Operating environment 2035

MINISTERIO DE DEFENSA

Operating Environment 2035

MINISTRY OF DEFENCE

Concepts Development Joint Centre (CCDC)
http://www.defensa.gob.es/ceseden/ccdc/

GENERAL CATALOGUE OF OFFICIAL PUBLICATIONS
https://cpage.mpr.gob.es

Published by:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

https://publicaciones.defensa.gob.es/

NIPO: 083-19-149-8 (e-book edition)
NIPO: 083-19-150-0 (online edition)

Publication date: May 2019
Layout: Ministry of Defence

CONTENTS

OPERATING ENVIRONMENT 2035

Summary

Knowing where and how global trends in the different political, social, technological, environmental and legal arenas will meet and, above all, compete will allow us to begin to understand possible future crises or conflicts. The interaction of these trends in areas of national interest will create situations with varying degrees of cooperation, competition and conflict that will shape the operating environment of 2035.

The Armed Forces will continue to be one of the foremost instruments available to democratic states for intervening in conflicts, ensuring the defence of their own countries and their allies' and contributing to international stability. However, the change envisioned in the characteristics of the operating environment that lies ahead are of such magnitude that it makes it very difficult to predict how armies should operate in the future and what characteristics they require to adapt to this change.

The main purpose of this document is to reflect on the characteristics of the Operating Environment in 2035, the possible scenarios or contexts where military operations will take place and the changes that our Armed Forces must confront to adapt successfully to this uncertain, complex environment.

Key words

Operating Environment, Armed Forces, Future, Prospects, Strategy, Military Implications, Scope of Action, Military Operations, Operational Scenarios, Adaptation, Transformation, Trends, Security, Defence, Dissuasion, Surveillance, Prevention, Response, Technology, Challenges, Vulnerabilities, Budgetary Instability, Lack of Modernization, Undercapitalization, Opportunities, Innovation, Interoperability, Joint Action, Optimization, Strategic Agility, Talent Management, Organization, Military Capabilities, 2035.

FOREWORD

A little over a year ago, the 2017 "Futures Programme" of the Higher School of National Defence Studies (CESEDEN) marked the beginning of the studies that have culminated in the development of this document. *Operating Environment 2035* is the result of collaborative work by a large number of experts from the Spanish Armed Forces (SAF), the Civil Guard, academia and industry, led by the Joint Centre for the Development of Concepts (CCDC), to try to understand the complex, uncertain world that lies ahead, in which the military must cooperate with the other instruments of national power to address the multi-faceted challenges that will go beyond the traditional field of Defence into that of Security.

CHIEF OF THE DEFENCE STAFF,
Army General Fernando Alejandre Martínez

For this reason, I would like to start by expressing my thanks to all those who took part in this process and gave their support so that this document could be more complete, realistic and objective.

The purpose of the Armed Forces is to provide a capable, effective Joint Force (JF) but the uncertainty and the need for constant adaptability demanded by the future operating environment make change the only constant in the search for that goal. This document therefore serves as a forward planning tool for promoting and inspiring the "change" that every organization requires so as not to remain anchored in the past.

The document does not seek to predict the future with any accuracy, as this is impossible, instead, using the foreseeable characteristics of the 2035 operating

environment, the document seeks to promote a creative debate and conduct an in-depth analysis so as to provide long-term guidelines for the lines of action, determine the strategic framework, reflect on the doctrine, plan the capabilities, develop the concepts and train the forces.

Writing the foreword to this document therefore gives me an opportunity to present an up-to-date vision of the commitment of the Armed Forces to the present and future of Spain, on the one hand, and, on the other, to answer the question of what kind of armed forces Spain will need in the 2035 operating environment.

This document, therefore, describes the characteristics that the Armed Forces must have in 2035 to address the future scenarios of the use of force, based on the criteria of feasibility and sustainability. With these characteristics, the military force will be able to confront the foreseeable challenges and the opportunities that will present themselves, seek areas for increasing the efficiency of the organization, modernizing the equipment and systems, or improving the ability to conduct integrated operations with the other instruments of state power and the other protagonists in the *National Security Strategy*, law enforcement, diplomats and individuals from the administration, industry and academia.

To conclude, I will add that the ideas reflected in this Operating Environment 2035 will allow us prepare to ensure that in 2035 our Armed Forces continue being the main guarantors of our sovereignty, independence, territorial integrity, constitutional order, international importance, progress and well-being, and, ultimately, freedom in 2035.

Madrid, 28 December, 2018

CHIEF OF THE DEFENCE STAFF
Army General Fernando Alejandre Martínez

EXECUTIVE SUMMARY

Knowing where and how global trends in the different political, social, technological, environmental and legal arenas meet and, above all, compete will allow us to begin to understand possible future crises or conflicts. How these trends interact with national interests will create situations with varying degrees of conflict, competition and cooperation that will shape the operating environment of 2035.

However, in spite of all the difficulties involved in predicting the future accurately, it is possible to state unequivocally that the military will continue to be one of the main instruments of democratic states for intervening in conflicts, guaranteeing the defence of their country and their allies', protecting national interests wherever these are found, contributing to international stability and providing the public with security and well-being.

Fortunately, our Armed Forces (SAF) have successfully adapted to the characteristics of the theatres of operations in which they have been involved in recent years. However, the changes that lie ahead are of such magnitude that it makes it very difficult to predict how services will need to operate in the future and what characteristics they will require to adapt to these changes.

The main purpose of this document is to reflect on the characteristics of the Operating Environment (OE) of 2035, the possible operational scenarios by the Armed Forces and the changes involved in adapting successfully to that uncertain, complex environment.

The **first section** analyses the **challenges** of the future operating environment, summarizing them as the risks, vulnerabilities (essentially, budgetary instability and a lack of up-to-date materiel, which could result in the decapitalization of the Armed Forces) and threats that compromise national security, including international armed conflicts, fragile or failed states, organized crime, terrorism, the proliferation of weapons of mass destruction, cyberattacks and manipulation and disinformation campaigns.

This document studies the promising **opportunities** that the Armed Forces needs to exploit in this environment have been studied, such as technological innovation, internal and international cooperation initiatives and the ability to understand the

situation, which will allow them to intervene beforehand to prevent conflicts or react efficiently to resolve them.

It also reviews some of the most decisive **features** that are believed will characterize OE 2035. They include the continuation and even intensification of crises and conflict; the increasing and increasingly diverse number of players with an ability to influence regional and international affairs; the strengthening of cooperation on security and defence both at home and abroad; the continuation of conventional strategies and an increase in non-conventional and hybrid strategies so as to gain an advantage over opponents; possible changes in military organizations to flatter, more horizontal structures so as to set a faster pace for operations, principally motivated by the appearance of these non-conventional threats or strategies and by technological developments in command and control systems; the retention of the traditional domain of physical operations together with a predominant use of cyber and cognitive domains; the use of densely populated urban areas as the preferred sites for confrontation; varied access to anti-access and aerial denial (A2/AD) systems by a larger number of countries; the militarization of outer space and, lastly, technological development.

The **second section** provides the **Operational Scenarios (OS) by the Armed Forces** in 2035. The Armed Forces will continue protecting national security interests, which, even though they may change throughout history, tend to remain in place for long periods of time. It is therefore predicted that in 2035, such interests will be similar to nowadays', namely those relating to national sovereignty, in which the asset protected is the Spanish Nation; those linked to achieving a stable international order with peace, security and respect for human rights; and those that affect the lives, safety, well-being and prosperity of the Spanish people, where the asset protected is the population.

To defend these interests, the armed forces will operate in the following scenarios:

- **OS 1 Dissuasion, Surveillance, Prevention and Response**, which is the raison d'être of the Armed Forces and where their mission leads to reactive operations in response to aggression and threats and on-going, preventive operations, i.e., the routine (24/7) performance of many activities of surveillance, security and control of sovereign maritime and air space.
- **OS 2 Projection of Stability Abroad**, in which, through operations involving peacekeeping and humanitarian aid, stabilization and support for development or, if necessary, collective defence, the Armed Forces defend our national security interests beyond our borders.
- **OS 3 Public Safety and Well-Being**, in which the Armed Forces carry out their mission through cooperation with other instruments of state power to contribute to security (terrorism, organized crime, cyberattacks, emergencies and catastrophes, non-combatant extraction operations (NEO) and state action (civil defence, support for scientific activities, customs supervision, etc.).

