resources allocated to it.

[129] Inevitably, an uncertain economic situation leads to competition between defence investment and other budget items, which requires a realistic prioritization exercise, as well as measures to ensure the possibility of military planning in the medium and long term, in an environment plagued by risks and threats.

Economic instability has a very negative impact on the resources allocated to the Armed Forces, making difficult medium- and long-term planning

[130] Therefore, in a comprehensive approach to security, it is necessary to guarantee security in strategic sectors which, if damaged, would cause significant damage to national economic activity.

[131] Our **energy vulnerability** is well known. Dependence on oil and gas imports will continue for decades to come, despite the change to the energy model that has begun. Spain's energy mix is highly varied, both in terms of energy sources and external suppliers. This diversification is Spain's greatest national strength regarding energy, but it means that national interests are global, albeit with special emphasis on North Africa and the Gulf of Guinea, beyond the main international exporters in the Persian Gulf.

[132] Spain's outstanding Liquefied Natural Gas (LNG) regasification capacity and nuclear capacity offer a high degree of flexibility and back-up capacity for renewable energies, which are at the forefront of the global energy transition and to which Spain is strongly committed.

[133] On the contrary, as evidenced in the energy crisis caused by the war in Ukraine, poor interconnection with our neighbours is one of the major weaknesses, which shall need to be addressed to increase, not only national energy security, but also within the EU.

Spain's Liquefied Natural Gas regasification capacity and nuclear capacity provide high flexibility and back-up capacity for renewable energies

[134] Migration is a phenomenon characteristic of mankind and is therefore one of the main mechanisms that have shaped today's societies. However, when it is highly intense over a short period or is used as a means of exerting pressure on neighbouring countries, it can become a serious security problem, most especially in **irregular migratory flows.** Indeed, they can become one of the main actions in a grey zone conflict.

[135] The main factors driving migration are the lack of subsistence resources, instability, conflict in their places of origin and the pull effect, fostered by the increasingly agile extension of cyberspace to places with fewer resources, thus promoting action in the cognitive domain. These circumstances are present in Spain's immediate geographical environment, whose southern border is particularly sensitive to this phenomenon.

[136] Although subject to fluctuations related to economic cycles, migration is a constant and growing phenomenon, as conditions in the countries of origin - especially the Sahel countries - are not likely to improve in the foreseeable future. Moreover, they may increase as a result of climate change, the rise of terrorism, demographic trends and growing regional conflict. This phenomenon can be used by certain actors as a means to exert pressure, slowing down or promoting mass mobilizations of migrants towards our borders at their convenience.

The main drivers of mass migration are to be found in the immediate geographical environment of Spain, whose southern border is particularly sensitive to this phenomenon

[137] **Emergencies and disasters** are unexpected situations that have a highly intense effect on the lives of citizens or the environment, with serious economic consequences. These phenomena may to intensify the effects of other threats, risks and challenges, creating situations that will foster them.

[138] When their cause is natural or accidental, and not the product of a hostile action, they are difficult to foresee and the response action is essentially reactive. However, it is possible to achieve an adequate state of readiness, in which the integration and interoperability of all means is of great importance to provide a rapid and effective response.

[139] As COVID-19 has shown, Spain is a country that is particularly sensitive to this type of emergency, both because it is a crossroads that brings together significant human movements and as one of the world's main tourist destinations. Preventative plans and sufficient reserves of resources to combat **pandemics** are essential, and comprehensive action by all national capacities is key.

Adequate readiness is required to provide a rapid and effective response to emergencies and disasters

[140] The effects of climate change are a driver of most of the challenges, threats and vulnerabilities identified in the National Security Strategy. It particularly affects the availability of resources, especially water, the proliferation of pandemics, extreme weather events and the intensification of migratory movements. It contributes to instability that can lead to failed states or cities, conflict, organized crime or terrorism.

[141] Thus, possible external theatres of operations that are now degraded may experience negative developments due to the worsening of the environment, increasing both instability and conflict and the living conditions of the troops displaced there. However, it does not seem likely to produce such significant effects on national territory in the period covered by this document. However, an increase in temperature, a reduction in rainfall, changes in winds and an increase in extreme phenomena that will affect the frequency and severity of emergencies and catastrophes are noted as impacts.

Climate change is an enabler of the challenges, threats and vulnerabilities identified in the National Security Strategy

Summary Table Chapter 1:

DRIVERS OF THE OE 2035

Definition of the Operating Environment

"Set of conditions, circumstances and influences, either fix or variable, affecting the employment of capabilities and decision-making, as they relate to the operation. The environment evolves with the intensity and speed with which these conditions, circumstances or influences evolve."
PDC-00

Characteristics of the 2035 Operating Environment

Mostly characterized by VUCA environments.

Volatility	Uncertainty	Complexity	Ambiguity
The increasingly frequent ocurrence of surprise and high-impact events and the capabilities of EDTs[13] make it difficult to identify trends or patterns.	The lack of certainty in the events to come creates an environment that is difficult to define. Hostile actions in the **grey zone**, AI or other EDTs, are challenges that are not without risk.	An environment characterized by a high number of interrelated factors. A **360º** and multidimensional spectrum, where **multi-domain** operations are integrated.	The difficult traceability of the authorship of attacks, especially in the cyber and cognitive domains, shall make it difficult to respond to actors who shall seek to exploit this weakness.

Geopolitical and social environment

The unipolar world led by the US has come to an end; its progressive military decline outside its borders has created security vacuums, which are being occupied by other actors. While it will remain the leader of the West, uncertainty shall increase due to its interest in the Pacific.

A multipolar world, with a growing bloc policy, with the US, China, the EU and Russia playing a leading role to varying degrees, with other state actors joining them. The leadership contest between the US and China is focused on trade, technology and economics, but has wider security implications.

Russia has been able to partially fill the strategic vacuum caused by America's voluntary withdrawal, especially in the Eastern Mediterranean, the Middle East and Africa. The recent invasion of Ukraine makes it difficult to foresee its future in the international environment.

Terrorism remains entrenched in the Sahel and the Middle East and is likely to expand again to other areas in Central and Southeast Asia.

13 EDTs: Emerging and Disruptive Technologies.

Military and security environment

Today, the dialogue-deterrence combination is an essential pillar in building stability and international relations, while only a limited number of states contemplate the use of the military instrument in their classical geostrategic conception.

Deterrence can be weakened by legislation that excessively limits the use of military capabilities and by a too reluctant political will to use them.

New forms of action based on global interconnectedness and the use of emerging technologies shall play a major role in conflict in the coming decades.

The pursuit of strategic objectives through actions in the grey zone leads to an ambiguous situation involving continued absence of peace without a full-fledged war.

Actions in the cognitive domain, enhanced by the use of cyberspace, primarily target the public, both opponents and their own.

New virtual confrontation scenarios are opening up, not forgetting outer space as an increasingly feasible and contested field of action.

Prominent role of technology-driven multi-domain conflict, with increased demands for speed in decision-making and response.

Challenges of the 2035 Operating Environment: Risks and Threats

Strategic and regional tension and its ultimate expression, armed conflict, is one of the most significant threats to national security.

Terrorism and violent radicalization, the possibility of action in the cyber and cognitive domains.

The influence of organized and serious crime and its interrelationship with terrorism.

Proliferation of weapons of mass destruction (WMD).

Spying and interference from abroad against national interests.

Cyberspace has brought about a technological revolution with consequences that are difficult to foresee.

Manipulation and disinformation campaigns turn cyberspace into a theatre of confrontation with direct implications in: land, sea, air and outer space.

Critical infrastructure.

Economic and financial stability.

Energy vulnerability.

Irregular migration flows.

Emergencies and disasters highlight the need to have plans and reserves in place to deal with them efficiently, as demonstrated by the pandemic.
The effects of climate change as a driver of challenges, threats and vulnerabilities.


L61


CS-30

CHAPTER 2

Operational scenarios for Armed Forces action

National Interests in the Security Environment

[142] The highest level of national interests are vital interests, that is, those which, if violated, would affect the very being of the nation and its survival. Article 8 of the Spanish Constitution states that "The mission of the Armed Forces [...] is to guarantee the sovereignty and independence of Spain, to defend its territorial integrity and the constitutional order". These interests can therefore be considered immutable.

[143] National interests in the security environment, within the framework of strategic interests, are directly linked to vital interests, since if the latter were violated, they would inevitably harm the former. It is up to the Government to decide what Spain's security interests are, and it will set them out mainly in the National Security Strategy and the National Defence Directive.

[144] National interests in the security environment, while mutable over time, tend to undergo little alteration. However, societal developments or major unforeseen events can make it necessary to redefine and prioritize these interests, as has happened to a large extent in the aftermath of the COVID-19 pandemic. Such events may lead to a temporary increase in the Armed Forces contribution to national resilience when facing crises of various kinds, using military assets for the benefit of civil society in emergencies. Although it is likely that there will be no profound changes in Spanish interests in the security environment in the period 2021-2035, these cannot be completely ruled out.

[145] The following are considered as National Interests in the area of security, as set out in the main documents that dictate the relevant[14] regulations:

---

14 Organic Law 5/2005, of 17 November, on National Defence, which develops in detail the constitutional missions of the Armed Forces; Law 36/2015, of 28 September, on National Security; National Defence Directive 2020; National Security Strategy; among others.

- **Interests concerning national sovereignty:** vital interests, linked to the mission of the Armed Forces, which guarantee the very existence of Spain as a nation, which is the protected asset. In this area, the military takes centre stage.
- **Interests necessary to achieve a stable international order of peace, security and respect for human rights:** strategic interests, necessary to obtain a stable security environment, which contributes to the defence of vital interests and exports our values as a nation. The Armed Forces shall be an important, but not the only, element in this international dimension.
- **Interests affecting the life, security, well-being and prosperity of the Spanish people**: interests, both vital and strategic, necessary for the State to guarantee citizens the appropriate conditions for them to develop their lives in peace and freedom. Maintaining a safe and secure environment is one of the State's main obligations. Given its capabilities and willingness to serve, the Armed Forces are an increasingly important element in preserving these interests, thanks to their contribution to the actions of other Power Instruments of the State.

Spanish legislation establishes the missions of the Armed Forces in the national interest

[146] The Armed Forces play a major role in safeguarding Spain's vital and strategic interests, through missions conducted in three different areas which, barring disruptive events that cannot be foreseen at present, shall remain stable until the 2035 horizon.

The Armed Forces' mission is to guarantee the sovereignty and independence of Spain, defending its territorial integrity and its constitutional order

[147] Three areas of action are considered for the Armed Forces and their use will be different in each. In the first, essentially within the framework of National Defence, the role of the Armed Forces is paramount, and entails employing all their capabilities and efforts. The military's specific potential actions are very different from those of any other State power, reaching, if necessary, high-intensity widespread combat.

[148] The role of the Armed Forces in the second area - projecting stability abroad - is very significant. Its work is manifested as a tool of the State used alongside others such as diplomatic, economic, cultural, etc., to build and preserve a stable and secure regional and global environment. The main ways in which the Armed Forces participate in this area are by integrating personnel and units into the command structures of International Defence and Security Organizations, in multinational peace support operations, *ad hoc* coalitions, partnerships or other international security cooperation activities. It may also be necessary to engage in combat, but normally at a lower level of intensity than in the previous area of engagement.

[149] Finally, the role of the Armed Forces in the third area of action is to contribute its capabilities to the National Security System. In these actions, the Armed Forces do not normally lead the process, but instead contribute their capabilities in close cooperation with the relevant authorities. The Military Emergency Unit (UME) is the element that is permanently dedicated to this area of action, although the entire Armed Forces may be used if necessary, depending on the severity and scale of the emergency, crisis or catastrophe. Situations requiring the participation of the Armed Forces may be more frequent.

Operational Scenarios of Action

[150] It follows from the above that the Armed Forces contribution to safeguarding vital and strategic national interests shall be made in three different areas, known as Operational Scenarios of Action. These contexts determine the situations and conditions in which the Armed Forces shall conduct the missions entrusted to them.

The Operational Scenarios of action make it possible to classify the type of operations that the Armed Forces shall have to conduct and the capabilities with which it must be equipped

[151] The contexts are not mutually exclusive. In fact, simultaneous action is envisaged in all of them, according to various missions and tasks. Therefore, perhaps the most demanding position for the Armed Forces would be needing to deal simultaneously with significant threats in all three contexts, which could overwhelm their capabilities.

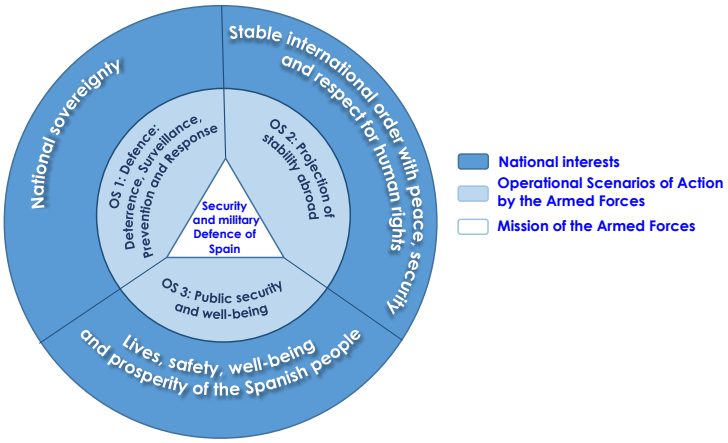
The Operational Scenarios considered are the following[15]:

- Operational Scenario (OS) 1: MILITARY DEFENCE (DETERRENCE, SURVEILLANCE, PREVENTION AND RESPONSE)
- Operational Scenario (OS) 2: PROJECTION OF STABILITY ABROAD
- Operational Scenario (OS) 3: PUBLIC SECURITY AND WELL-BEING

[152] The relationship between Operational Scenarios and national interests in the security environment is visualized in the table below:

---

15 Ibid. notes 1, 2, 3 and 4.



OS1. Military Defence (Deterrence, Surveillance, Prevention and Response)

OS1. Military Defence (Deterrence, Surveillance, Prevention and Response)

[153] It is the main Operational Scenario of action. It is here that the Armed Forces conduct their fundamental mission, and it is their reason. It is therefore the most demanding context, where it may be necessary and possible to engage in high-intensity combat. If required, the Armed Forces shall apply all their capabilities to guarantee the sovereignty and independence of the nation, its territorial integrity and its constitutional order. In this context, autonomous defence capability is essential.

To guarantee the sovereignty and independence of Spain, its territorial integrity and constitutional order, the Armed Forces shall apply all their capabilities

[154] The Joint Doctrine for the Employment of the Armed Forces PDC-01(A) sets out the two ways in which this mission shall be executed. If an external threat or aggression arises, it shall be executed through military prevention and response operations. This defence can be conducted either autonomously or in the collective defence environment within the EU or NATO framework. However, even in the latter case, an autonomous defence capability is essential to be able to react immediately to aggression, allowing time for collective defence mechanisms to be activated effectively. In either case, the availability of a credible military force, and the willingness to use it if necessary, is essential.

[155] In the event of possible internal challenges to national sovereignty, constitutional order or territorial integrity, Armed Forces support may be required to resolve them.

[156] Spain's membership of the main ISDO represents a security guarantee, since it obliges the rest of the allied nations to collaborate in preventing aggression or threats. Likewise, it also obliges Spain to collaborate in solidarity to defend any of its allies that are threatened or attacked, providing its share of the required capabilities. In the case of NATO, this occurs by invoking Article 5 of the Treaty, and in the case of the EU Article 42 of the Treaty of the European Union, which explicitly sets out the principle of collective defence. The European quest for greater strategic autonomy, and the expected Defence budget increase, will most likely enhance the EU's security dimension. However, this will continue to rely primarily on the necessary cooperation and understanding with NATO in OS1, as well as on the indispensable capacity for autonomous defence.

[157] In this Operational Scenario, the permanent missions of the Armed Forces play an essential role, maintaining an active alert to deal with any threat to security regarding sovereignty and national interest. With a permanent and purely national character, the Joint Force guarantees these missions to maintain presence, monitor, provide security and control in the land, maritime, aerospace and cyberspace areas of sovereignty and national interest.

[158] They have a deterrent and preventative function, not only nationally, but also contribute to allied deterrence, as well as enabling a first reaction to hostile actions in any field. Effective deterrence, the sum of having the proper capabilities and the will to use them, is a guarantee of peace and stability.
Although this OS encompasses all areas of operation, both physical and non-physical, it is considered that the dynamics in the traditional physical domains shall be maintained over time, although they will all be subject to the dizzying technological progress underway. Thus, artificial intelligence, robotics and autonomous systems with lethal capabilities shall assume a much greater role and scope.

[159] At the same time, the concepts of deterrence, surveillance, prevention and response shall undergo important innovations in the global spaces that make up the cyberspace and cognitive domains and will therefore be conducted as multi-domain operations. Their special characteristics make these immaterial domains scenarios where the traceability and attribution of hostile actions and aggressions are difficult. Moreover, they may come from state actors as well as non-state groups or even lone individuals. Therefore, current deterrence and prevention capabilities are limited and need to be developed to adapt to the new challenges.

The concepts of deterrence, surveillance, prevention and military response shall undergo major innovations in the cyberspace and cognitive domains

[160] Thus, while deterrence, surveillance, prevention and response actions provide some security, in the non-physical operating domains, because they are difficult to trace and attribute, the adversary is capable of attacking at a time and place of its choosing. In these areas, it will be necessary to set out the threshold of conflict, deterrence, prevention and gradual military response, specifically with regard to hostile activities in the non-physical operating domains.

[161] For conflict in the grey zone, referring to the type of conflict that is neither an open confrontation nor a state of full peace, the technical and legal shortcomings and gaps in the non-physical domains have a great impact. It is in this field that this type of aggression shall move, which makes it very difficult to detect and neutralize. It is therefore very necessary to develop broad knowledge of this type of conflict, making it possible to anticipate and avoid, as far as possible, merely reactive actions.

[162] This state or situation could be described as permanent competition. Thus, specifically, it shall be necessary to design proactive national strategies - not exclusively military - that will make it possible to identify the vulnerabilities of the potential adversary, exercise deterrence on them, prevent them and, if necessary, to act in advance. This concept, which reality is beginning to be imposed upon us, shall profoundly alter our current concept of national defence.

[163] The operations and missions managed within OS1 shall be conducted in the land, maritime and aerospace domains, as well as in a cross-cutting manner in the cyberspace and cognitive domains, generally adopting a multi-domain nature. The cross-cutting nature of the non-physical domains shall allow them to act as multipliers or enablers of military operations in all physical domains. These multi-domain operations are likely to take place in a context of both conventional and hybrid conflict, as the current and future development of technology gives the latter mode of action capabilities and possibilities never before available.

[164] However, it is important to note that armed conflict remains one of the most significant threats to national security. If they were to occur, they would be highly demanding in terms of intensity for the Armed Forces, and all human and material resources, both military and non-military, will have to be committed. This makes it necessary to always be prepared for such an eventuality, and otherwise it would encourage potential adversaries to use military force against Spanish national interests. Being continuously prepared to deal with such a conflict is the basis of the required national military capability and an essential part of deterrence.

[165] The Armed Forces capabilities, and their willingness to use them when necessary, constitute deterrence. If the adversary is uncertain that their confrontation shall succeed or is certain that it will lead to a rapid and forceful response, with an outcome contrary to his interests, it will not act. Therefore, maintaining the capacity and willingness of our Armed Forces to act is essential for effective deterrence and is the key to defence in peacetime.

[166] While armed conflict between powers cannot be ruled out, proxy wars are more likely, in which third states, using state or non-state actors, would seek to employ conventional, non-conventional or hybrid strategies to destabilize, delegitimize or affect national interests.

[167] With specific reference to the cyberspace operating domain, its importance grows as globalization advances. The increasingly complete interconnection of systems, people and things through the internet makes all nations, including Spain, both more powerful and more fragile. This vulnerability stems from the dependence on IT connectivity in all strategic sectors: energy, finance, healthcare, food logistical chains, emergency services, etc.

Thus, the power of large technology companies, especially manufacturers of operating systems, hardware and widely-used network infrastructure, which can easily block a state's supply chain, should not be ignored.

[168] Since acting in cyberspace is relatively simple, both the actors with the capacity to act in it and the targets worth attacking and available to them are multiplying. The same is true in the cognitive domain. Thus, while conventional hostile actions are not likely to occur in Spain's immediate security environment, aggression in both spheres is not only highly likely, but occurs daily, in increasing volume and to create instability or internal chaos in society.

[169] Cyberattacks could be caused by three different actors: States, organized groups (terrorists, criminals and hacktivists) and isolated individuals. The targets of cyber-attacks shall be the networks and systems of the Armed Forces and defence, but also those that are potentially less robust. The systems of other public administrations, critical infrastructure and essential national services are always susceptible to attack, to cause serious economic damage and/or generate instability and internal chaos.

[170] In the cognitive domain, the main focus shall not be on the Army, Air Force and Navy, but on the hearts and minds of individuals. It is increasingly likely that, by 2035, actions in this area will predominate for two main reasons:

- Because of the **need of support for the government's use of the military**. The government will need to win the support of society through a greater communication effort based on a prior "detoxification" of information. The Armed Forces, under the leadership of the government, shall therefore have to strengthen strategic communication at all levels.
- Because our potential adversaries know the **strategic value of shaping and conditioning public perceptions in pursuit of** their political objectives. These actions do not necessitate investing large sums in sophisticated weapon systems and they avoid being subject to the rejection of the international community, since they use less violent, albeit more efficient, methods. The most dangerous of these actions include the disruption of electoral processes, the promotion of nationalism and independence, and the financing of radicalized and violent groups or organized crime networks.

[171] To win the battle of narratives, the Armed Forces, closely coordinating with other branches of government, must be able to conduct operations in the cognitive domain. Through multiple means, acting both autonomously and as part of multinational forces, they must be able to counter the adversary's narratives with their own, actively, immediately and while trying to maintain the initiative. At all events, the involvement and leadership of the highest level of the nation in the narratives battle is essential.

The fields of operation have expanded into cyberspace and cognitive domains. Operations in both should be influential in the design of future Armed Forces

[172] Therefore, it can be affirmed that OS1 shall find itself being continuously deployed, not only due to undertaking the Armed Forces permanent missions, but also due to an uninterrupted succession of non-conventional aggressions to national interests and security. Indeed, the latter shall most likely be the predominant, though not the sole, means of action in the conflict of the 2035 environment, and hence there is a strong need for the ability to lead and direct in terms of military strategy.

[173] The geographical scope of application of OS1 shall remain Spain, as well as maritime and aerospace areas of priority interest for national security. Having two archipelagos separate from the mainland and sovereignty over North Africa makes it essential to maintain a favourable military situation. To this end, control of maritime and air lines of communication with these territories is a priority, which makes it necessary to consider A2/AD scenarios.

[174] In conclusion, Operational Scenario 1 is in a moment of transition. It shall remain essentially military but shall increasingly need to collaborate with other state capabilities, both public and private, to ensure its success from an integrated perspective. The Armed Forces are generally more resilient than the rest of Spanish society due to their nature and means, but its chances of success in the strategic

framework of its military defence mission shall depend to a large extent on its ability to equip itself with new technologies that enable multi-domain operations and allow it to contribute effectively to the nation's overall resilience.

OS2. Projection of Stability Abroad

[175] This second Operational Scenario, or OS2, refers to the national interest in contributing, together with our partners and allies, to international security and to defending our values in fulfilling our commitments. This is the framework for Spain's contribution to building and maintaining a stable international environment of peace, security and respect for human rights. This context includes the activities of the Armed Forces aimed at protecting its strategic interests, and includes combat if necessary.

[176] This context may not be as decisive as OS1 and OS3 for the very survival of the nation, or for the survival and well-being of its citizens. However, having a stable environment, with values common to our own, democratic values and respect for international law and human rights, makes the actions conducted in this context a net contributor to national security and prosperity, as well as to defending national strategic interests.

Stability projection actions abroad contribute decisively to national security and prosperity

[177] It is a variable context. Their actions often take place in a multilateral context, but may also be bilateral, at the request of a nation that feels its stability and security are being threatened. National participation can be effected under the umbrella of one of the ISDO to which Spain belongs, or through an *ad hoc* coalition formed specifically to address the security problem in question. The most demanding operations in this context would most likely be those that are within the framework of collective defence, in which the Armed Forces would have to intervene as a result of aggression suffered by an ally. These would fall within the framework of the agreements and treaties signed by Spain and the organizations to which it belongs, of the coalitions in which Spain may join to defend its national interests or in response to requests for assistance from friendly countries.

[178] Less demanding crisis response operations (CRO), usually involving low- to medium intensity environments, are also possible and so far more frequent. By contrast, they can be very protracted, requiring a very considerable long-term effort. On the other hand, military support and assistance operations are increasingly frequent and contribute significantly to increasing Spain's prestige.

[179] In the foreseeable Operating Environment of 2035, given the large number of emerging challenges, increased international competition and ongoing rearmament, a trend towards closer international cooperation is to be expected. This shall require a readjustment of this cooperation, particularly in view of the expected further development of the defence pillar in the EU. However, not updating the decision-making mechanisms of various ISDO, as well as recent experiences such as the withdrawal from Afghanistan, or the invasion of Ukraine, make it necessary to review the mechanisms for activating and executing this international cooperation to be truly efficient.

[180] The inclusion in the international corpus of norms covering the responsibility to protect, which obliges international intervention in a country's internal affairs in the event of genocide, war crimes, ethnic cleansing or crimes against humanity, is an example of one of the great advances of the 20th century in this context. However, progress such as this may be rendered *de facto* inoperative by growing bloc politics, the decision-making mechanisms still in place in the Security Council, or by the unaffordable cost of an operation that may not guarantee an acceptable outcome. Therefore, despite the obligation to provide the legitimacy granted by the UN Security Council resolutions, *de facto* situations are likely to arise in which military operations or missions are launched based on the leadership of the power whose interests are most threatened, with the support and participation of its partners and allies through *ad hoc* coalitions.

[181] In a more unstable and unsettled world than in past decades, it will probably be necessary to prioritize participation in missions and operations as part of OS2. Those that could most intensely affect Spain's immediate security environment or our interests, areas of priority interest, or those led by our main partners and allies, will be given the highest priority. However, although less likely, participation in missions in

any geographical area cannot be ruled out, so the capacity for global projection shall remain a key capability for the Armed Forces.

[182] The european eastern flank and our southern border, the area between the North African coast and the Gulf of Guinea, are the most likely areas where stability and security projection missions can be conducted most frequently and intensely. Apart from geographical proximity and economic interests, the ease with which the problems plaguing the African continent can easily affect Spain, underline this reality. Irregular migration, which is expected to increase significantly in the future, as well as other associated criminal activities, are clear examples.