The third and final section studies the **characteristics that the Armed Forces should have in 2035** in order to perform their duties successfully: some are general, such as agility, feasibility, sustainability, efficiency and a strong information management capability; others are specific to each OS, such as credibility and resilience in OS 1, strategic mobility and interoperability in OS 2 and flexibility and interoperability in OS 3.

The final part of this section analyses the **changes needed in the Armed Forces** so that they can constantly adapt to OE 2035. A balanced application of innovative changes to "people, ideas and tools" are required Following the different areas of DOTMLPF-I (the acronym in Spanish for Materiel, Facilities, Personnel Resources, Training, Doctrine, Organization and Interoperability), a relationship is established between "people" and human resources, training and organization, between "ideas" and doctrine, and between "tools" and materiel and facilities. Last, but not least, this document analyses potential areas of change to be implemented in the AF as a result of the OE 2035.

The choice of 2035 is not arbitrary. In addition, this time frame is similar to what allied countries use for prospective analysis; in addition, a period longer than 15 years forms part of what Defence Planning rules consider to be "long-term" when planning military capabilities that will be required, depending on the foreseeable strategic and operating environments.

2035 is "just around the corner" and, the huge rate of change, due to scientific and technological innovation, will probably affect all facets of life, including the military; as such, many of the ideas that will be discussed in this document have their roots in the present. Given the openness of the future, the intention behind this document was to propose possible situations in which the future may evolve, as dogmatic assertions would not stand up even in the near future.

Foresight is not a way of guessing or making predictions about the future based on the successes and failures of what has already been tried. It is a complex process of research and anticipatory reflection about the possibilities that the different possible futures offer. Foresight purpose is to have, in the present, a logical explanation of a reality that is better than the one provided solely by knowing the past and analysing the present and the forecasts that are within our reach.

In its Annual Research Plan, the National Defence Advanced Studies Centre (CESEDEN) designed a "Future Works" programme that tasked the Spanish Institute for Strategic Studies (IEEE) with writing a document that would include global geopolitical trends in the period between 2019 and 2040; such programme also tasked the Concepts Development Joint Centre (CCDC) with writing one defining the operating environment in 2035, to be understood as the set of circumstances that identify changes in conflicts and the way of approaching them, with the aim of viewing how the on-going process of change within the Armed Forces should be approached in order for them to adapt to that environment.

This latter document, entitled "*Operating Environment (OE) 2035*", is a prospective study of the future, from an essentially military strategic perspective, in order to influence it and to help decision-makers regarding the future design of the Armed Forces, so that they will be able to counteract or minimize the challenges and take advantage of the opportunities that these future scenarios will offer.

As a result, taking into account the current context and the forecast evolution of events, that in the operating environment of 2035 crises and conflicts are considered very likely to continue between actors who will fight to pursue their interests; that the military forces of the democratic countries will continue to be one of the main players in assuring the defence of their countries, preservation of international peace and stability, and the safety and well-being of their citizens.

The **first objective** of this document, in line with those already published in neighbouring countries, is to present ideas that will make it possible to look in depth and understand in advance the possible and most important future occurrences of a strategic nature. It will also facilitate to make decisions in the present that will allow us to inspire and offer guidelines for the design of the Armed Forces of the future, thereby contributing to their continuing adaptation to the new environment, so that they can confront with a certain guarantee of success an uncertain, complex future.

The **second** but no less important objective consists of contributing to disseminating the awareness of defence, by presenting to society the challenges and threats that could put its stability and well-being at risk in the near future and defending the view that protecting our national security interests with the active collaboration of the Armed Forces is necessary, important and legitimate.

Methodologically, the starting point was the trend analysis made by the IEEE in its document "*Panorama of geopolitical trends. Horizon 2040*" and a detailed review of a wide variety of studies similar to *OE 2035* made by the armed forces of neighbouring countries -bibliographical research)-.

In the second stage, 94 experts from various military organizations collaborated on a process that used data acquisition software to refine and enhance the conclusions obtained in the previous stage -bibliographical review-.

Then, individuals from business and the universities also took part in the third stage. The aim was to have alternative, critical interpretations so as to obtain a more objective document that was open to new ideas and would make it possible to anticipate possible "black swans[1]"[1] in areas outside the military that could however have a powerful impact on security and defence.

The document is **organized** into three chapters:

Chapter 1, "CHARACTERISTICS OF THE FUTURE OPERATING ENVIRONMENT" defines the key factors that will foreseeably shape the operating environment of 2035. These factors are listed by subject: lines of action, operational domains; resources and

[1] The Black Swan theory is a metaphor that describes an event that comes as a surprise (to the observer), has a major effect, and is often inappropriately rationalized after the fact with the benefit of hindsight.
The theory was developed by Nassim Nicholas Taleb to explain:
The disproportionate role of high-profile, hard-to-predict and rare events that are beyond the realm of normal expectations in history, science, finance and technology.
The non-computability of the probability of consequential rare events using scientific methods (owing to the very nature of small probabilities).
The psychological biases that make people blind, both individually and collectively, to uncertainty and to the huge role played by rare events in historical affairs.
Unlike the earlier black swan problem in philosophy, the Black Swan Theory (in capitals) refers only to unexpected events of great magnitude and consequence and their dominant role in history. Such events, considered extreme outliers, collectively play vastly larger roles than regular occurrences.

capabilities; challenges and opportunities; operations or missions, and other variables that determine the way in which armed conflicts may possibly arise.

Chapter 2, "OPERATIONAL SCENARIOS OF ACTION BY THE ARMED FORCES" lists the contexts in which the Armed Forces will operate in 2035 to protect and guarantee national security and defence interests.

Chapter 3, "NEED FOR CHANGES IN THE ARMED FORCES TO ADAPT TO OE 2035" analyses the implications of changes to the Armed Forces, so that they can confront the challenges of the future operating environment with a greater probability of success.

Lastly, it should be noted that *OE 2035* is not a final product; it will be subject to an on-going process of revision and updating, originally set at every three years, in order to synchronise publication of updated editions with the beginning of the defence planning cycles. Nevertheless, whenever circumstances make it advisable, new revisions will include ideas and concepts that will lead to changes in the future operating environment, thus facilitating the on-going process of adapting the Armed Forces.

CHAPTER 1
CHARACTERISTICS OF OPERATING ENVIRONMENT 2035

"Lucky chance is usually nearly always the prize of persistent effort."

Santiago Ramón y Cajal

1. Challenges of Operating Environment 2035

01 The aim of this document, *OE 2035,* is not to make an internal analysis of the Armed Forces, or to determine possible strategies or lines of action to be implemented by them to meet their objectives. Its main aim is to make an external analysis of the operating environment[1] in which the Armed Forces will predictably operate in 2035, by determining the challenges or negative or adverse situations outside the organization that could affect it and the opportunities or positive factors created in the environment that, once they have been identified, can be exploited.

02 Recent documents from friendly nations and allies about "futures" describe the future geopolitical and security scenario based on the characteristics of Volatility, Uncertainty, Complexity and Ambiguity (VUCA) environments (Figure 1), which, although they exist now, really belong to the future and, in all probability, will even have intensified by 2035.

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

[1] As stated above, the geopolitical factors addressed by the Spanish Institute of Strategic Studies (IEEE) in its document "Panorama of geopolitical trends. Horizon 2040" have been taken into account.

03 The **volatility** of a situation leads to swift changes that make it difficult to identify trends or patterns. These changes also reduce the stability of existing processes, although these difficulties can be countered by a proper evaluation and identification of the most decisive patterns of change with the greatest impact on security.

04 Most of the important changes that are occurring (Brexit, the refugee crisis, the emergence of populism, the progressive displacement of the strategic centre of gravity to the Pacific, the new use of information and associated technologies as a weapon, such as fake news, etc.) are disruptive and their consequences, as yet unknown, are leading to **uncertainty**, which makes it difficult to anticipate new events, prepare for future scenarios, form a balanced view of the emergence of new risks and threats to security, and know how to take advantage of the innumerable opportunities that the future could bring. It will therefore require an understanding of the situation to plan for and anticipate unexpected situations, avoiding reactive, short-term decisions.

05 Each event that is in turn interrelated with other possible, later events is determined by a multiplicity of causes and factors that are increasing the **complexity** of the modern world and lessening the possibility of having a comprehensive knowledge of the relationships that govern how it works, making it difficult to make the right decisions for the future. It will be necessary to get away from stereotypes and simple, unique solutions; on the contrary it will be required to act with an open mind, with a vision of the future and holistic thinking, using methodologies and tools that make it possible to approach the analysis and synthesis of complex problems systematically.

06 Lacking a knowledge of the situation makes it difficult to give an unequivocal, appropriate answer to the key questions (who, where, why, when and how). The **ambiguity** makes it difficult to correctly identify the causes and effects of events and, therefore, to make the right decisions. Agility makes possible to react with flexibility and adaptability to unknown or confusing situations.

07 Like the *2017 Spain's National Security Strategy (NSS)*, which, in chapter 4, identifies the main threats and challenges to national security, this document will analyse the challenges for the military operating environment in the year 2035. For the purposes of classification, these have been divided into: **(1) risks, (2) vulnerabilities, (3), ethical and legal aspects, and (4) threats.**

1.1. Risks

08 According to *NSS 2017,* **risks** are situations that "without being threats in themselves, increase vulnerability, create situations of instability, or may foster the emergence of other threats aggravate them or accelerate their fruition". Among these we should highlight the possible disintegration of the political, economic and social system of some African countries; the demographic imbalance between Europe and Africa; the migratory pressures from the southern shores of the Mediterranean; poverty and the unequal distribution of wealth in Spain and between Spain and North Africa; the fight for natural/energy resources; the effects of climate change on this country

and the Mediterranean region; possible industrial and natural emergencies and catastrophes; possible epidemics and pandemics, etc. In the operating environment of 2035, which is potentially more unstable than the preceding one, the emergence and development of these risks among potential rivals could create a chain effect of new threats.

2. Vulnerabilities

09 The **vulnerabilities** arising from our country's geographical, socio-political, economic and technological situation will require the adoption of measures to minimize them, if we want to prevent their turning into threats to our security and defence. Sharing borders or interests, respectively, with extremely unstable regions like the Maghreb and Sahel; the vulnerability of our supply lines; the problems of territorial cohesion inside Spain; Spain's low birth rate and demographic situation; the high dependency on energy from abroad; the lack of awareness in Spanish society of security and defence; the intrinsic vulnerability of critical infrastructure and essential services, due to their generalized connectivity; and the limited resources set aside for innovation and investment in technology (in disruptive areas, space capabilities, the modernization of the Armed Forces materiel, etc.), which could put our strategic autonomy and interoperability with our allies at risk. All these vulnerabilities are negative internal elements that would weaken our stability and lead to a situation of insecurity.

2.1. Ethical and legal aspects

10 The present-day **ethical and legal aspects** that govern crises and armed conflicts could pose a significant challenge to the operation of Western Armed Forces in 2035, if the appropriate actions are not taken to adapt legislation to fit the requirements of the new operating environment. The unstoppable development of science and technology; the cultural changes in society's way of viewing the use of violence in armed conflicts; the new codes of human behaviour; emerging threats or unstable situations; the changing character of conflict; the new hybrid strategies, etc. will have important consequences for the question of whether the current principles of International Humanitarian Law (IHL), such as distinction[2], proportionality, military necessity and the prevention of unnecessary suffering, among others, will also be applicable to the 2035 operating environment.

11 On the other hand, the debate on the need to implement **new international regulations** governing the use of force should address issues like responsibility for causing civilian casualties; the possibility that robots would harm civilians or cultural assets and the foreseeable negative consequences of the application of artificial intelligence to the decision-making process; implementing lethal capabilities in autonomous systems; genetic engineering and improving the physical conditions of combatants; discriminating between combatants and non-combatants in densely populated areas

[2] Distinction between civilians and combatants, and between civilian objects and military objectives

(big cities, on the coasts, etc.), in cyberspace or in "grey areas[3]" or hybrid strategies; the regulation of certain actions in cyberspace or on the electromagnetic spectrum; the responsibility of states for "proxy wars"; the commitment of the NATO countries to missions outside its territory; the appearance of collateral damage; the dichotomy of states for guaranteeing the exercise of individual freedoms and the security of their societies; etc.

12 The appearance of threats and hybrid strategies, the increasing trend toward non-conventional forms of conflict and the blurring of the traditional borders between peace and war also pose **new ethical and legal challenges**. The quantitative and qualitative difference between the Western Armed Forces and those of potential adversaries could lead to the latter justifying and using certain weapons, strategies, techniques, resources, etc. foreign to the norms, rules and uses of current IHL, which should lead us to develop ethical and legal responses (possibly leading to a certain "legal asymmetry" between the public and the aggressors) that would fit those new situations.

---

[3] PDC-01 (A). A "grey area" is the one in which "the spectre of conflicts in which actions on the margin of the principle of good faith between states (*bona fide*) predominate, which, in spite of noticeably disturbing the peace, do not cross the thresholds that would permit or require an armed response". The size of this grey area grows with "legal loopholes or excessively protectionist regulations, political, social, organizational weaknesses and the resilience of states, the bureaucratization of conflict management and the complexity of the decision-making process."

13 However, it would not be appropriate to drift into a very restrictive legal framework in response to the changes ahead, as this could result in the systematic infringement of the rules by states, either through the use of force or the production and use of certain weapons and munitions, thereby minimizing the effectiveness of a legal system that aims to protect people.

2.2. Threats

14 According to *NSS 2017,* threats "jeopardize or undermine national security" and their occurrence could require the reaction or intervention of the Armed Forces, autonomously, as part of the international security and defence organizations (ISDO) of which Spain is a member or to support other instruments of the state. The following are the principal threats:

15 **Armed international conflicts** (Figure 2). Although it is considered that the probability of classic confrontations between states will lessen in the future, the possibility cannot be ruled out that some of the contenders might consider using, at least partially, a combination of conventional, non-conventional and hybrid methods and strategies, to which the capability, organization and doctrine of the Armed Forces would need to adapt. It could also happen that the opposing sides would escalate their use of force and destabilize the security environment, triggering a major conflict.

Figure 2: International Armed Conflicts[			
2035 Operating Environment	**WHO?**	Potential adversaries	State actors
	WHAT?	Interest threatened	Territorial integrity and national sovereignty. International and regional security and stability. Collective defence
	WITH WHOM?	Autonomously	Yes
		Internal partnerships	Other instruments of national power
		External partnerships	ISDO (NATO, EU), multilateral, minilateral and bilateral agreements on cooperative security
	WHERE?	Regions	National territory, NATO and EU areas of interest and territory of nations with standing cooperative security agreements.
		Domains	Land, sea, airspace and cyberspace
	HOW?	Adversary's lines of action	Conventional, non-conventional and hybrid
		Own lines of action	Conventional and hybrid
	WITH WHAT?	Adversary's resources/ capabilities	Command and control, information and anticipation, confrontation, protection, projection, support
		Own resources/ capabilities	Command and control, information and anticipation, confrontation, protection, projection, support

16 **Fragile and failed states** (Figure 3) constitute a significant threat that could destabilize the security of the region. With the rise of globalization, the threats tend to become global and the search for solutions to them involves a coordinated international effort, normally through the ISDOs to which the countries belong.

17 The geographical position of Spain and the possibility of having failed states close by could have serious consequences for our interests, such as a huge, uncontrolled flow of refugees toward our borders, an insecure electricity supply and the possible use of those fragile or failed states as refuges for non-state actors who would threaten national and international security and even provoke armed conflicts close to our borders.

Figure 3: Fragile or failed states

2035 Operating Environment	**WHO?**	Potential adversaries	State and non-state actors (terrorist organizations and organized crime, proxies, etc.)
	WHAT?	Interest threatened	Safety and well-being of Spanish residents. International, regional and national security and stability.
	WITH WHOM?	Autonomously	Yes
		Internal partnerships	Other instruments of national power
		External partnerships	ISDO (NATO, EU), multilateral, minilateral and bilateral agreements on cooperative security
	WHERE?	Regions	NATO and EU areas of interest and those of nations with which there are cooperative security agreements
		Domains	Land, sea, airspace and cyberspace
	HOW?	Adversary's lines of action	Conventional, non-conventional and hybrid
		Own lines of action	Conventional and hybrid
	WITH WHAT?	Adversary's resources/ capabilities	Command and control, information and anticipation, confrontation, protection, projection, support
		Own resources/ capabilities	Command and control, information and anticipation, confrontation, protection, projection, support

18 One of the non-state actors that normally exploits the vulnerabilities of fragile and failed states (corruption in the administration, insecurity and lack of police control, etc.) is international **organized crime** networks (Figure 4), which operate with total impunity in the illegal trafficking of people, drugs, weapons, etc. These networks can also be involved in piracy, attacks against shipping and mass illegal immigration, and even be connected to terrorism as a source of financing. In addition, these criminal networks may be used by third states, which conceal the former's criminal activities under external political action. All of the above gives non-state actors tremendous potential for destabilizing the regions in which they operate. The geographical location of Spain as a "port of entry" to the EU makes it especially vulnerable to criminal organizations from America and Africa, especially the Maghreb, Sahel and Gulf of Guinea.