[183] It should not be forgotten that the current instability and conflict in the Mediterranean and the Middle East will continue for a long time. These scenarios are highly likely to prolong ongoing missions, hence the contribution to other missions that may be undertaken will have to be balanced, like our military presence in Eastern Europe.

[184] In these spaces, as in any other where it is necessary to act, it is very important to strengthen knowledge of local cultures, to respect them and to make efforts to involve them in the motives and values of the operation. In these environments, the contribution of women to conflict resolution has proven very valuable. Since they are capable of intermediation that is often denied to male members of the deployed contingents, the participation of female personnel in this type of mission and their

training for interaction with the local female public may have a differentiating and substantial importance.

It is important to strengthen knowledge of local cultures, respect them and make efforts to involve them in the motives and values behind the operation

[185] The phenomena of organized crime, terrorism and irregular migration, associated with the fragility of the states in the African region, only underscore the importance of maintaining the capacity for national projection in the region, in terms of leadership in a multilateral framework if necessary or, in particularly critical situations, unilaterally.

[186] Thus, Spain should contribute to strengthening Europe's strategic autonomy, with a special focus on its southern border and in coordination with NATO's southern approach. It is difficult to envisage the EU becoming a global security provider - rather, it is limited to its immediate security environment - which is why it is necessary to increase the effectiveness of EU missions in Africa and Eastern Europe. A major international cooperation effort is essential in all fields, not only to rebuild the security structure, but also comprehensively in cooperative security, procuring an implementation of political and economic structures that improve

development and the quality of governance in the proximities of Europe, from an integral perspective.

[187] Without significant progress in these areas, we can expect a proliferation of military operations in Spain's immediate security environment in the coming years. When the combined effects of climate change and the African demographic explosion are greater than they are today, the fragility of the states in the area and the pressure on Southern Europe will foreseeably increase. Similarly, the role to be played by the EU in the reconstruction of Ukraine and the stabilization of its eastern border will be very important.

[188] Humanitarian disasters are not always linked to the resolution of a more or less intense armed conflict. Those related to natural disasters (earthquakes, tsunamis, floods, fires, etc.), which are highly unpredictable due to their own causes, are also important. Often, the Armed Forces will not lead the intervention but will always be a facilitator of aid, especially in the first phases after the disaster. Nor should it be forgotten that, on certain occasions, international aid will only be possible if it provides a solid security element that allows other elements of the government, aid workers, the Red Cross, etc., to carry out their tasks.

[189] As with OS3, although internally, the Operational Scenario of international stability projection involves relations, coordination and cooperation with a very broad spectrum of actors. These range from local authorities, ISDO, military and civilian representatives of other contributors, NGOs, aid workers, and even, increasingly frequently, contractors for auxiliary services that the mission may require. All these participants make for a complex scenario, where the good work and capacity for empathy that characterize the members of the Spanish Armed Forces are highly important values. These qualities not only produce a better international image, but also provide added value in terms of the deployed contingent security.

[190] In conclusion, it may be stated that this OS2 is highly significant for Spain. Firstly, and fundamentally, because of its contribution to national security, since membership of the ISDO is a major deterrent factor. Secondly, because the excellent performance of the Armed Forces in international missions in which it participates lends prestige to Spain and helps place it in the position it deserves on the international board.

[191] However, it must be considered that there will be other security missions that shall have to be tackled autonomously and as a priority, when membership of these ISDO does not guarantee that they will be fulfilled. These efforts will basically be a consequence of our geographical location (North Africa, Gulf of Guinea or Sahel) and our historical context (Latin America) and are included in the Defence Diplomacy actions that include Cooperative Security activities.

[192] It is important to maintain these Cooperative Security activities, as they are complementary to those of organizations such as the EU and NATO, contributing significantly to Spain's prestige and interests in the region.

[193] These Cooperative Security activities may be conducted by the Spanish Armed Forces bilaterally in priority countries for Spanish external action. Their purpose shall be to strengthen military capabilities so that these countries can thereafter be self-sufficient in security matters. Preventative efforts with our neighbours in the diplomatic, economic, policing and military spheres are of paramount importance for national security, to address the four elements considered fundamental for the stabilization and security of the area: development aid, improvement of security and defence structures, human rights and governance.

[194] Also included in this Operational Scenario is the need to evacuate Spanish residents abroad when instability in another country place their lives or interests at serious risk, in what are known as Non-combatant Evacuation Operations (NEO).

[195] An added advantage of this type of mission abroad is the positive perception that our Armed Forces achieve in Spanish society, which recognizes them as an instrument of peace and international stability, and that they contribute decisively to maintaining public support for the military institution.

These missions are perceived positively by Spanish society, which recognizes them as an instrument of peace and international stability, and they help maintain its support for the military institution

[196] Finally, as with OS1 and OS3, there is a need to balance the allocation of resources and capabilities among the foregoing Operational Scenarios and Overseas Stability Projection OS2.

OS3. Public security and well-being

[197] This is the context of the Armed Forces contribution to the National Security System. In a social and democratic state governed by the rule of law, as the Constitution provides, its main commitment to its citizens is to provide the security environment necessary for them to live their lives in peace and prosperity. In the aforementioned commitment, the capabilities and actions of the Armed Forces may be essential in particularly serious or critical circumstances.

The state's primary commitment to its citizens is to provide the security environment necessary for them to live in peace and prosperity

[198] The permanent presence and availability of the Emergency Military Unit is the Armed Forces' main contribution in this environment. This contribution to the State's action to support its citizens may be supported by the participation of the rest of the Armed Forces in major disaster situations.

[199] The military's involvement in the regulations covering and institutional architecture of public security is consolidated mainly through Law 17/2015, of 9 July, on the National Civil Protection System and Royal Decree 1097/2011, passing the UME Intervention Protocol.

[200] The aforementioned new hostile forms of action, mainly in the intangible spheres of operation, while conceptually falling under OS1, may trigger disasters that clearly fall under OS3. Cyber-attacks on critical activities and infrastructure would directly affect citizens as a whole. These actions shall require the contribution of the means and capabilities of the entire Armed Forces, supporting the civilian authorities, to resolve the crisis. In the case of health emergencies, the participation of the Military Health Service, as a specific contribution to the National Health Service, is another essential aspect.

[201] The possible influence of climate change, which would increase the number and intensity of extreme meteorological phenomena, may require more frequent intervention by the Armed Forces to support the public, with resources exceeding those of the UME. The Armed Forces possess characteristics and capabilities that are useful in these situations, including transporting personnel and materiel, rea-

ching locations that are difficult to access, providing telecommunications where they do not exist or have been lost, planning and training their personnel, discipline in their actions, self-sacrifice and a permanent commitment to serve the public.

[202] Both civilian authorities and citizens themselves are increasingly aware of these capabilities. This perception, together with the increased likelihood of major disasters, leads to the expectation that the contribution of the Armed Forces in scenarios considered within this OS3 may become more frequent.

[203] In view of this, for the Armed Forces to be able to contribute along with the rest of the instruments of the State in these missions, the creation of coordination and action procedures seems unavoidable.

The mission to protect the lives and well-being of citizens shall require a higher degree of readiness and the generation of Armed Forces procedures to fulfil them

[204] Actions in this OS3 are particularly well regarded by the public as a whole. In a national context of a false sense of absence of threat, it is very positive that the Armed Forces show themselves to be close and useful to citizens. However, it is necessary to bear in mind that this situation raises a potential problem in a society like Spain's, where there is little culture or awareness of defence, even in the Government and Civil Service. This problem consists of considering the Armed Forces a highly useful multi-purpose tool, whose recurrent use dilutes their reason as the main force responsible for Spain's military defence, and whose main form of action is combat.

[205] None of the operations or activities detailed in this OS3 are an exclusive function of the Armed Forces, but rather work conducted by the Armed Forces on an ad hoc basis, complementary to the essential work conducted by other Instruments of the State.

[206] Similarly, a greater degree of participation in the National Security System, defined as a set of bodies, resources and procedures that operate in a single structure, shall be essential. Thus, the competent bodies in the area of National Security shall be able to assess threat, crisis or disaster factors and situations, gather and analyse information for decision-making in crises, detect needs and coordinate all actions, both inter-ministerial and private sector.

[207] This greater involvement of the Armed Forces in the National Security System may require the design and implementation of periodic exercises with a sufficient level of ambition to practice and refine common procedures and coordination mechanisms in advance.

[208] This Operational Scenario of action shall be developed mainly in national territory, although actions abroad shall also be possible. One example would be to assist Spanish citizens residing or passing through areas affected by emergencies or disasters, in agreement with the local authorities. Another would be in extreme situations, when the local authorities affected are overwhelmed by the magnitude of the disaster and request international assistance to safeguard their citizens as far as possible. This

type of action can take the form of bilateral requests, in the context of European solidarity or through ISDOs managing the emergency multilaterally.

[209] This second modality of external intervention, within the scenarios that fall under OS3, is intermingled with those previously considered in OS2. Again, the boundaries between the three Operational Scenarios of action are partially blurred, as indicated above.

[210] Beyond their participation in disaster or emergency situations, the Armed Forces make other very valuable contributions to State action. These take the form of highly complex technical tasks, requiring both highly specialist personnel and equipment, conducted with a high degree of rigour and safety, and which bring multiple benefits to society. They include areas such as oceanography, hydrography, cartography, aerial photography, radio-aid calibration, fishing inspection, protection of underwater heritage, environmental protection, VIP transport, collaboration with the security forces, etc.

[211] One tool available to the Armed Forces, which has not been sufficiently explored and exploited in Spain to be able to provide the best response to emergency situations or major disasters, is that of reserve. With a high incidence in other Armed Forces in our geographical and cultural environment, it has shown its usefulness in Spain on an ad

hoc basis and in very specific areas. Further evolution and development of our military reserve could make its contribution more significant in the OS3 environment.

One tool that has not been sufficiently explored and exploited in Spain to provide the best response to emergency situations or major disasters is the military reserve

[212] In conclusion, just as the previous concept of conflict could be placed in a defined time frame, the current one exists in a context of permanent competition, with periods of greater or lesser activity or severity of the actions conducted, within a general framework of the conception of National Security as a comprehensive system.

[213] Thus, it can be assured that the OS3 shall also be permanently activated. In short, the Armed Forces shall be one of the main elements of national resilience, not only contributing decisively to it, but also promoting its reinforcement in society as a whole.

The Armed Forces are one of the main elements of national resilience, which can contribute to strengthening national resilience in society as a whole

Summary Table Chapter 2:
OPERATIONAL SCENARIOS FOR THE ARMED FORCES ACTION

National Interests in the Security Environment

The highest level of national interests are vital interests, that is, those which, if violated, would affect the very being of the nation and its survival.

It is up to the Government to decide what Spain's security interests are, and it will set them out mainly in the National Security Strategy and the National Defence Directive.

The following are considered:

- **National sovereignty interests.**
- **Interests necessary for a stable international order of peace, security and respect for human rights.**
- **Interests affecting the life, security, well-being and prosperity of the Spanish people.**

"The Armed Forces have the mission of guaranteeing the sovereignty and independence of Spain, defending its territorial integrity and its constitutional order."

Operational Scenarios of Action

These contexts determine the situations and conditions in which the Armed Forces shall execute their mandated missions. The contexts are not mutually exclusive; simultaneous action is planned for in all of them, through various missions and tasks.

OS1: Military Defence (Deterrence, Surveillance, Prevention and Response)	OS2: Projection of Stability Abroad	OS3: Public security and well-being
– It is the main Operational Scenario of action. It is here that the Armed Forces conduct their fundamental mission and it is their raison d'être. – Autonomous defence capacity is essential. – The concepts of deterrence, surveillance, prevention and response shall undergo major innovations in the cyberspace and cognitive operating domains, taking the form of multi-domain operations. – OS1 is in transition, although it shall remain essentially military, it shall need to collaborate with other state and public-private capabilities to ensure success.	– **Spain's contribution** to building and maintaining a stable international environment of peace, security and respect for human rights. – It is a **variable** context. Its actions often take place in a **multilateral** setting, but can also be **bilateral**, at **the request** of a nation that feels its stability and security are being threatened. – In the future OE, it is to be expected that there shall be a trend towards closer international cooperation. – Spain should contribute to strengthening Europe's strategic autonomy, with a special focus on its southern border and in coordination with NATO's southern approach, avoiding excessive attention to Western Europe.	– The contribution of the Armed Forces capabilities to the National Security System. – The capabilities and actions of the **Armed Forces** may be **indispensable** in serious or critical circumstances. – The contribution of the Armed Forces in such OS3 scenarios, at the request of civilian authorities, shall be **increasingly frequent**. – There is a need to establish **procedures** for **coordination** and **action** across the instruments of the State and the Armed Forces to articulate these missions. – Further evolution and development of the military **reserve** could make its contribution to OS3 more relevant. – The Armed Forces shall be one of the main elements of **national resilience**.
"The Operational Scenarios of action make it possible to classify the type of operations that the Armed Forces must conduct and the capabilities with which they must be equipped."		

CHAPTER 3

Armed Forces adaptation to the OE 2035

Characteristics of the Armed Forces in 2035

[214] So far, we have described both the environment in which the Joint Force shall operate in the coming years and the Operational Scenarios in which it shall undertake its missions. The content of this last chapter focuses on drawing conclusions; it proposes the characteristics that the Armed Forces of 2035 should have and shows the main challenges and opportunities it shall face to achieve these characteristics.