Figure 4: Organized Crime			
2035 Operating Environment	**WHO?**	Potential adversaries	State actors (proxies) and non-state actors
	WHAT?	Interest threatened	Public safety and well-being. International, regional and national security and stability.
	WITH WHOM?	Autonomously	Yes
		Internal partnerships	Law enforcement agencies
		External partnerships	ISDO (NATO, EU), multilateral, minilateral and bilateral agreements on cooperative security
	WHERE?	Regions	National territory, NATO and EU areas of interest and those of nations with which there are cooperative security agreements
		Domains	Land, sea, airspace and cyberspace
	HOW?	Adversary's lines of action	Non-conventional and hybrid
		Own lines of action	Conventional and hybrid
	WITH WHAT?	Adversary's resources/ capabilities	Apt for irregular confrontation
		Own resources/ capabilities	Command and control, information and anticipation, confrontation, protection, projection, support

19 These organizations have succeeded in equipping themselves with some purely military resources (conventional and CBRN weapons, pocket submarines, unmanned aerial vehicles, signal intelligence, etc.) and above all in efficiently exploiting cyberspace for their operations, which makes them into a dangerous threat for the security of countries, requiring a significant police effort to combat them and, possibly, the support and cooperation of the Armed Forces.

20 Future conflicts will be characterized by asymmetric progression trends, two threats are of particular importance: **terrorism** and the proliferation of **weapons of mass destruction (WMD)**.

21 The significance of **terrorism** (Figure 5) lies in the probability of this threat increasing due to the predictable future rise of radicalism, whether political, ideological or religious, and in the use by terrorists of very varied and innovative methods, which would make preventing them difficult.

22 To reach their political, religious or ideological aims, terrorism will continue to be used by non-state groups and actors. In addition, it is very probable that certain states will continue to use terrorism, through their **proxies**, in "proxy wars" to promote their own political interests.

23 Terrorism restricts the normal functioning of societies and forces nations to increase the size of their **police forces**; also, Armed Forces could be required to support police on certain missions or with certain capabilities or to help to prevent the appearance and expansion of all types of radicalism on an international scale.

24 Technological knowledge will become increasingly widespread because of the Internet and it must be assumed, without a shadow of doubt, that the weapons and substances that can be obtained on-line will be used. In principle, it is forecast

that the use of conventional weapons and chemical, biological, nuclear and radiological (**CBRN**) agents or products will continue to be an option for terrorists, together with innovations in the areas of robotics, nanorobotics, unmanned systems and electromagnetic pulse (EMP), among others.

Figure 5: Terrorism			
2035 Operating Environment	WHO?	Potential adversaries	State actors (proxies) and non-state actors
	WHAT?	Interest threatened	Public safety and well-being. International, regional and national security and stability
	WITH WHOM?	Autonomously	Yes
		Internal partnerships	Law enforcement agencies
		External partnerships	ISDO (NATO, EU), multilateral, minilateral and bilateral agreements on cooperative security
	WHERE?	Regions	National territory, NATO and EU areas of interest and those of nations with which there are cooperative security agreements
		Operating areas	Land, sea, aerospace, cyberspace and cognitive space
	HOW?	Adversary's lines of action	Non-conventional and hybrid
		Own lines of action	Conventional and hybrid
	WITH WHAT?	Adversary's resources/capabilities	Apt for irregular confrontation
		Own resources/ capabilities	Command and control, information and pre-emption, confrontation, protection, projection, support

25 After the almost complete disappearance of ETA sponsored terrorism, the main terrorist threat, violent extremist organizations will pose the main terrorist threat

26 In the coming years there will likely be a **proliferation of weapons of mass destruction (WMD)** (Figure 6) and their delivery systems, due to the increasing number of countries with this capability. Because some WMD can be easily manufactured, WMD will increasingly become the weapon of states and non-state actors that wish to achieve regional or global political objectives.

Figure 6: Weapons of Mass Destruction (WMD)			
2035 Operating Environment	WHO?	Potential adversaries	State actors (proxies) and non-state actors
	WHAT?	Interest threatened	Public safety and well-being. International, regional and national security and stability
	WITH WHOM?	Autonomously	Yes
		Internal partnerships	Other instruments of national power
		External partnerships	ISDO (NATO, EU), multilateral, minilateral and bilateral agreements on cooperative security
	WHERE?	Regions	National territory, NATO and EU areas of interest and those of nations with which there are cooperative security agreements
		Operating areas	Land, sea, airspace
	HOW?	Adversary's lines of action	Non-conventional
		Own lines of action	Conventional
	WITH WHAT?	Adversary's resources/capabilities	Apt for irregular confrontation
		Own resources/ capabilities	Command and control, information and anticipation, confrontation, protection, projection, support

27 The breaking of the nuclear status quo by some powers and the proven trend toward the irrational use of increasingly lethal violence by certain terrorist groups makes WMDs one of the most dangerous risks for the future security environment. As chemical, biological and radiological weapons have appeared, nuclear weapons have ceased to be the only concern and, in addition, although it is true that the risk of complete annihilation that existed during the Cold War has lessened, the possibility of **massive, indiscriminate attacks** has grown. Concern regarding the proliferation of WMDs comes from the possibility that there may be launch vectors in the hands of uncontrolled groups in North Africa, which would allow them to hit parts of Spain.

28 Another of the most striking threats in the future operating environment will be **cyberattacks and manipulation and disinformation campaigns**, as a result of the emergence and territory of nations with standing cooperative security agreements.

29 **Cyber threats** (Figure 7) can come from three different actors: States, non-state actors or "hacktivists" and isolated individuals.

30 There is a great variety of **cyber potential targets**, from government networks and systems (government departments and critical national infrastructure) to non-government ones, to which great damage can be done in a relatively easy and economical manner. The exposure to these attacks will increase proportionally to the growing dependency on technology and telecommunications networks.

Figure 7: Cyber Threat

2035 Operating Environment	**WHO?**	Potential adversaries	State and non-state actors (terrorist/ criminal/hacktivist groups and isolated individuals)
	WHAT?	Interest threatened	National sovereignty. Public safety and well-being. International, regional and national security and stability
	WITH WHOM?	Autonomously	Yes
		Internal partnerships	Other instruments of national power
		External partnerships	ISDO (NATO, EU), multilateral, minilateral and bilateral agreements on cooperative security
	WHERE?	Regions	National territory, NATO and EU areas of interest and those of nations with which there are cooperative security agreements
		Operating areas	Cyberspace
	HOW?	Adversary's lines of action	Non-conventional
		Own lines of action	Conventional
	WITH WHAT?	Adversary's resources/ capabilities	Apt for irregular confrontation
		Own resources/capabilities	Defence, exploitation and attacks in cyberspace, training and awareness-raising

31 The difficulty in countering cyberattacks lies in their constant evolution, growing sophistication, identifying and locating the aggressor. This threat is **transversal**, since it can be used by other threats with a significant multiplier effect. The Armed Forces telecommunication systems and information systems could

be compromised by this threat as it would affect the efficiency of planning and carrying out operations.

32 The aim of **manipulation and disinformation campaigns** (Figure 8) is to "influence" societies, especially the psyches of the individuals who make them up, by directly targeting their opinions, attitudes, wishes, visions, beliefs, feelings, etc., in order to shape them and use them for their own interests by distorting people's perception.

33 There are those who consider that elections in constitutional systems are **critical infrastructure**[4], since interference in them, with the aim of biasing the result of some elections to favour the interests of outside actors, is clearly a threat to the "efficient functioning of state institutions and government departments" that not only destabilizes the country but also goes against the very core of interests that are vital to a nation, such as sovereignty, independence and unity.