[215] The range of missions and operations they shall have to conduct shall be very broad, both as regards the types of operations and missions and their gradation, the size and composition of the contingent involved and the intensity of the actions. It is therefore necessary to be prepared to, simultaneously, to conduct conventional missions, to intervene in a cross-cutting manner in aspects that may affect National Security, to comply with the international commitments that Spain assumes for the benefit of international peace and security and, frequently, to contribute to the security and well-being of citizens. This shall all take place in a more intense and accelerated time pattern than at present, ultimately sketching a matrix of availability, effort and continuous demands placed upon the Armed Forces.

[216] Therefore, the organization and the people who constitute the Armed Forces must seek to achieve the greatest possible degree of strategic agility, which requires understanding the situation; conducting operations at the operational level; and rapid execution at the tactical level. The ability to adapt and respond quickly, effectively and efficiently to a wide range of unpredictable situations and potential adversaries shall be the factor that determines success in the future Armed Forces.

[217] Information readiness and management shall be the key element, as shall a military strategy capable of anticipating events. Anticipating one's own actions as far as possible shall avoid a chain of responses to situations that are already underway and which provide a strategic surprise for the adversary. A high degree of anticipation shall provide the initiative and strategic advantage that shall allow the conflict to be resolved favourably.

[218] It is therefore desirable to have a single, comprehensive and multi-domain national system of indicators and alerts, as set out in the National Security Strategy 2021. Its purpose is to detect hostile actions in the grey zone early in a context of possible hybrid conflict, since this is the most likely scenario. Although the AFs do not lead or manage the system, their contribution must be very significant.

[219] Several qualities shape the credibility of national military power:

- **High combat capability**: with the aptitude necessary to fulfil the combat missions required, in their moral, intellectual and physical components. This must be reflected in the confrontation superiority with our potential adversaries.
- **Balance**: to be effective and to be able to cope with future risks, a balance must be struck between the capacities to act in the five operational domains envisaged.
- **Multi-domain integrated**: able to act effectively in a conflict in which the aforementioned fields of action are interrelated and simultaneous, forming a single, multifaceted environment.
- **Response Capability**: to identify and respond to unexpected circumstances, which requires anticipation and sufficient force availability to operate when required, as well as high readiness to be deployed when and where required. Units will need to be at the right level of readiness to operate within increasingly demanding timeframes.
- **Strategic mobility**: to ensure the deployment, projection and sustainment of our force, it is necessary to have the appropriate means of transport for the mission. The trend towards increased instability outside our borders will make it recommendable to enhance the rapid projection capacity of contingents of different sizes. A sufficient degree of strategic mobility is also essential to defend our national territory, given its dispersed and discontinuous nature.
- **Viability**: credible military power requires a viable force with the means to fulfil missions. To this end, the Armed Forces must enjoy the necessary financial resources, sustained through time and according to their needs. The lack of financial resources would diminish the credibility of the Armed Forces, especially in the most serious crises that are potentially harmful to national interests. Efficient management of human and material resources will be a prerequisite for achieving the desired effects with the force and capabilities that are strictly necessary.
- **Readiness and sustainability**: to ensure their rapid and effective response to any situation, for as long as and at the level of readiness and intensity the situation demands. This shall enable it to maintain an effective presence in the theatre for as long as necessary.
- **Versatility**: to be able to respond quickly and effectively to a wide variety of threats, situations, environments and missions. Even those that could not have been anticipated. It requires flexibility to have various alternatives available in different situations, when the results obtained or new situational changes make it recommendable to move among the available options, rapidly forming contingents that are modularly adjusted to ensure effective mission fulfilment.

- **Resilience:** to overcome unfavourable situations, to maintain its capacity to act in degraded environments and to show an unwavering will to win. Elements that could contribute to the resilience of the Armed Forces would be the redundancy of capabilities, the availability of reserves and sufficient national industry to meet its most critical needs.
- **Innovation and adaptability**: to generate or develop new organizations, capabilities and doctrines that make it easier to achieve the assigned tasks. Constantly evolving, adapting its mentality, organization, processes, structure, etc., without the processes of adaptation ever entailing a reduction in the capabilities or availability to tackle the missions entrusted to it. Adaptation should never mean abandoning the essence and values that guide the actions of the Armed Forces.
- **Interoperability**: to interact within the joint scope of our own Armed Forces and to support civilian authorities in situations requiring it, with the AFs of allied countries, enabling them to integrate into and contribute to the full range of missions assigned to it in a multi-domain and multinational environment. This concept refers not only to equipment, but also to education, training and procedures.
- **Moral fortitude**: to internalize the missions entrusted to them, with self-sacrifice, loyalty and determination. The Armed Forces must be an example of permanent dedication to the service of the nation, based on a set of values which, as set out in the Royal Ordinances for the Armed Forces, must be observed, promoted and demanded, because they constitute the basis and foundation of our daily work.

A necessary change

[220] New technologies and ways of waging war are causing accelerated changes in Security and Defence paradigms. They are profound enough to bring about, in turn, significant changes in the organizations responsible for guaranteeing security. And they shall become even more so in the years to come. On the other hand, change is a necessity if organizations are to be up-to-date and dynamic.

[221] Unlike in the past, the changes underway shall not bring about a period of stability after their implementation, but, on the contrary, shall lead to an even greater acceleration of innovation. The Armed Forces, large and complex organizations with a long history and a vast organizational culture, change requires a constant process of adaptation, which puts them under severe stress.

[222] The changes underway are so far-reaching and rapid that even constant adaptation may not be sufficient in certain areas, and decisions must be taken that entail a genuine transformation of these areas. However, transforming does not involve a break with accumulated experience, nor an essential alteration of the missions and nature of the Armed Forces, which shall be maintained in the OE 2035.

[223] What will guarantee the success of the Spanish Armed Forces in the coming years shall be to adapt constantly to the new Operating Environment: the personnel who form part of it, their ideas, the tools at their disposal and of the organization itself, without ruling out more profound developments in areas that are identified as more innovative or disruptive.

[224] Perhaps the greatest challenge of the ongoing change process is to pace it in the identified areas: personnel, ideas, tools and organization. Simultaneous adaptation at similar rates offers synergy, efficiency and effectiveness, while becoming a driver of continuous adaptation. This is difficult to achieve, as the incorporation speed of new tools is currently faster than the ideas development speed or the profiles of those joining the Armed Forces. A greater and more dynamic flow of personnel between the Armed Forces and civil society is likely to be necessary, especially in areas of major technological innovation.

[225] As regards organizational change, in institutions such as the Armed Forces, which have a long history and a certain inertia, and which are subject to a long list of state regulations that generate bureaucratic servitude, the pace of adaptation may not adapt to the necessary changes.

[226] These changes cannot occur exclusively in a military environment but must be synchronized with those of the nation and its institutions as a whole. In this regard, citizens' perceptions of the daily presence of risks and threats and the need to make sacrifices to preserve their security must evolve.

Changes in the conception of security cannot occur exclusively in a military environment but have to be synchronized with those of the nation and its institutions as a whole

Challenges and opportunities

[227] The Armed Forces' process of evolution, which ensures, in the 2035 environment, the aforementioned qualities, means a set of undeniable challenges, but also unquestionable opportunities. National security and defence require meeting these challenges, taking advantage of the many opportunities to make the Armed Forces more effective in a changing world. The speed of change in the security environment, makes it necessary to minimize misdiagnosis, while demanding implementation of necessary changes that cannot be delayed in a number of areas.

[228] However, the evolution must be pragmatic, in an enabling environment that is ambitious but within the reach of national resources. To systematize the description of the perceived challenges and opportunities, the main aspects to be modified are articulated around the **DOTMLPF-I** factors (Doctrine, Organization, Training, Materiel, Leadership, Personnel resources, Facilities, Interoperability). However, we must not lose sight of the fact that many of the elements are cross-cutting or at least interrelated.


GENERAL DYNAMICS
European Land Systems
Santa Bárbara Sistemas
TRACTORA DE LA INDUSTRIA DE DEFENSA
SAPA Placencia
SDLE
VCZAP
GENERAL DYNAMICS
European Land Systems
Santa Bárbara Sistemas
GENERAL DYN
European Land Systems
Santa Bárbara Sistemas
SASCorp
Structural Aerospace Systems

Materiel

[229] The materiel factor shall be dominated by technological innovation and experimentation, which are already an intrinsic part of military strategy. The most advanced technologies are increasingly available to multiple actors, and hence significant technological disadvantage will be difficult to counter and shall in turn amount to a decisive operational disadvantage in the confrontation. Technological superiority must be one of the most important drivers of change, and shall remain one of the most important elements of the Operating Environment in 2035, while also bearing in mind the need to remain interoperable with our allies.

[230] The competition for technological advantage in the areas covered by the Defence Technology and Innovation Strategy (DTIS) 2020 is crucial. These technologies include artificial intelligence, quantum computing, information management, aerospace systems, directed energy weaponry, combat cloud, operational integration of manned and unmanned vehicles, cyber weapons, big data, robotics, energy generation and storage, metamaterials and advanced manufacturing techniques, non-lethal capabilities, etc., with a strong focus on potentially disruptive technologies.

[231] Technology alone is not decisive unless it is strongly linked to the evolution of doctrine and training. In the military domain, the application of disruptive technologies shall cause operational changes, with organizational consequences, coupled with profound doctrinal and strategic changes.

[232] Although the costs of technology have generally fallen, applying the most advanced technologies to military equipment and weapon systems entails a notable increase in their acquisition, sustainment and operating costs. It shall therefore be necessary to plan properly those weapon systems the Armed Forces need to be able to meet future challenges in relation to the resources envisaged. The planned increase in the budget allocated to defense must therefore be carefully prioritized and oriented towards capabilities that will ensure superiority in warfighting and the effective integration of new forms of action in a multidomain environment.

[233] Most of the technologies that shall be fully deployed in 2035 are already present at various stages in their development, although many of them shall obviously have reached a higher degree of maturity and applicability than today, hence the opportunity to make them and their further developments available cannot be missed.

[234] In parallel, the constant acceleration of time driven by the technological race also leaves scope for the emergence of significant changes in science and engineering. This opens up the possibility of strategic pivots, one of those historically rare points of technological diverge, which provide a surprise innovation factor in conflicts. These emerging and disruptive technologies are difficult to detect, and their impact on warfare even more so, but there is no doubt that ignoring them or adopting them late is usually synonymous with defeat.

[235] On the other hand, the widespread and easy access to advanced technologies by a multitude of actors is a spur to the discovery and application of disruptive technologies, hence the availability of these technologies provides an unquestionable military advantage. This is likely to be the way forward for the two superpowers - the United States and China - as they seek to gain superiority through research and development in a variety of areas.

[236] Under current security and defence conditions in Europe, it seems that the EU will not be able to keep pace with the United States. Therefore, the technological gap is likely to widen, and interoperability, even within NATO, may be compromised. However, under the European Common Security and Defence Policy, initiatives have been launched to bridge this technological gap as far as possible.

[237] A more intense symbiosis between the Ministry of Defence, the universities and the entities that constitute the Defence Technological and Industrial Base (DTIB) shall be decisive in maintaining the pace of development of other nations and organizations as much as possible. Currently, the civilian sector acts as a technology driver, often presenting the most important innovations in the form of dual-use technologies. It is therefore important to balance the traditional view of military customer-driven technologies with this innovative capacity in the civil sector.

[238] This, together with the aforementioned need for efficiency and viability, makes it necessary to promote and facilitate innovation and dual developments in coordination with other ministries, mainly the Ministry of Industry, Trade and Tourism, the Ministry of Science and Innovation and the Ministry of Finance and Public Authorities, whenever the operational requirements so allow.

[239] The participation of the Defence Technological and Industrial Base (DTIB) from the initial phases of the conception of the operational requirement will help to satisfy

military needs optimally, reducing design times, delays and the acquisition of unsuitable systems and equipment, as well as avoiding the development of capabilities that do not pertain to the operational needs of the Armed Forces. The review of the factors to be borne in mind in the current procurement processes, whether industrial, technological, personnel or financial, must be included from the outset, hence coordination among all actors is essential.

[240] The procurement of equipment and weapon systems through the Spanish defence industry has generally been a win-win commitment for both parties. Therefore, the Armed Forces, in coordination with the Secretary of State responsible for the department's industrial and technological policy, should contribute to the debate or prioritization of technologies for operational reasons. As far as possible, the Armed Forces should contribute to developing them, while accepting that in the field of innovation a certain culture of flexibility in procurement processes must be internalized as a way to progress successful technologies and projects.

[241] A second mechanism to reduce the technological disadvantage as far as possible is to cooperate with our main partners and allies through joint projects mainly in the European environment. The European Defence Agency (EDA), the Permanent Structured Cooperation (PESCO), as well as the European Defence Fund (EDF) initiative, show a clear will to boost Europe's industrial technology base.

[242] On the other hand, the multinational initiatives created ad hoc have already gone a long way and shall have to be strengthened. Thus, essential efforts are required to ensure that Europe's aforementioned strategic autonomy is built on a sufficient technological base. Furthermore, other bodies of the General State Administration should contribute to this collaborative effort, to define joint strategies, actions of common interest or provide adequate funding.

[243] The intensive use of cyberspace has already opened up an unconventional dimension of the Armed Forces' matériel, but it shall become even more important in the near future. Establishing a network of networks to enable the reception, processing and transmission of information, based on the need to share in a multi-domain environment, seems essential. Secure access to these networks shall be one of the key factors in 21st century security.