34 These practices are known to have been used by third countries, through their intelligence services. What is "new" is technological innovation, which has led to the **emergence of cyberspace** as the most efficient medium for projecting state power through manipulation and disinformation campaigns.

Figure 8: Manipulation and Disinformation Campaigns

2035 Operating Environment	**WHO?**	Potential adversaries	State and non-state actors
	WHAT?	Interest threatened	National sovereignty and constitutional order. Public safety and well-being. Stability and national security
	WITH WHOM?	Autonomously	Yes
		Internal partnerships	Other instruments of national power
		External partnerships	ISDO (NATO, EU), multilateral, minilateral and bilateral agreements on cooperative security
	WHERE?	Regions	National territory
		Operating areas	Cyberspace and cognitive
	HOW?	Adversary's lines of action	Non-conventional
		Own lines of action	Conventional
	WITH WHAT?	Adversary's resources/ capabilities	Apt for irregular confrontation
		Own resources/ capabilities	Command and control, information and anticipation, confrontation, protection, projection, support

[4] Law 8/2011, of 28 April, establishing measures for the protection of critical infrastructure. Art. 2, e) defines critical infrastructure as being "the strategic infrastructure whose functioning is indispensable and does not permit alternative solutions, so that any disturbance or destruction of it would have a serious impact on essential services". Art. 2, a) defines essential services as "the service needed to maintain basic social functions, healthcare, security, the social and economic well-being of the public, or the effective functioning of state institutions and the public administrations".

35 On a more practical level, manipulation and disinformation campaigns would try to influence Western public opinion by undermining the **cohesion of their countries' alliances or coalitions,** the legitimacy of their military operations, the morale of their societies when faced with losses, the financing for and motivation of their armies, etc.

36 To supplement the preceding identification of the challenges to national security, we should remember the words of the former US Secretary of Defence, Donald Rumsfeld, who considered that, due to the rate of change in a globalized world, it was difficult to determine and characterize those that will pose problems in the coming years, although three types could be distinguished: those that we know about but do not know when they might develop (**known knowns** – e.g., weapons of mass destruction in the hands of terrorists); those we guess at but do not know (**known unknowns** – e.g., the consequences of biogenetics, climate change, etc.); and those that we cannot even guess at (**unknown unknowns** – e.g., new threats arising from technological development).

3. Opportunities

37 The characteristics of the future operating environment pose significant challenges to security, but they also offer opportunities that the Armed Forces could exploit.

38 Technical innovation in the coming years in fields like biology, bio and nanotechnology, medicine, robotics, artificial intelligence, information and communication systems, autonomous systems, advanced materials, additive manufacturing, quantum computing, etc. will offer unprecedented advantages to the Armed Forces and, obviously, to our adversaries as well. Faced with these technological developments, the aim will be to adopt a pre-emptive strategy, not a reactive one, through close cooperation with academia, business, the public sector, the private sector and the military to try to prevent our potential adversaries from accessing the new technologies, or at least slowing them down. More structured planning, with a focus on comprehensive life-cycle management, and the leadership role of the civil sector in technology will make procurement processes more efficient. This technological advantage must not only affect systems and capabilities; it must also go hand-in-hand with changes in the culture, regulations, organization, training, procedures and doctrine, if we are to have superiority in the conflict.

39 Globalization and the interdependence of the different actors, as well as the need to give comprehensive answers to these future multilateral and multidimensional challenges, must lead us to leverage the new opportunities in order to **grow and improve our collaborative efforts**. Measures therefore need to be adopted and developed that will permit the appropriate interoperability and cooperation, in response to an increasingly all-inclusive view of security.

40 Outside the country, to contribute to anticipating and avoiding possible crises, solving conflicts and bringing stability to our own environment, Spain must take advantage of the opportunities available to it to **be integrated into the ISDOs** of which

it is a member and to promote agreements on security with all the **bilateral, minilateral[5] and multilateral initiatives** that share our objectives.

The number and variety of the threats, in addition to the cost of purchasing future weapons systems, could make it necessary to intensify cooperation on capability planning to promote current initiatives like "Smart Defence" and "Pooling & Sharing", and others of a similar nature that could be established.

[5] Rodrigo Calvo, R. M. *Multilateralismo y minilateralismo en el orden regional: un análisis de las conversaciones a seis bandas* (Multilateralism and minilateralism in the regional order: an analysis of the six-party talks). Estudios de Asia Oriental. Universitat Oberta de Catalunya. Prácticum 87.047. pp. 40-41. The emergence of new powers and non-state actors, the need for greater multilateral cooperation and the failure of traditional multilateralism, like that of the United Nations, to adapt to the new international realities has made nations with common interests create a series of smaller "minilateral" groups that have a common theme and are rarely institutionalized, with the aim of cooperating selectively on world affairs and avoiding the bureaucratic isolation and institutional rigidity of the big multilateral organizations.

41 Internally, the increasingly fine dividing line between security and defence, or between internal and external security, must lead the authorities to favour relations of **coordination and cooperation with other instruments of state power** in the broadest sense, as part of the respect for the powers legally assigned to each of the actors called upon to intervene. In this sense, it is considered essential to progress towards empowering a global crisis management capability, given the wide number and differing nature of the crises or conflicts that will arise in the future and which will undoubtedly affect the security of this country and its citizens.

42 The enormity of the challenges in the 2035 operating environment, the availability of the Armed Forces' capabilities and organizational and operational characteristics, and reasons of efficiency could favour an intensification of the current cooperation between the Armed Forces and civilian authorities on tasks that were traditionally considered to be civil defence (public safety and well-being, the resilience of the state, catastrophes, both natural and manmade, calamities and other public necessities).

43 **Technological advances in the ability to understand the situation** (space-based surveillance systems (SBSS), Joint Intelligence, Surveillance and Reconnaissance (JISR) systems, situation awareness, the development of knowledge (big data, artificial intelligence, etc.) and knowledge sharing (access to the same information and communication technologies (ICTs), etc.) can create opportunities for the Armed Forces to respond more adequately to crises, as they provide an effective instrument for intervening proactively and preventing conflicts, or acting reactively and effectively to resolve them.

44 The professionalism, efficiency and effectiveness of the **Armed Forces as an instrument of the state** in resolving conflicts; the legitimacy of the causes that are assigned to them by represented popular will; their exemplary actions in these causes, in accordance with national and international legal order; the transparency of their management and organization; and the ethical principles and values that govern their operation are an example to Spanish society that, due to their recognition and social support and their compliance with their constitutional mandate, should be recognized as a factor in national cohesion and a guarantee of the sovereignty and independence of Spain and should be transmitted to society through the appropriate strategic communication of an awareness of defence.

4. Characteristics of Operating Environment 2035

45 When studying armed conflicts, some factors never change and others change over time. The permanent nature of armed conflicts has always been characterized by a contest of wills in which three **key factors** interact: (1) violence, hate and enmity; (2) a game of chance, friction[6] and uncertainty regarding the actions of the opponents, and (3) their purpose, as a political instrument. But armed conflicts also contain a variable social and cultural characteristic that changes and evolves over time. This variable component develops and is expressed through the operating environment, which differs from moment to moment.

[6] Friction is a term in military science for when plans do not go as they were designed and originally conceived, contributing to the unpredictability of the acts of war

46 The operating environment can be defined therefore as the **framework in which all the variables interact** that have an immediate influence on actions that the different actors implement through military operations to reach or satisfy their policy objectives. Therefore, the operating environment would be made up of the actors (state and non-state) and their ways of relating to each other (in isolation, in alliances, coalitions, etc.); the strategies (conventional, asymmetrical or hybrid); the domains (land, sea, aerospace[7], cyberspace and cognitive); the resources and capabilities; the challenges and opportunities; the operations or missions that implement the strategies, and a long list of variables that determine the way in which the Armed Forces needs to operate.

47 In 2035 the operating environment will be characterized by the **continuation of crises and conflict**, to be understood as recourse to confrontation, whether peaceful or violent, to resolve disputes between various actors who are fighting for a variety of interests, and not just armed conflict.

[7] In the domain of aerospace, it is possible to distinguish between two clearly defined spaces: airspace and outer space

48 To prevent crises from becoming contagious and to preserve national stability, it will be appropriate to **prioritize the use of pre-emptive and preventive strategies** over reactive or response strategies. Considering the difficulties involved in evaluating the prediction, extension, duration and intensity of crises and conflicts, given the speed with which they evolve, it will be imperative to gain information superiority, which will make it possible, in turn, to have decision-making superiority. Should we not be able to anticipate crises, it will be necessary to articulate the way to act swiftly to mediate, evaluate and create the response.

49 We moved from a bipolar world during the Cold War to a unipolar world in the 90s and we are witnessing the configuration of a multipolar world marked by a **rising number and diversity of the actors**, state and non-state, with the ability to influence regional and international affairs as a result of technological development and interconnectivity. The varied list of non-state actors will include humanitarian groups, non-governmental organizations (NGO), big multinational corporations and even individuals, as well as terrorist organizations and organized crime. These last criminal organizations should be particularly noted because of their impact on security and international stability when operating autonomously or with a certain dependence on state actors in what have come to be called "proxy wars".

50 This variety of actors and relationships will complicate the efforts to develop strategies and specific military capabilities. It will therefore be difficult to identify the source of the aggression and to make the classic distinction between combatants and non-combatants.

51 Given the complexity, diversity and magnitude of the challenges confronting the Armed Forces in the future operating environment, it will be imperative to **strengthen cooperation** on security and defence both externally (e.g., the European Union's (EU) Structured Permanent Cooperation (PESCO)) and internally, as established in section 2 of this chapter when dealing with the opportunities that the Armed Forces will need to exploit.

52 Externally, in addition to Spain's commitment to the UN, NATO and EU, ad hoc **multilateral, minilateral and bilateral agreements** will be sponsored and encouraged with specific countries, and even with non-state actors who contribute to the goal of cooperative security. This trend toward external cooperation on security and defence cannot prevent this country from continuing to maintain its own credible, effective defence capability, since we might have to face situations in which we could not count on foreign support.

53 Internally, there will be a need for **greater cooperation with the various ministerial departments**, other government departments and the private actors involved in security and national defence (industry, universities, research centres, etc.), starting with respect for the established framework of powers.

54 The **strategies or lines of action of the potential adversaries** will be as many and as varied as the opponents trying to harm national interests. However, they can be summarized as a continuation of conventional strategies and an increase in non-conventional and hybrid strategies. The result of all this will be an increasing overlapping of criminal activity (terrorism, organized crime, etc.) and armed conflict.

This will possibly lead to more activity on the part of the Armed Forces in their legal powers as law enforcement agents (the neutralization and committal for trial of pirate groups) and more policing capabilities in the Armed Forces joint actions. The actions of gendarmerie-like police forces, as has been happening in different theatres of operations in recent decades, are particularly appropriate. Due to its military nature, the Civil Guard (CG) is a particularly suitable institution for deploying robust units with policing capabilities to conflict zones with a destabilized environment or to support the Armed Forces crisis management and peacekeeping military operations, either autonomously or when integrated into multinational organizations.

55 The possibility of armed conflicts between states using **conventional theories, strategies, tactics and resources** is low but does exist, and their consequences will always be serious. This possibility will make it necessary to maintain some credible conventional capabilities, with the aim, firstly, of discouraging any attempt to threaten this country and, secondly, of guaranteeing a military response should the remaining stability mechanisms fail.

56 Conversely, **armed conflicts resulting from internal crises and the weakening of some states** will continue into the future. In fact, practically all the conflicts in which the Armed Forces has been involved in the last decade correspond to this model. The response to the situations that they present is at times non-military or at least does not correspond to the traditional actions of military forces, even though it is these forces that have normally been used. Therefore, it is possible to envision that in the year 2035 there will be a continuation of major conflicts, presumably long-

lasting ones, that will involve large coalitions, far from their national territory, mainly in fragile or failed states, plus other minor conflicts that will be limited to shorter periods of time, in very specific areas, involving fewer people, in smaller coalitions with fewer resources.

57 The redistribution of global and regional strategic power with ambitions to revise the current status quo and the emergence of non-state actors with global or regional agendas will lead to a great disproportion or asymmetry between the political and military forces of the opposite sides, which will oblige the parties that are at a disadvantage to use **strategies, procedures and techniques that are non-conventional**, or foreign to international norms and common military tradition, in order to alter the confrontational scenario. Here, the use of technology will be maximized, the tactics will be more flexible, the importance of the human element will increase and the support of the population will be sought. All this will be done to gain an advantage over more powerful opponents, or who at least have more resources. Among these strategies, terrorism, guerrilla warfare, resistance, insurgency, etc. should be highlighted, as they will be used to minimize our superiority in the confrontation.

58 Future conflict will increasingly use **hybrid strategies**, in the sense that our potential adversaries will employ a wide range of techniques, conventional or unconventional, of greater or lesser intensity, to exploit our weaknesses.

59 In an environment in which public international law at times shows signs of inadaptability, the dichotomy between peace and war, which previously had an identifiable transition point, with a declaration of war or the signing of a peace treaty, is already very hazy and will become a blurred continuum that is not easy to catalogue. The traditional border between peace and war will fade, making it difficult to modulate the responses and identify the end of the conflict using the classical ideas of victory or defeat, so that the lack of a clear resolution and the political and social effects will linger for a long time.

60 Should the possible aggressors consider the implementation of hybrid strategies too daring, imprudent or risky, fearing they would give them away or trigger possible responses from the powers attacked, they could resort to exploiting the "**grey area**", in which the aggressors, even with a limited economic and military capability, would have some possibility of success over their economic and military superiors. This is a prior stage to open conflict or the violent use of military forces by a state actor that also uses other instruments of state power in "ambiguous warfare" to gain specific strategic objectives.

61 The **ambiguity of future conflict** (characterized by the overlapping or indeterminacy of the nature of the combatants, the strategies employed, the "weapon systems", etc.), a better knowledge of the situation at all levels of command (by increasing the volume of information and the speed with which it is updated) and technological developments in the area of command and control (which will make it possible to directly transmit orders from the higher ranks to the lower) will impose changes on military organizations that will make operations go at a faster pace right from the planning to the execution stage and allow them to operate with the necessary flexibility in an ambiguous, diffuse environment.

62 The other "**operating domains**" of cyberspace, cognitive domain and outer space will be added with increasing intensity to the traditional physical domains of land, sea and air. There will be an increasing tendency for all these domains to become fused and it will be increasingly difficult to know the source of the effects observed in one specific domain, as the borders between them will become blurred (multi-domain or cross-domain battle). Military operations in all these domains will be implemented under the principle of unity of action and almost always simultaneously and continuously, so as to provide multi-dimensional and comprehensive responses. In all these domains, the technological component is going to play an essential role in achieving freedom of action.

63 The social advances and conquests of recent decades and a general aversion to violence have made traditional confrontation based on mutual physical destruction lose its validity. This will mean that the **cognitive domain**, which is very close to the intellectual and spiritual essence of human beings (as it feeds their values, attitudes, conscience, education, prejudices, perceptions, etc.) and the **cyber domain** will become the major "new battlefields" for solving international disputes, which were previously resolved by an exchange of fire. The importance of ideas and legitimizations will increase the battle for the narratives and intensify the strategies used to influence and gain superiority in the cognitive domain. Possibly, what will happen in 2035 will be that the excess of completely biased information will make it impossible to know the

truth or the reality, so that societies will live in a world of mistrust in which nobody will know what is true and what is not.

64 To prevent the possible intervention of the Armed Forces in future conflicts from generating **negative perceptions in society**, by not identifying a direct relationship between the risks and threats that these conflicts entail and the protection of our territorial integrity or our interests, it is advisable to explain to the public, by means of a coordinated strategic communication effort, that our participation will bring benefits and will not lead to major problems or, to put it another way, to present the public with the risks and costs of not becoming involved. To legitimize our positions, we must be actively and proactively engaged with the media and have sufficient flexibility to act reactively when events require this. We must be the first to inform, or accuracy could be lost.

65 It is not possible to predict the regions in which the Armed Forces could be involved in 2035 as no prediction that could be made based on current conflicts can prioritize some areas over others. However, it is foreseen that the major areas of interest in which the Armed Forces could participate in the coming years will be Spain's national territory (a continuation of their on-going surveillance and security missions and involvement in catastrophes or natural disasters); geographical areas of national interest (the Mediterranean and its southern and eastern coasts; Africa, especially the Sahel, Gulf of Guinea and Horn of Africa, on cooperative security

missions to contribute to regional stability; and Latin America, with multinational military cooperation activities and to support the civil authorities in the event of catastrophes, natural disasters, with humanitarian aid, etc.) and the areas that are determined by our membership in the UN, NATO and the EU, or the coalitions or initiatives in which Spain could become involved. However, globalization will determine whether the defence of our national security interests could oblige us to intervene anywhere in the world.