[244] In a changing and complex future, understanding the Operating Environment and making decisions quickly is an essential requirement. A database management system and the application of technologies and artificial intelligence to process it (big data) dramatically enhances and accelerates the ability to analyse information and turn it into knowledge. Decision support systems will enable commands at every level to keep pace with operations, giving them an operational advantage.

[245] Building collaborative, instantaneous and intuitive situational awareness at all levels of command, from commander to combatant, will seek to eliminate the fog of war. At the same time, it is imperative not to over-inform and saturate the human element. Cyber defence shall be essential to ensure that the adversary does not act on our systems to learn or alter, even in real time, our own situational awareness.

[246] To achieve this, the human-machine relationship through HMI (Human-Machine Interface) technologies will be fundamental. The data presentation must be clear, user-friendly and effective, so as not to saturate the operator or cause him/her to overlook information that is important to the operation, while maintaining acceptable levels of operator stress.

[247] The general trend shall be to endow autonomous systems with artificial intelligence and autonomy of action, with greater decision-making capacity and a higher degree of freedom, applying robotic technologies to ensure they do not have to be piloted automatically. Although fully autonomous systems shall be possible, an appropriate degree of human control over them must be maintained at this stage.

[248] One of the great future dangers is that such artificial intelligence could be compromised by a cyber-attack and used against those who developed it, especially with regard to weapon systems. Thus, a false flag attack against illegitimate targets, or any other form of aggression, may damage the image and interests of its original controllers.

[249] RPAS are useful in multiple types of operations in the land, naval and aerospace domains. They already perform ISR missions, target acquisition, artillery support, communications relay, electronic warfare, minesweeping and neutralization, naval surface and submarine warfare, air combat, improvised explosive device (IED) detection, measurement of environmental conditions in CBRN contaminated environments, cargo transport, route clearance, search and rescue in hard-to-reach areas, emergencies and disasters, etc. In the future, these systems will become even more important and will be used in a wider range of tasks.

[250] The operational integration of manned and unmanned vehicles is an enormously complex challenge, but it shall be one of the most widely-used forms of action. This integration shall reduce casualties, reduce operational costs, be a force multiplier and increase accuracy, reducing the incidence of human error.

[251] Artificial intelligence embedded in autonomous systems, which will become increasingly numerous and capable, will increase the catalogue of acceptable risk situations by not endangering human lives in tasks such as surveillance and reconnaissance or suppression of defences. However, using them in combination with lethal capabilities shall be the subject of wide-ranging controversy, both legally and in terms of public opinion. Notwithstanding their usefulness in situations requiring very high reaction speeds, such as missile/rocket defence or UASs, their use must be compatible with ethics and legitimacy in military operations.

[252] The confrontation between autonomous machines with lethal capabilities seems to be beyond the period covered by this paper - 2035 - but its first manifestations cannot be ruled out. At all events, the current state of technology and its foreseeable development make the emergence of this scenario in the longer term appear inevitable.

[253] There will also be advances in the human-machine combination, providing the warfighter with systems that complement and augment their capabilities. Examples include the use of exoskeletons and endoskeletons, stealth systems, vision, sensorization, remote diagnosis and medical treatment, and augmented reality. Advanced networked tactical simulators shall enable much of the training and coaching to take place, while process and procedure simulators shall facilitate the digital transition of personnel to new forms of management and administration.

[254] Developing new sensors and communication systems shall go hand in hand with robotization processes and nanotechnology. Increasingly affordable and capable space platforms shall also become available, facilitating their own disposition, but also that of potential adversaries. In this sense, a certain militarization of outer space seems inevitable.

[255] Advances in quantum computing will endow computers with far superior properties compared to classical computing. The speed of quantum computing will bring new dimensions to resolving complex problems in certain areas. It will enhance and accelerate the capabilities described in the foregoing paragraphs and shall serve to develop elements and systems to support the development of operational capabilities. On the other hand, to ensure the protection of information and data, new quantum encryption algorithms will have to be developed to counter the processing power of quantum computing.

[256] The initiation of research into and development of hypersonic weapon systems by some powers opens up a new range of possibilities and threats. Their effect on operations could be considerable, radically diminishing the effectiveness of existing anti-aircraft and anti-missile systems. The development of both new hypersonic weapons and those aimed at neutralizing them is therefore to be expected.

[257] Directed energy weapons emit electromagnetic energy without consuming conventional ammunition. They only require an electrical power source, so they could be powered by energy generated by the carrier vehicle itself or even self-supplied by solar, wind or other sources. Their advantages in terms of precision are significant, greatly reducing the risk of collateral damage. They also reduce the logistical problem of supplying ammunition, freeing up weight and volume in transport systems.

[258] Laser technology, Electromagnetic Pulse (EMP) Emission and High-Power Micro-Wave Weapons (HPM), major avenues of development, are of concern. These technologies may potentially be capable of exploiting the vulnerability of electronic systems, the cornerstone of 21st century Armed Forces equipment and systems. The main applications could be anti-missile and anti-projectile, destruction of airborne platforms, self-protection

of ships against subtle vessels, integration of HPM means with conventional weaponry, mine neutralization, vehicle immobilization, degradation of air defence systems, etc. The development of technologies capable of counteracting their effects while protecting their own systems shall be increasingly necessary.

[259] New super-materials such as graphene, borophene and other nanomaterials, additive manufacturing (AM or 3D printing) and nanotechnology will substantially change construction, metallurgy and medical processes. The manufacture of smaller and better-performing devices, lighter and longer-lasting batteries, new stronger and lighter composite materials, individual protections with high ballistic resistance, new composite armour, more efficient, selective and sensitive sensors to detect nuclear, biological, chemical and explosive agents are on the way to revolutionizing military equipment and systems.

[260] The impact of these technologies has the potential to significantly evolve the conduct of operations in a variety of fields. They are expected to influence essential aspects substantially such as castrametation, in-theatre sustainment of weapon systems, *in-situ* manufacturing of spare parts or self-repair, self-supply of energy, Micro and Nano RPASs, swarm attacks, field medicine, reduction of radar, infrared and acoustic signature of systems, etc.

[261] As for conventional weapon systems, their use in future conflicts is likely to decline, with hybrid strategies and information operations playing the major roles. However, their use and readiness will need to be maintained, since the possibility of conventional armed conflict has not disappeared and can even be developed as a strategic

surprise against adversaries who have neglected this conventional dimension of conflicts, so they are in any case an essential element for deterrence.

[262] Likewise, the possible theatres of operations at a lower technological level remain, in which insurgency, subversion and asymmetric confrontation continue to predominate. In certain areas and environments, the technological disadvantage may favour adversaries such as urban guerrillas or terrorist organizations, diminishing their vulnerabilities by lacking those that are inherent in using them, especially in terms of communications.

[263] While ongoing inter-power competition shall take place in a multi-domain environment, conventional operations shall predominantly take place in urban and coastal environments, as populations rapidly concentrate there. This shall leave large empty spaces in the interior of continents, which shall lose much of their strategic value, except in specific locations endowed with an abundance of strategic resources. Therefore, it shall be recommendable to assess the provision of more facilities and systems suitable for operating in urban and coastal environments.

[264] The sustainment of systems and platforms must also evolve towards greater agility and efficiency. It shall be important to design the sensorization and connectivity of systems in a predictive sustainment philosophy. New platforms will need to have standardized designs that are easily configurable for each user, with the most extensive use of hybrid propulsion, networked autonomous operation capability and digitization of the supply chain. This shall mean a fundamental change in materiel logistics and maintenance.

Facilities

[265] Although the number of MINISDEF facilities has decreased, the deficiencies in the maintenance of many of the infrastructure are manifest and, on some occasions, critical. Besides the necessary funding, measures should be taken to adequately maintain the infrastructure that are considered essential, optimizing their use as much as possible.

[266] The facilities must also be energy efficient, with self-generation and storage systems for the energy produced that guarantee sufficient autonomy for the operation of critical systems. The development of new air conditioning systems (active and passive) to replace the current ones, which in many cases produce a high carbon signature, can drastically reduce energy consumption both at Homebase and during operations.

[267] New facilities should be designed as multifunctional, with a high level of standardization, automation and robotization. Equipped with transport terminals compatible with the use of networked intelligent autonomous vehicles, mainly in the case of logistics facilities.

[268] For infrastructure to be built or transported to the Operational Theatre, their modular design and the use of additive printing for in-situ manufacturing of certain elements shall have to be borne in mind, reducing their dependence on TN for maintenance.

[269] Efforts should be made to reduce the environmental footprint (emissions, consumption, discharges, waste, etc.) of military infrastructure, achieving greater stealth in operations, while contributing to the Sustainable Development Goals.

Personnel resources

[270] Despite the apparent prominence of technology, the human resource shall remain the most critical. It shall be essential to put in place measures to get the best out of the available personnel and to make their distribution more flexible according to the capabilities required by the Armed Forces in 2035. The qualitative advantage over potential adversaries shall lie in the talent management and readiness of our personnel, as well as the ability to retain critical personnel.

[271] The new tasks assumed by the Armed Forces (space and cyberspace) require adequate specialization, as well as the need to maintain adequate availability in force units. As a result, the numbers, distribution by jobs, corps and specializations of Armed Forces personnel shall have to be reviewed, and new specializations shall probably have to be created. At the same time, the sharp demographic decline and the sociological evolution of the Spanish population may lead to difficulties in recruiting and retaining personnel.

[272] Forecasting the human resources required must be part of creating and maintaining any capability, through a prioritization exercise, to adapt capabilities to forecasts of personnel availability.

[273] Personnel management should be more flexible, allowing for the transfer of personnel dedicated to a given function to be increased or reduced more quickly. In this

regard, consideration should be given to extending and improving the possibilities for temporary attachment to the Armed Forces, depending on the various needs of each of the Army, Air Force and Navy, at all levels. Sufficient funding should be made available to outsource services or tasks that can be performed by civilian personnel, which will offer the necessary specialization and continuity, together with improving the current reservist model.
Similarly, it would be necessary to attract military personnel and ensure they remain in post, especially technical and highly specialist areas that require remaining in place, thus bringing their working and financial conditions into line with those that can be found in other ministries.

[274] Competition in the employment market for personnel will be difficult. Attracting and retaining increasingly analytical and technical personnel with high-level skills will be very difficult in competition with civilian demand. Indeed, this will probably be one of the biggest challenges in the coming years. The improvement of socio-economic conditions, quality training adapted to the times, life/work balance the quality of life of the members of the Armed Forces will be decisive in this respect. If progress is not made along these lines, there is a risk that the Armed Forces will become a training ground for specialist technicians to meet civilian demand in some areas, undermining Defence needs.

[275] There are other aspects to be improved that shall also contribute to personnel retention, such as better selection, promotion of talent and setting out career models. Moreover, the

selection process should be improved to base it on merit and ability criteria from a 360° perspective, increasing the delegation and assignment of responsibilities to personnel at the middle and entry levels. Efforts should also be maintained as regards continuous training throughout their career, together with establishing an effective model for the transition of personnel between their service in the Armed Forces and other areas of public service, as well as companies in the Defence sector.

[276] In contrast to a long-standing trend towards generalist, the increasing complexity of the tasks of the Armed Forces shall require diversification and specialization of career profiles. Within these profiles, there shall be a need for greater horizontal development of personal careers, without this being detrimental to their career progression. This shall make it possible to maintain, for the various processes, a basic core of personnel capable of maintaining their full autonomous functioning (know-how concept).

[277] There has also been a tendency to standardize the profiles of Armed Forces members. The change underway is likely to drive the need for personnel with much more varied skills and profiles. This shall allow everyone to be placed where they can perform best.

[278] To optimize the performance of our personnel, it is necessary to manage the talent of our personnel according to their competencies. To this end, it shall be a primary requirement to define a catalogue of key competencies at the various levels of the organization. According to this catalogue, establishing the competency profiles of each job position shall facilitate the person-position assignment, thus improving the fulfilment of the mission. This process shall require a database that collects the competencies of our personnel.

[279] In this context, the evolution of training and personnel development programmes shall have to be maintained. Therefore, educational establishments shall have to adapt to new specializations and curricula to meet emerging technologies and the evolving

modes of action of the Armed Forces. Legal and regulatory adaptations shall most likely be necessary to provide the Armed Forces with the necessary specialist personnel, ensuring greater continuity in its tasks than is currently the case.

[280] Members of the Armed Forces are targeted for disinformation and recruitment by hostile elements more intensively than the average citizen. Increased actions in the cyber and cognitive operating domains may recommend further strengthening of counterintelligence efforts in the Armed Forces.

[281] Despite the high esteem in which our population holds its Armed Forces, we should insist on the tasks of promoting defence culture and awareness among the population, as these are still lower in Spain than in neighbouring countries.

Training and Leadership

[282] Comprehensive training, readiness and personal development, both individually and collectively, shall facilitate the adaptation of the Armed Forces to the future Operating Environment. The mere transmission of knowledge and skills is not enough, but it must be taught to think in different, sometimes even disruptive, ways that shall enable it to deal effectively with diverse and equally disruptive environments.

[283] Leadership has always been a determining factor in conflicts. The importance of new, more complex leaderships is now emerging, with traditional characteristics and others oriented towards continuous adaptation that can withstand the complexity of operations, their high pace and the dispersion of simultaneous actions in different operating domains - material and immaterial - which shall be executed in a decentralized manner in dynamic environments.

[284] It is not easy to train reliable, innovative, adaptive managers, prepared to make decisions per national and international laws, in an environment with major legal and ethical constraints, in chaotic situations and at a dizzying pace. To this end, it shall be necessary to continue to insist on elevated moral qualities, high levels of commitment, motivation, excellence, discipline, a high degree of availability and adequate physical capacity. From there, training in new technologies and training in the cyberspace and cognitive domains of operation must be intensified.