66 It is also not possible to predict with any accuracy **in which areas of confrontation operations will take place**, although, as has occurred previously, the warring parties will exploit the advantages that are available to them. For this reason, the weaker side will always seek the more difficult geographical areas (densely populated urban areas, coasts, mountainous areas, border areas, underground, etc.); places in which they can obtain the greatest gain at the least cost (economic and financial centres, vital communication centres, government installations, etc.); critical infrastructure and services essential to the nation (power grids, telecommunications networks, tourism, etc.); and the global commons, such as cyberspace, maritime space, airspace and outer space. The confrontational environment will therefore depend on the nature and magnitude of the threat, and the political objectives sought, which will cause the adversary to exploit the advantages offered by the environment.

67 The characteristics of the future operating environment pose great challenges to the forces themselves. They must be prepared to counter threats in a great variety of places in which a technological advantage will not totally guarantee superiority in the confrontation, due to the difficulty of observation, identification and attack.

68 The evolution of certain social and demographic trends will determine which possible adversaries might use **densely populated urban areas** as their preferred place for a confrontation. However, wars will only be won by dominating the great "empty" spaces that surround these environments. The number and variety of possible actors in the fray; the use of critical infrastructure and non-combatants as human shields; the limitations on technology in terms of location and identification; the difficulty of differentiating between combatants and non-combatants; the density and congestion of manned and unmanned vehicles; the limitations on the methods and weapons used due to the risk of collateral damage, etc. will be determining factors in deciding the difficulty of the operations and restricting the freedom of action of the forces involved.

69 Operations in dense populated areas, over reduced distances, will require **reducing the decision making process.** In addition, planning and executing activities in these areas will require focusing on the ability to work together and a high degree of interoperability with our future partners and allies.

70 Technological and economic progress will also permit more countries to develop, in part or as a whole, **Anti-Access/Area Denial (A2/AD) systems**, which will be important for the strategy to be used in future conflicts; in the past such A2/AD systems were restricted to great powers with significant investment in armament programmes. This will create significant operating problems and, by extension, strategic problems for the Western forces, which have been accustomed for many years to operating out of operating bases and with almost invulnerable support infrastructure and communication lines. In this sense, it is worthwhile to emphasize that, in spite of the technical difficulties involved in developing these systems, technology transfer between the powers could also alter this situation.

71 Commercial and military activities strongly depend on access to the **global commons**, so that developing A2/AD capabilities will seriously restrict the Western countries and their freedom of movement by limiting the strategic autonomy that the West has enjoyed up till now. Protecting freedom of movement within global commons will continue to be one of the major objectives of the Armed Forces, so as to guarantee essential services to the public.

72 Within these global commons, it is worthwhile to highlight the role to be played by outer space and cyberspace as the main places for confrontation in 2035.

73 In **outer space**, which is part of aerospace, there will be systems that are essential for the economic and social development of countries, making them a valuable objective for states and terrorist and criminal organizations, as a result of the increasing accessibility and reduced cost of space technology. The possibility, therefore, of deploying weapon systems and the need to protect orbiting assets will lead to a growing militarization of space, despite the ambiguous restrictions of current treaties and international principles. The use of space by an increasing number of actors and competition between the great powers for hegemony in space could lead to conflicts over the rights to territory in space, the exploitation of Earth resources or the use and occupation of areas of Earth orbit.

74 In regard to the Armed Forces, since space systems provide information on the weather and navigation around the globe, intelligence, surveillance and reconnaissance (ISR) and communications, Spain must make the right decisions in regard to its space capabilities, if it wishes to remain interoperable with our major partners and allies, who are firmly committed to strengthening their leadership in space-related technologies.

75 **Cyberspace**, which is already a reality, will increase exponentially between now and 2035. It is expected that our adversaries will continue to look for ways to exploit vulnerabilities in this area, since any action in this domain is very profitable and inconspicuously adjusts to the interests and motivations of a variety of actors, such as states, terrorists and even individuals. While the cost of attacking in cyberspace is relatively low, defending this area is a complex task due to the great number of entry points, and this situation is not expected to change. Limited resources will dictate that defensive efforts need to be concentrated on the most probable targets, so that intelligence will be decisive for predicting what they will be. Cooperation with our allies will be essential to provide early warning and mitigate the effects of possible attacks.

76 As already mentioned, **technology** is one of the most significant **drivers of change for the future operating environment** but by itself it does not guarantee success. There are many examples that confirm this idea (Vietnam, Afghanistan, Iraq, etc.). Also, an excessive dependency on technology has undesired effects, especially in degraded contexts and environments (electromagnetically, with no navigation information, no communications, no Internet, etc.), so that it will be necessary to counter this vulnerability with technologies that are suitable for use in degraded environments and are capable of eliminating the dependency of weapons systems on enabling technologies (global positioning system (GPS), spectrum bands, etc.) so as to counter these effects. In addition, it will be necessary to have appropriate training based on "old" procedures.

77 It will be necessary to monitor emerging technological areas, such as space, cyberspace, robotics and autonomous systems, artificial intelligence, big data, biology, medicine, nanotechnology, new materials, directed energy, efficient energy storage systems, 3D/4D printing, the Internet of things, quantum computing, etc. Innovation

and advances in all these areas will permit significant improvements in physical and intellectual skills, through advances in brain augmentation and human military performance, automating and speeding up processes, increasing the efficiency and effectiveness of armies, better qualified military contingents, the ability to anticipate challenges and threats, and an increase in the precision and effectiveness of weapon systems.

78 However, accelerated technological innovation also has a negative side: increasing access to knowledge will favour the appearance of new threats that will be difficult to combat and the on-going reduction in cost and easy access to some of these technologies will provide greater protagonist to individuals and groups that have the ability to produce uncontrolled effects that are difficult to predict.

79 Although many of the characteristics that will dominate the 2035 operating environment are foreseeable, **strategic surprise** will always be possible. As its name suggests, it will be difficult to predict or evaluate; it should be understood as the sudden or unexpected questioning of the pre-existing strategic balances in terms of adversaries, alliances, operating environments, resources, strategies, areas of confrontation, etc. Social, political, environmental, military or technological advances or events could therefore profoundly alter the strategic landscape, to the point of making the models for the existing or predicted the Armed Forces inappropriate.

80 Volatility, uncertainty, complexity and ambiguity are a summary of the features characterising a highly unstable future. The best strategic response, therefore, would consist of **Armed Forces that are agile, cooperative and open to change, with versatile work teams adapted to the environment**, in what in business is known as a "light footprint strategy", meaning one in which an organization exploits the opportunities with an open, innovative attitude, without allowing the opportunities to become threats.

Summary of Chapter 1

AIM: "**To determine the characteristics that will make up the operating environment in 2035"**

SUMMARY:

1. Risks of the 2035 operating environment: Characterized by VUCA environments. They are divided into *challenges, vulnerabilities, ethical and legal aspects and threats.*

2. Opportunities: The Armed Forces must be able to exploit the opportunities that will be offered by the future operating environment. These include technological innovation, external and internal cooperation to confront what will be complex, multi-dimensional challenges, an improved capacity to understand the situation and more professional and modern Armed Forces as an instrument of the state for resolving conflicts.

3. Characteristics of Operating Environment 2035.

- The use of proactive, preventive and dissuasive strategies will take priority over reaction or response.
- The number of actors capable of influencing international affairs as a result of technological development and interconnectivity will increase and diversify.
- The overall multi-dimensional nature of security will require the Armed Forces to increase their cooperation with foreign state and non-state actors and with the other instruments of state power and even national power inside the country.
- Conventional strategies will continue, with an increase in non-conventional and hybrid strategies.
- In addition to the traditional physical environments (land, sea and air), other operating domains – cyberspace, cognitive domain and outer space – will increasingly be used.
- The geographical areas of interest to the Armed Forces include Spain's national territory, areas of national interest and those determined by Spain's membership in NATO, the UN and EU and wherever the defence of our national security interests is required.
- The areas of confrontation in which operations will take place will be:
  - More difficult areas where the adversary has an operating advantage (densely populated urban areas, coasts, mountains areas, underground, border areas, etc.).
  - Places where the greatest gain can be obtained for the least cost (economic and financial centres, communication centres, government installations, etc.)
  - Critical infrastructure and services essential to the nation (power grids, telecommunications networks, tourism, etc.)
  - Global commons, including outer space and cyberspace.
- Technology will be one of the most significant drivers of the change in the 2035 operating environment, although by itself it does not guarantee success.
- A strategic surprise in any area (adversaries, alliances, technology, doctrine, etc.) would hinder any of the features described above and, as a result, any model for the Armed Forces that might be proposed would become inadequate.