[285] Leadership training should be geared towards promoting a change of cultural and organizational mindset, reinforcing innovation and problem-solving in combat that is adapted to the reality of new Operating Environments.

[286] Military Education Centres should promote leadership training and training in critical and original thinking. To identify the suitability of personnel for certain positions or levels of the organization, from the moment they enter the Armed Forces, they must be equipped with situational assessment systems, using measurement tools that allow for this. Thus, it shall be possible to provide each individual with the training, development and training vector best suited to his or her skills throughout his or her career. In the

more complex, diverse and specialist Armed Forces of the future, aligning individual capacity with the needs of the institution in career paths becomes even more important for proper performance and results.

[287] Military exercises shall remain essential to test the ability to perform the tasks assigned in the operational plans developed for mission accomplishment, as well as to exercise deterrence to support the management of our area of interest and our peacetime surveillance activities. They will need to develop to incorporate new areas of operation, concepts, technologies and systems, with particular attention to developing integrated multi-domain exercises.

[288] The new simulation capabilities shall provide major advances in exercise force training capabilities, enabling the integration of simulated systems with real systems in multi-domain environments, with the inclusion of realistic events according to live-virtual and constructive (LVC) simulation principles. Thus, they shall contribute more effectively to improving the operational capability of the force, reducing costs and increasing safety in their execution.

[289] It should never be forgotten that the training of personnel, regardless of their specialization and position in the organization, must be geared towards their training for optimum performance in combat, a specific form of action and the reason of the Armed Forces.

[290] The application of mentoring and coaching techniques, mainly at different levels of management, can help to optimize their performance, improving personal skills in areas such as stress management, time organization, quick reading techniques, reducing the learning curve in each new assignment, etc.

[291] As a means of adapting to increasingly disruptive and rapid change and uncertainty in the Operating Environment, the Armed Forces shall have to undertake a continuous effort of experimentation, which shall play a key role in readiness planning and shall be an increasingly common activity for commands and units.

Doctrine

[292] It is an intellectual construct that aims to translate theories of warfare into the real world, guiding the effective employment of the Armed Forces. It must be applied judiciously and flexibly, as its main source of information is the study and lessons learned from conflicts that have already occurred, whose conclusions and lessons shall be applied to future conflicts so as not to make the mistakes of the past. However, although nourished by proven truths, without a forward-looking approach, doctrine would always prepare the Armed Forces for past conflicts and could lock them into concepts and ways of acting that may have become obsolete.

[293] Today, doctrine faces the great challenge of continually keeping up to date, increasing its speed of adaptation and incorporating new types of doctrinal products required. This adaptation must keep pace with the rapid evolution of the Operating Environment, of technology and its impact on ways of warfare. Therefore, doctrine must present proposals or solutions for the use of force in the face of the emergence of new tactical concepts, disruptive technologies, changes in the geopolitical environment, the dominant ideologies in their societies, the evolution of their citizens, etc., to anticipate events and avoid outdated reactive movements.

[294] This vision of doctrine takes on a greater dimension in the face of the innumerable and profound changes that our societies are undergoing, to the point of being able to speak of a change of era which, necessarily, through multi-domain operations, shall have a great impact on these ways of waging war and facing security challenges.

Organization

[295] The organization of the Spanish Armed Forces has undergone a remarkable evolution in recent decades, in such a way that it can be considered a continuous and uninterrupted process of adaptation. Faced with the accelerated changes we are experiencing, it is moving towards process and project management as opposed to organic structures that are proving to be too bureaucratic, and therefore lack the necessary agility to respond to the future environment.

[296] In a similar way as in operations, structures should be optimized, making them flatter and allowing for decentralization of resources and decision-making. Greater leadership, inspiration, motivation and trust-building would enable lower-level management to better support decision-making.

[297] Hierarchical structures now tend to coexist with so-called Network Centric Operations (NCO). Network centric operations are based on three elements: geographically dispersed forces, a high degree of training and experience, and a robust and reliable network linking them. This type of operation decreases the vulnerability of forces, reducing casualties and strengthening their command and control.

[298] However, it shall always be necessary to exercise authority from the highest political levels to the military authorities and from the latter to the tactical executors. Given this reality, it is essential to deepen the design of processes that facilitate the chain of command's agility in the direction, coordination and control of the execution of operations.

[299] These new processes must be able to respond to more chaotic and less linear environments, with cross-cutting interactions from different lines of action of the adversary. It shall therefore be necessary to adapt our response capacity to a distributed environment. Access to a large volume of information and the rapid interaction of all levels of the chain of command, and even with other actors outside the organization, can become unmanageable for an organization that is too vertical. Therefore, all members of the Armed Forces, even at the lowest levels, must exercise a certain level of leadership, forming a collective and shared leadership of the organization. This evolution shall require the implementation of changes in the processes, mindset and culture of our organization, beyond merely adapting to technological advances. But, above all, it shall require deepening the current vision of leadership (Mission command), encouraging the delegation of authority, risk-taking, initiative and the ability to adapt responsibly to the purposes of the command.

[300] Given that most future operations shall be conducted in coordination with other state and non-state, national and international actors, the Armed Forces should be brought as close as possible to these actors. Not only from the point of view of interoperability of systems, but also in cultural and procedural aspects, which shall facilitate synergistic and effective action.

[301] Better defined backbone processes, coordinated with specific Army, Air Force and Navy processes, shall allow for greater efficiency and continuity in force readiness, operational employment and resourcing.

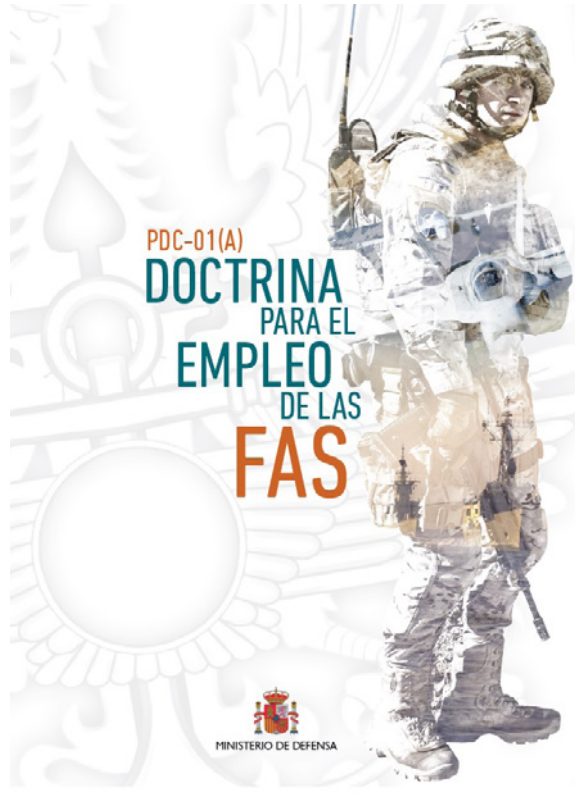
[302] Moreover, deepening strategic military relations, both within the EU and NATO, with other national institutions and with business and civil society, by sharing information in an agile and secure way, shall better prepare the Armed Forces for future challenges.

[303] Ultimately, all of the above should lead to a significant increase in the agility of the decision-making process in the face of an increasingly fast-paced battle. Key to achieving this is the interoperability of intelligence services that are integrated into a Command-and-Control network to allow analysts access to shared ISR and intelligence products. Thus, commanders shall have what they need to conduct actions that, aligned with command directives, require maximum speed of execution.

Interoperability

[304] The above technological innovation and experimentation have a prerequisite in terms of interoperability. This must be further developed in the context of our military partners and allies so that new systems are fully interoperable. Only in this way shall it remain possible to use them in the most demanding operations and in multi-domain operations.

In the national field, there is a need to evolve towards cooperative combat, both in weapon systems and in the use of the combat cloud, with the technological development that this implies.



[305] To achieve this, besides combined integration in operations, more intense cooperation initiatives must be added in the areas of capability planning, education and training, information sharing, procedures, etc. In short, to seek deep interoperability from the outset, which is not a final expression of different processes that converge in operations, but rather arises from a design based on common requirements from the beginning of the Force & Capabilities generating process.

[306] It is also necessary to advance in interoperability with the command, control and communications systems of the rest of the public administrations,

mainly those that the Armed Forces can support in the framework of OS3. Moreover, the Armed Forces shall sometimes also have to coordinate their operations with non-state actors, whether national or foreign, such as multinationals, NGOs, local populations, individuals, etc.

[307] Only in this way shall it be possible to act quickly and effectively in the military's contribution to the security and well-being of citizens, over and above the military forces special endowment in this area, as the Emergency Military Unit's case.

[308] Security has an increasingly comprehensive approach to provide global responses to future challenges and shall require Armed Forces with a greater capacity to interact with each other and with other actors in a multi-domain environment. In this regard, it shall be necessary to deepen, as a priority, joint action in areas such as C2, CIS, JISR, cyber defence, strategic communication and personnel readiness.

Potential areas of change for the Armed Forces in adapting to the Operating Environment 2035

[309] The main trends identified in terms of new ways of conducting conflict, and eventually combat and warfare, indicate that rapid reaction to a wide variety of different situations and missions shall be required. The preponderance of information, knowledge of the context, identification of opportunities and anticipation of other actors and events shall be essential.

[310] Understanding the situation, in an accurate analysis and assessment of the huge amount of information from multiple sensors, through the processing of big data and artificial intelligence, shall be decisive. The high pace of actions shall make it more difficult to redirect erroneous analyses and activities. The advantages in knowledge and understanding shall make it possible to adapt decision cycles to the prevailing rhythms of the new environment.

[311] Decisions taken shall have to be implemented quickly and effectively, shortening the decision cycle and influencing the environment across the board in such a way as to impose a high battle tempo on the adversary.

[312] For this to happen, it shall be key to have three elements that act simultaneously and seamlessly from the beginning of the crisis: **strategic leadership** that provides the frame of reference for a Military Strategy, which establishes clear strategic objectives and the effects to be achieved. **Political will** must ensure the integration and synchronization of all capabilities available to the state (not only military) to create lethal and non-lethal effects against the identified target. **National resilience** to conflict needs to be planned and prepared, requiring the construction of a narrative underpinned by strong and unequivocal national values and reference points.

[313] The instruments of the Armed Forces to achieve the coordinated action of these three key elements shall be, among others:

- Enhancing leadership, initiative and talent as a multiplier factor, with an emphasis on mission-oriented command.
- To achieve a situation of budgetary stability and predictability, which allows for an adequate, balanced, stable and flexible endowment to conduct the necessary modernization and sustainment of the Force, as well as to contribute to the commitment to our allies.
- Exercise command from a multi-domain, collaborative, instantaneous and intuitive situational awareness.
- To make the necessary efforts in the field of intelligence, both to anticipate events and to acquire the aforementioned situational awareness. Studying and understanding the adversary is a decisive factor in the conflict.
- Include artificial intelligence-based tools in the analysis, decision and execution processes, making them more efficient.
- Pay particular attention to the concept of the "combat cloud", as a key element in multidomain operations. An interconnected network for the exchange of data and information within the battlespace, where each user or platform transparently provides and receives essential information, which can be used across the full range of military operations.
- Adopt streamlined, more horizontal and decentralized structures, where decision-making is appropriately delegated to implementation levels, simplifying processes where possible.

- Shaping the Force, resources and capabilities to move from Joint to Multi-domain operations.
- To configure, based on a modular conception of capabilities, multi-purpose, interoperable units with high readiness, versatility, flexibility and resilience. Multiple small units with these characteristics can create a more complex scenario for the adversary than a smaller number of heavier units.
- Execute actions in as decentralized a manner as possible, with permanent awareness of the command's intentions and a high degree of initiative.
- Expedite actions in the cyberspace operating domain through pre-planned responses, as reactive decision-making is particularly ineffective in this area.
- Set up agile logistics to sustain the operation over time.
- Define control mechanisms to measure the validity of decisions, providing metrics of the results obtained.

- Provide appropriate, proportionate and credible military response actions, causing physical and non-physical effects in all areas of operation.
- Design new capabilities and means of deterrence in the cyber and cognitive domains.
- Strengthen cyber-defence and supply chain control of all weapon systems, to ensure that adversaries do not act on them by rendering them inoperable, diminishing their effectiveness or using them against us.
- Incorporate the most advanced cyberspace-based offensive techniques and tactics into the military's own response arsenal, as the most likely battlefield in an environment of continuous competition.
- Promote the study and implementation of legal and ethical provisions on the military use of new technologies, indicating the modalities and limitations for their legitimate use.
- Combat the adversary's ability to conduct lawfare activities against our interests.
- Facilitate the implementation of concepts to counter possible A2/AD adversary actions, to preserve the necessary freedom of action and to be able to realize the chosen response option, ensuring operability in degraded environments.
- Define from the outset and at the highest level an internal and external communication strategy, STRATCOM, which is integrated into the decision-making processes.
- Integrate operations in the cognitive domain as part of the response options, as they are a new and growing battlefield.
- Establish the necessary mechanisms to combat disinformation on their own and opposing societies.

- Having resilient or alternative systems in place, to be able to continue operating in saturated and degraded environments.

[314] In short, the set of factors determining the Operating Environment in 2035; the challenges and opportunities it presents; the Operational Scenarios in which the Armed Forces shall conduct their missions; the characteristics they must have; the instruments the Joint Force must have at its disposal and the main trends detected in the profound process of change in which the world is immersed, allow us to point out the following areas of potential change:

[315] **Improving strategic agility**: This requires a military strategy that anticipates major risks and threats and provides firm and clear guidance, anticipation of appropriate and practicable response options, superior information collection and processing, immediate availability of intelligence products in a networked command system, a rapid decision cycle and a high battle tempo.

[316] Likewise, it is necessary to reinforce strategic leadership, through continuous monitoring of the achievement degree of strategic objectives and associated strategic plans; permanently adjusting the efforts required of the Armed Forces in each of the identified strategic lines of action, seeking to achieve the appropriate effects at all times; aligning the military activities and efforts conducted both within the framework of autonomous operations and those developed within the framework of the ISDO; and applying an appropriate communication strategy (STRATCOM).

[317] **Reducing the logistics footprint:** to this end, areas such as stock adjustment, predictive maintenance, standardized and easily configurable platforms, hybrid propulsion systems for vehicles and energy generation and storage should be explored. Thus, progress must be made towards simpler supply chains, platforms with lower fuel consumption, more efficient infrastructure and maintenance.

Reducing the logistics footprint also has the effect of reducing emissions, consumption, discharges, waste, etc., which contributes to society's commitment to the environment being shared by the Armed Forces, both in their fixed installations at Homebase and deployable in operations.

[318] **Optimize operating and sustainment costs**: provide the Armed Forces with a new digitalized organization with agile and lean structures, in collaboration with the private, institutional and multinational sectors. Move towards a new procurement model for weapon systems, improving the process of determining needs and ensuring funding throughout the entire life cycle. Increase participation in multinational procurement programmes, have a harmonized integrated logistics management system and predictable funding.

[319] **Optimize the number and distribution of military personnel**: demographic evolution, the automation of processes, the introduction of autonomous systems and the improvement of combatant survivability, come together with the emergence of new

forms of action and combat. This makes it necessary to reflect on a balanced and flexible distribution of military personnel in the various specialities and tasks required in future missions, sizing each area appropriately to be able to provide an effective response in a joint, multi-domain environment.

[320] **Improve talent management**: the VUCA environment of 2035 and the increasing complexity of military operations shall require professionals with leadership, determination, initiative, agility, flexibility, creativity and adaptability. Personnel management shall need to focus on maximizing the capabilities of each individual Armed Forces member, placing them in the position where they can best contribute to the common effort, exercising mission-oriented command. Efforts should also be made to recruit and retain those who best serve the interests of the institution, in competition with the labour market.

[321] Similarly, it is important to increase the presence of military personnel in national society. Although significant progress has been made in this area in recent years, further efforts are required to integrate the military better and thoroughly into Spanish society. This applies both to commanding officers and to troops and sailors, the latter mainly at the end of their commitment to the Armed Forces. This greater presence would favour society's knowledge of the Armed Forces, understanding of their mis-

sions, greater concern among national elites for defence matters and, in short, society's full support for the Armed Forces in crisis or conflict situations.

[322] **Committing to technological superiority**: together with doctrinal innovation, the availability of more advanced technology than that of the adversary shall be key to guaranteeing superiority in the confrontation. Given limited national capabilities, it shall be essential to develop a strong, innovative and sustainable national defence industry, collaboration within the ISDO to which Spain belongs, and participation in joint development programmes for military equipment and systems, mainly in Europe. The nation's materiel and financial support shall be decisive in maintaining a technologically superior Armed Forces capable of meeting the security challenges to come.

[323] **Improve analysis and surveillance capabilities, strengthening the collection and processing of information:** a complex and changing environment, with a large number of actors involved, dispersed in different areas, requires superiority in information processing. Therefore, the collection and systematic observation (surveillance) or limited in space and time (reconnaissance) with sensors and warning systems, together with the rapid processing and dissemination of the information obtained, shall be decisive in the conflict. It therefore seems an essential priority to strengthen JISR systems, both autonomous and non-autonomous, and processing systems that enable the rapid and optimal generation of intelligence.

The provision of a system of indicators, alerts and trends is a valuable tool to enhance these analysis and monitoring capabilities.

[324] **Improving capabilities in the cyberspace, cognitive and outer space domains of the aerospace domain**: traditional domains are joined by new battlefields, both considered in isolation and transversally to the other domains, through unconventional and hybrid threats and strategies in an ever-increasing performance in the "grey zone." These involve new ways of waging war that are imposed on us by potential adversaries, which makes it necessary to develop and strengthen our capabilities in these areas, generating effective deterrence, prevention and military response in them.

[325] On the other hand, it is equally necessary to maintain and enhance counterintelligence and information security capabilities that prevent the leakage of sensitive information. The cross-cutting penetration of hostile actions in the cyberspace and cognitive operating domains can facilitate the intrusion of potential adversaries into areas of defence interest.

[326] Moreover, a continuous effort is required to maintain good strategic communication. There is a growing need for credibility in the use of military capabilities, which requires defending one's own population from possible information poisoning by the adversary, who could thus exploit a structural weakness of democratic nations. Storytelling is one of the main weapons in present and future conflicts, where it can be as important to win on the field of public opinion as on the battlefield. The strategic value of informing citizens about the legitimacy of political and military objectives is undeniable. Fostering a greater culture and awareness of security and defence among the Spanish population is one of the great challenges of the future Operating Environment.

[327] **Improving interoperability:** it is important to maintain the ongoing effort to standardize systems and procedures with allied militaries in a multilateral environment. But it is also necessary to improve the coordination and interoperability of the military's contribution, upon request of the authorities, to the National Security System. The number and frequency of situations, whether or not provoked by hostile action, in which the lives and well-being of the population may be threatened, seem increasingly recurrent. Therefore, the support of the military instrument in these situations may be required more frequently. These missions and tasks may, on occasion, exceed the capabilities of the UME and require a greater contribution from the Armed Forces.

[328] To improve this contribution of the military instrument to the National Security System, it is necessary to conduct exercises and activities that facilitate better coordination with the other actors involved.

[329] **Continuous and flexible adaptation of the organization, designing solutions to implement the necessary changes identified:** efforts and investments, changes in people, ideas, tools and organizations are essential to prevailing in the new scenarios in the field of security and defence. The coming years shall require an intense and continuous effort to change, which may even be disruptive in some respects, with

necessary adaptation of the regulatory framework, both for these organizational adjustments and for those derived from the use of new technologies. Failure in this process could seriously compromise Spain's military defence, the reason of the Armed Forces, in an increasingly competitive and risk-ridden environment.

[330] The main conclusion of this study is that there is a need for Armed Forces adapted to the new times. To maintain a credible combat capability capable of facing the risks and threats of the future, major innovative efforts and intellectual, cultural, technological and materiel investments are essential. The coming years shall require courageous and imaginative decisions to fulfil our mission and be useful to Spanish society. Maintaining effectiveness and increasing efficiency shall require an effort to transform our Armed Forces to avoid obsolescence and a decrease in their military value, which shall require convincing Spanish society of the transcendental importance of this process for its security and well-being.

[331] They shall need to be highly combat capable, balanced and responsive to the challenges of the moment. They must be fully integrated into the multi-domain environment that shall characterize operations in the coming decades. They must also be sustainable and versatile, interoperable with our allies and the National Security System, and strategically mobile enough to operate wherever they are required.

The transformation process must lead to Armed Forces capable of fulfilling its assigned missions and contributing decisively to Spain's security, with the moral fortitude necessary for its permanent dedication to the service of the nation.

Summary Table Chapter 3:

ARMED FORCES ADAPTATION TO THE OE 2035

Characteristics of the Armed Forces in the OE 2035

The range of operations they will have to conduct shall be very broad, both in terms of types of operations and missions and in terms of their gradation, the size and composition of the contingent involved and the intensity of the actions.

All of this will occur in a more intense and accelerated time pattern than at present, drawing in short a matrix of availability, effort and continuous demands for the Armed Forces.

The ability to adapt and respond quickly, effectively and efficiently to a wide range of unpredictable situations and potential adversaries will determine the success or failure of the future Armed Forces.

The qualities that make national military power credible are:

- **High combat capability**
- **Balance of action in the 5 operating domains**
- **Multidomain integration**
- **Response capability**
- **Strategic mobility**
- **Economic viability**
- **Readiness and sustainability**
- **Versatility**
- **Resilience**
- **Innovation and adaptability**
- **Interoperability**
- **Moral fortitude**

A necessary change

The changes underway are so far-reaching and rapid that even constant adaptation may not suffice in specific areas, and decisions must be taken to bring about a real transformation of these areas.

Perhaps the biggest challenge of the ongoing change process is to match it in the areas identified: personnel, ideas, tools and organization.

Challenges and Opportunities

National security and defence require addressing these challenges, exploiting the many opportunities to make the Armed Forces more effective in a changing world.

To systematize the description of the perceived challenges and opportunities, the main aspects to be modified are set out around the DOTMLPF-I factors.

Materiel. It shall be dominated by technological innovation and experimentation.

Facilities. Optimize its use to the maximum, with multifunctional, standardized and automated design.

Personnel. It shall remain the most critical factor, including talent management and retention capacity.
Training and Leadership. Comprehensive training, readiness and personal development shall facilitate the adaptation of the Armed Forces to the future Operating Environment.
Doctrine. Present proposals or solutions for using the Joint Force to anticipate developments.
Organization. Optimize flatter structures, allowing for decentralization of resources and decision-making, based on networked operations (NCO[1]).
Interoperability. Arising from a design based on common requirements from the start of the Force & Capabilities generation process.
Potential Areas of Change of the Armed Forces in adapting to the OE 2035 To achieve the characteristics that the Armed Forces should have by 2035, the following areas of change are identified:
1. Improving strategic Agility
2. Reducing the logistical footprint
3. Optimizing operating and maintenance costs
4. Optimizing the number and distribution of military personnel
5. Improving talent management
6. Committing to technological superiority
7. Improving analytical and monitoring capacities by strengthening the collection and processing of information
8. Enhancing aerospace cyberspace, cognitive and outer space capabilities in the aerospace domain
9. Improving interoperability
10. Continuous and flexible adaptation of the organization, designing solutions to implement the necessary changes identified
"The transformation process must lead to Armed Forces capable of fulfilling their missions and contributing decisively to the security of Spain, with the moral fortitude necessary for their permanent dedication to the service of the nation."

1 NCO: Network Centric Operations.

Glossary of terms

WMD	Weapons of Mass Destruction
AM	Additive Manufacturing
A2/AD	Anti-Access / Area Denial
BTIDB	Defence Technological and Industrial Base
CCDC	Concepts Development Joint Centre
CESEDEN	National Defence Advanced Studies Centre
CIS	Communications and Information Systems
OS	Operational Scenario
COVID-19	Coronavirus Disease 2019
CRO	Crisis Response Operations
C2	Command and Control
DDN	National Defence Directive
DIVDEF	Force Development Division
DPD	Defence Policy Directive
EDA	European Defence Agency
EIDE	Defence Industrial Strategy
EMACON	Joint Defence Staff
EMP	Electromagnetic Pulse
OE	Operating Environment
2035 OE	2035 Operating Environment
NSS	National Security Strategy
ETID	Defence Technology and Innovation Strategy
AF	Armed Forces
FCSE	State Security Forces and Corps
LNG	Liquefied Natural Gas

HMI	Human-Machine Interface
HPM	High Power Microwave Weapons
AI	Artificial Intelligence
IEEE	Spanish Institute for Strategic Studies
IED	Improvised Explosive Device
ISR	Intelligence, Surveillance and Reconnaissance
JISRI	Joint Intelligence, Surveillance and Reconnaissance
LAR	Lethal Autonomous Robotics
LVC	Advanced simulation techniques (Live-Virtual and Constructive)
MINISDEF	Ministry of Defence
DOTMLPF-I	Materiel, Infrastructure, Human Resources, Training, Doctrine, Organization-Interoperability
CBRN	Nuclear, Biological, Chemical-Radiological
NCO	Network Centric Operations
NEO	Non-combatant Evacuation Operations
SDG	Sustainable Development Goals
ISDO	International Security and Defence Organizations
NGO	Non-Governmental Organizations
UN	United Nations
OSCE	Organization for Security and Co-operation in Europe
NATO	North Atlantic Treaty Organization
RPAS	Remotely Piloted Aircraft System
STRATCOM	Strategic Communication
NT	National Territory
EU	European Union
UME	Military Emergency Unit
VUCA	Volatility, Uncertainty, Complexity and Ambiguity
OZ	Operations Zone

References

- *Spanish Constitution, 1978*.
- Organic Law 5/2005, of 17 November, on National Defence.
- Law 8/2011, of 28 April, establishing measures for the protection of critical infrastructure.
- Law 36/2015, of 28 September, on National Security.
- Spanish Institute for Strategic Studies (IEEE). (2021). *Panorama of geopolitical trends. Horizon 2040 (2nd Edition)*.
- Action Plan for the drawing up of the "Futures Studies" programme, signed by DICESEDEN in March 2017.
- Office of the President of the Government, National Security Strategy 2021.
- National Defence Directive 2020.
- Defence Policy Directive 2020.
- Doctrine for the Employment of the Armed Forces, Joint Doctrine Publication (PDC)-01-(A), 2018.
- Defence Industrial Strategy 2015.
- Defence Technology and Innovation Strategy 2020.

Bibliography

EUROPEAN DEFENCE AGENCY (EDA). (2008). *Future Trends from the Capability Development Plan* (CDP).

Alberts, D. S. (Dir.) *et al*. (September 2003). *The Agility Advantage*. CCRP Publication Series.

Alberts, D. S. (March 2001). *The Information Age Anthology Volume III: The Information Age Military*. CCRP Publication Series.

ATHENALAB. (2020). *Desafíos para la seguridad y la defensa en el continente americano 2020-2030 (Challenges for security and defence on the American continent 2020-2030)*.

Bialos, J. P. & Koehl, S. L. (2016). *What America's Big New Defense Plan Gets Wrong*. The National Interest.

JOINT CENTRE FOR CONCEPTS, DOCTRINES AND EXPERIMENTATION (CICDE) France. (2012). *Conflicts in the Next 15 Years and Operational Consequences*.

JOINT CENTRE FOR CONCEPTS, DOCTRINES AND EXPERIMENTATION (CICDE) France. (2016). *Environnement Opérationnel Futur 2035*.

CENTRE FOR THE DEVELOPMENT OF CONCEPTS AND DOCTRINE (DCDC) UK. (2014). *UK Joint Concept Note 1/14, Defence Joint Operating Concept*.

CENTRE FOR THE DEVELOPMENT OF CONCEPTS AND DOCTRINE (DCDC) UK. (2014). *Future Operating Environment 2035*. *Strategic Trends Programme*. 1st ed.

CENTRE FOR THE DEVELOPMENT OF CONCEPTS AND DOCTRINE (DCDC) UK. (2014). *Global Strategic Trends (GST) out to 2045*. *Strategic Trends Programme*. 5ª ed.

COMMAND AND CONTROL CENTRE OF EXCELLENCE (C2COE), NATO. (2014). *Exploring Command and Control in an Information Age*. Estonia, Information Age Seminar.

DEFENCE INNOVATION CENTRE (CID) Italy. (2012). *Military Implications of the Future Operating Environment*.

MILITARY CENTRE FOR STRATEGIC STUDIES Italy. (2007). *The world in 2030. Regional Trends*.

HIGHER CENTRE FOR ADVANCED NATIONAL DEFENCE STUDIES (CESEDEN). (April 2010). Monograph no. 115.

Colom, G. (2016). *Transforming the Spanish military*. DEFENCE STUDIES. Vol. 16, no 1. Seville, Universidad Pablo de Olavide. Pp. 1-19.

NATIONAL INTELLIGENCE COUNCIL (NIC) United States. (2017). *Global Trends: Paradox of Progress*.

Dubik, J. M. (2009). Leadership beyond the Chain of Command. Army Magazine. Vol. 59, no 12.

Dworkin, A. (2013). Drones and targeted killing. Defining a European position. European Council on Foreign Relations.

U. S. (2021). ARMY *Regaining Arctic Dominance US Army in the Arctic*.

CHIEF OF THE DEFENCE FORCE of Australia. (2016). *Future Operating Environment 2035*.

Frías, C. J. (2017). El sistema internacional y las Fuerzas Armadas en el horizonte 2050 (The international system and the Armed Forces at Horizon 2050). *Documento de Opinión 106/2017*. IEEE.

UK GOVERNMENT. (2021). *Global Britain in a Competitive Age*.

UK GOVERNMENT. (2021). *Defence in a Competitive Age*.

Grissom, A. (2006). The future of military innovation studies. *Journal of Strategic Studies*. 29, no. 5.

Horowitz, M. and Scharre, P. (2015). *Meaningful Human Control in Weapons Systems*. Center for a New American Security.

HUDSON INSTITUTE CENTER FOR DEFENSE CONCEPTS AND TECHNOLOGY. (2020). *Reforming the US Military for a New Era*.

ISDEFE. (2021). *Estudio para la implantación de la inteligencia artificial en el ET* (Study for the Implementation of Artificial Intelligence in the ET, 2021).

CHIEF OF FORCE DEVELOPMENT Canada. (2014). *The Future Security Environment (FSE) 2013-2040*.

JOINT AIR POWER COMPETENCE CENTRE. (2020). *Joint Air and Space Power Conference 2020*.

Jordan, J. (2017). *Grandes tendencias políticas y sociales de interés para la seguridad y la defensa. Perspectivas europeas y norteamericanas*. (Broad political and social trends of interest to Security and Defence. European and North American perspectives.) Research document 01/2017. Future Studies Programme. IEEE.

JOINT CHIEFS OF STAFF United States. (2016). *Joint Operating Environment 2035. The Joint Force in a Contested and Disordered World.*

JOINT CHIEFS OF STAFF United States. (2012). *Mission Command White Paper*.

Kadtke, J. & Wells II, L. (2014). *Policy Challenges of Accelerating Technological Change. Security Policy and Strategy Implications of Parallel Scientific Revolutions*. CTNSP at NDU, DTP 106.

Keegan, J. (2001). *A History of Warfare*. Alfred Knopf (ed.).

KÖRBER-STIFTUNG, INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES. (2019). European Security in Crisis.

Kotter, J. (2002). *The Heart of change*.

Leveringhaus, A. and Giacca, G. (2014). *Robot Wars. The regulation of Robotic Weapons*. Oxford Martin School.

TRAINING AND INDOCTRINATION COMMAND, TE. (2020). *Tendencias 2018-2019* (Trends 2018-2019, 2020).

ALLIED COMMAND TRANSFORMATION (ACT), NATO. (2017). *Strategic Foresight Analysis (SFA) Report*.

ALLIED COMMAND TRANSFORMATION (ACT), NATO. (2018). *Framework for Future Alliance Operations (FFAO)*.

ALLIED COMMAND TRANSFORMATION (ACT), NATO. (2021). *ACT Strategic Foresight Analysis (SFA) Regional Perspectives Report on Russia*.

ALLIED COMMAND TRANSFORMATION (ACT), NATO. (2020). *ACT Strategic Foresight Analysis (SFA) Regional Perspectives Report on North Africa and the Sahel*.

ALLIED COMMAND TRANSFORMATION (ACT), NATO. (2020). *Food for thought paper post COVID-19 global security landscape*.

Marsal, J. (2015). *Tecnologías disruptivas y sus efectos sobre la seguridad*. (Disruptive technologies and their effects on security.) *Annual Research Plan 2015*. Working Document 12/2015. CESEDEN.

MINISTRY OF DEFENCE OF FRANCE. (2020). *Concepto de empleo de las Fuerzas Armadas 2020* (Concept for the Employment of the Armed Forces 2020).

MINISTRY OF DEFENCE OF THE NETHERLANDS. (2020). *Defence Vision 2035. Fighting for a safer future*.

MINISTRY OF DEFENCE OF THE UNITED KINGDOM. (2020). *Science and Technology Strategy 2020*.

NATO ADVISORY GROUP ON EMERGING AND DISRUPTIVE TECHNOLOGIES. (2020). *Annual Report 2020*.

Morales, S. (2017). *El futuro de la naturaleza de los conflictos armados* (The future of the nature of armed conflicts). Framework Document 17/2017. IEEE.

López, P. (2009). Tecnologías disruptivas. Mirando el futuro tecnológico. (Disruptive Technologies. Looking at the technological future.) *Boletín de Observación Tecnológica en Defensa n.º 25*.

Posen, B. R. (1986). *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars*. Ithaca: Cornell University Press.

Prickett, S. (2003). *Developing Operational Leaders for the 21st Century*. Joint Military Operations. Newport (USA): Department Naval War College.

RAND CORPORATION. (2020). *The Future of Warfare*.

REAL INSTITUTO ELCANO. (2020). *España y la crisis del coronavirus: Una reflexión estratégica en el contexto europeo e internacional* (Spain and the Coronavirus Crisis: A Strategic Reflection in a European and International Context, 2020).

Richards, Ch. (2001). *A Swift, Elusive Sword: What If Sun Tzu and John Boyd Did a National Defense Review*. Center for Defense Information.

Riola, J. M. (2015). *Tecnologías disruptivas y sus efectos sobre la seguridad* (Disruptive technologies and their effects on security.) Annual Research Plan. Working Document 12/2015. CESEDEN.

UN SECRETARY-GENERAL. (2004). *A more secure world: our shared responsibility.* Report of the High-level Panel on Threats, Challenges and Change.

NATO SECRETARY-GENERAL. (2020). *NATO 2030: United for a New Era*.

Serra, J. (2013). *Liderazgo creativo: una receta para las Fuerzas Armadas del siglo XXI* (Creative leadership: a recipe for the Armed Forces of the 21st-century). Monograph no. 136. *El liderazgo en las Fuerzas Armadas del siglo XXI (Leadership in the Armed Forces of the 21st century)*. ESFAS.

Simon, L. (2016). The third US Offset Strategy and Europe's Anti-Access Challenge. *The Journal of Strategic Studies*. Institute for European Studies. Vrije Universiteit Brussels.

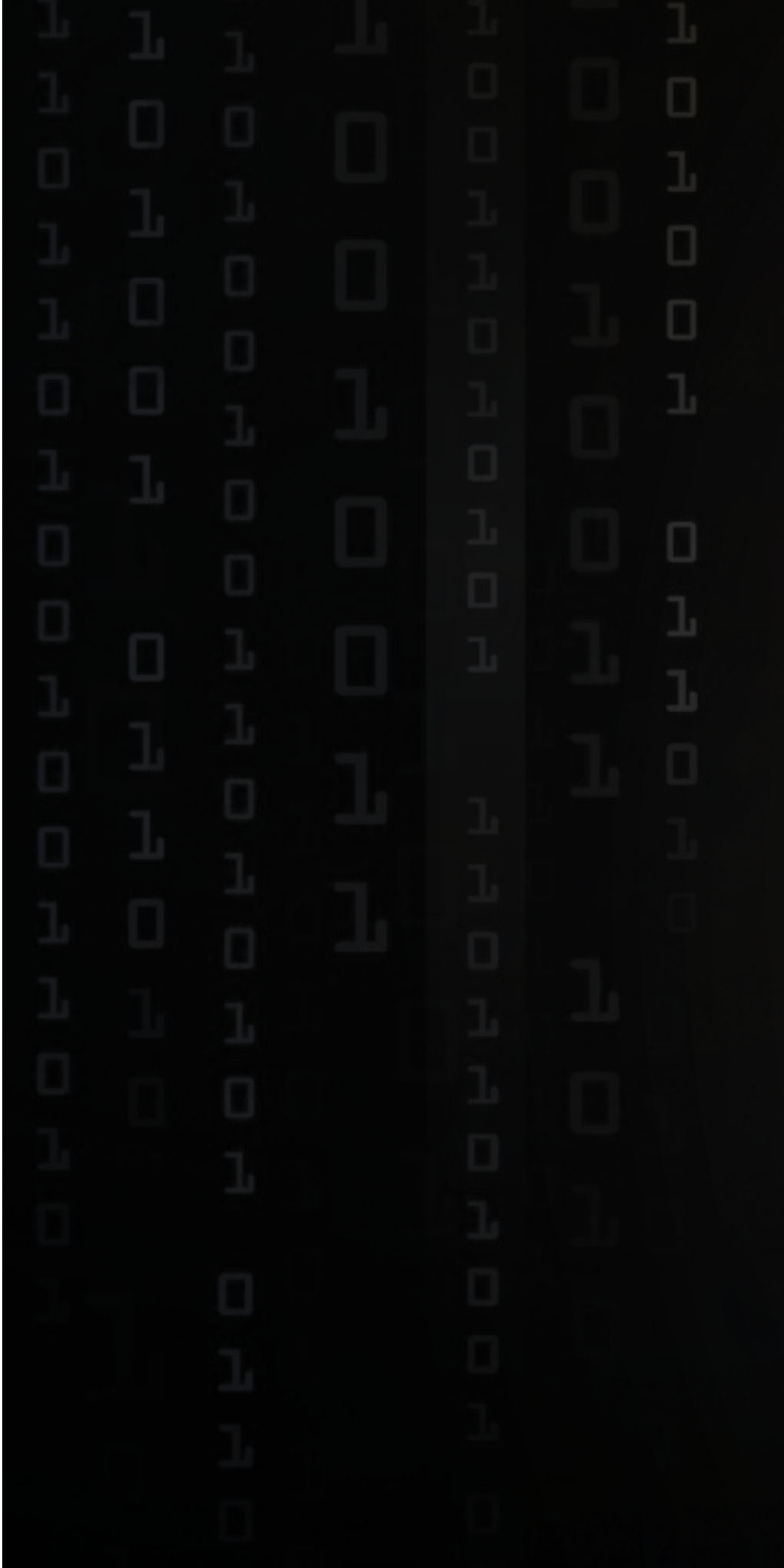
THE HAGUE CENTRE FOR STRATEGIC STUDIES. (2021). *The Implementation of Robotic and Autonomous Systems: The Future is Now, prepare for 2045*.

Toffler, A. & H. (1993). *War and Anti-war. Survival at the Dawn of the 21st Century*. Little, Brown and Company.

EUROPEAN UNION. (2016). *Shared vision, common action: A Stronger Europe*.

Villena, C. (2014). El impacto de las nuevas tecnologías y las formas de hacer la guerra en el diseño de las Fuerzas Armadas (The impact of new technologies and ways of waging war on the design of the Armed Forces). Security and Defence Documents, no. 61. CESEDEN.

WORLD ECONOMIC FORUM. (2021). *The Global Risks Report 2021*. 16th edition.



PUBLICACIONES
Pd
DE DEFENSA

GOBIERNO
DE ESPAÑA

MINISTERIO
DE DEFENSA

SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

SUBDIRECCIÓN GENERAL
DE PUBLICACIONES
Y PATRIMONIO CULTURAL