CHAPTER 2
OPERATIONAL SCENARIOS OF ACTION BY THE ARMED FORCES

"The militia's mission is to defend freedom,
one of the most precious gifts that the skies gave to men."

Miguel de Cervantes

5. National security interests versus operational scenarios of action by the Armed Forces

81 "**What to protect and in which conflicts to intervene**" is a key factor in designing the type of the Armed Forces that will be needed in 2035 to counter the challenges of the future effectively. However, answering these questions or setting the right priorities

falls into the political sphere, therefore it is not the objective of this document and is therefore not the aim of this document.

82 Instead, this document lists the duties or operations that the AF should carry out to fulfil its mission. The **mission of the Armed Forces**, which is included in Spanish legislation, as it is in most countries, has a permanent nature that, overall, can be summarized as guaranteeing the security and military defence of Spain and the well-being of its citizens. These missions are carried out to preserve, protect and guarantee national security interests or, as other texts put it, our principles and values. Sometimes they will coincide and there will be no problem when the time comes to make decisions. But at other times there will be some contradiction and it will be necessary to choose some and not others. For the purposes of this document, the term "national security interests" will be used to refer to "principles and values" as well.

83 Assuring the safety and defence of Spain and the well-being of the Spanish people has therefore a **permanent nature**. It was the same for the forces in the 17TH century as it is for today's forces and will presumably be the same for those of 2035. However, the operations or duties undertaken to fulfil that mission have varied over time in order to adapt to the changing characteristics of each operating environment (risks and threats, domains, ethical and legal aspects of the conflicts, socio-cultural principles of the people, etc.)

84 National security interests have also been unpredictable and changed throughout history, although they have remained valid for long periods of time. However, it is indispensable to redefine these interests constantly so that they are understood by the public and its support for the government is not hampered or impeded when state resources and, as a last resort, the FAS are being employed to defend and protect these same interests.

85 According to current Spanish legislation, three large sections of national security interests are, and presumably will continue to be in 2035, the subject of a "**security and defence effort**" or, as the recent National Security Act says, what the State is obliged to protect[1]:

1. *Interests regarding* **national sovereignty**. *These are "vital interests" since the* **asset protected is the very existence of the Spanish nation**.
2. *Interests related to having a* **stable international order with peace, security and respect for human rights**. *These would be included in "strategic interests" as they bring security to our area and contribute to the defence of vital interests, and in "other security interests", which are those that refer to achieving a stable international order.*
3. *Interests that affect the* **lives, safety, well-being and prosperity of the Spanish people**. These are also "vital interests" as the asset protected is the people.

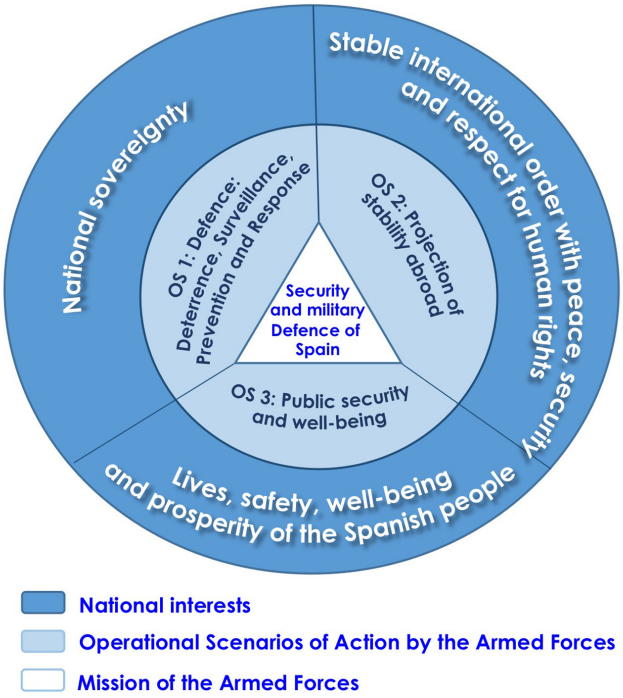
[1] Law 36/2015, of 28 September, on National Security. Art. 3: "For the purposes of this law National Security shall be understood to be State action intended to protect the freedom, rights and well-being of the public, to guarantee the defence of Spain and its constitutional principles and values, and in addition to contribute, together with our partners and allies, to international security by fulfilling the commitments assumed."

86 In 2035 the Armed Forces will continue to be one of the main instruments of the state that provides the political authorities with the capability to protect the above-mentioned national interests.

87 In line with these, the following are the **Operational Scenarios of Action by the Armed Forces** [2] (Figure 9):

- Operational Scenarios (OS) 1. DEFENCE: DISSUASION, SURVEILLANCE, PREVENTION AND RESPONSE.
- Operational Scenarios (OS) 2. PROJECTION OF STABILITY ABROAD.
- Operational Scenarios (OS) 3. PUBLIC SECURITY AND WELL-BEING.

Figure 9. National security interests vs operational scenarios of action by the Armed Forces



[2] Organic Law 5/2005, of 17 November, on National Defence, Title III, Chapter I, Art. 15. Missions: "The Armed Forces, in accordance with article 8.1 of the Constitution, 1, are assigned the mission of guaranteeing the sovereignty and independence of Spain, defending its territorial integrity and constitutional order. 2. The Armed Forces contribute militarily to the security and defence of Spain and its allies, in the framework of the international organizations of which Spain forms part, in addition to peacekeeping, stability and humanitarian aid. 3. The Armed Forces, together with the Institutions of the State and the Public Administrations, must preserve the security and well-being of the citizens in cases of serious risk, catastrophe, calamity or other public needs, as established in current legislation. 4. The Armed Forces may, in addition, carry out missions to evacuate Spanish residents overseas, when circumstances of instability in a country put their lives or their interests at serious risk."

6. OS 1. Defence: Dissuasion, Surveillance, Prevention and Response

88 The Armed Forces will continue to have the mission of guaranteeing the sovereignty and independence of Spain and defending its territorial integrity and constitutional order in the face of all types of aggressions.

89 National Defence is the main mission of the Armed Forces and its **raison d'être**, since it is intended to protect the central core of the national interest that assure the existence of the country as a free and sovereign entity. Such is the importance of this mission that it is included in the Spanish Constitution.

90 This mission would be carried out by means of **response operations**[3] to dissuade, negate and, given the case, neutralize and defeat any aggression that could put national survival at risk, and **permanent operations**[4] to provide dissuasion, surveillance, prevention, security and control of the national territory, sovereign areas and priority areas of interest. The importance of the value protected is such that it requires the Armed Forces to have the military capabilities needed to carry out these missions successfully.

91 The possible challenges that could infringe upon vital Spanish interests could therefore be of an **external or internal nature**[5]. Among the former are armed conflicts and **proxy wars**, and among the latter problems of territorial cohesion[6].

92 Armed conflicts continue to be one of the most significant threats to National Security[7]. Should a conflict arise, depending on its intensity, it would be very demanding for the Armed Forces if all the human and material resources of the nation were compromised; so that it is necessary for them to be prepared for such an eventuality, since not doing so would encourage possible adversaries to use military force against Spain's national interests. Being constantly ready to face up to such a conflict constitutes the necessary basis for the national military capability.

93 Proxy wars would be more probable than conventional armed conflict, as third states, through state or non-state actors, would try to employ non-conventional or hybrid strategies to destabilize, discredit or affect national interests. Some of the actions used could come from the "grey area", so as to make possible responses difficult, although it is not considered that the use of the Armed Forces in any foreign country is foreseeable.

---

[3] Publication of Joint Doctrine (PDC)-01 (A), Chief of the Defence Staff (EMAD). March 2018. P. 52. "Response Operations are those that, to respond to or to prevent a crisis, take place on national territory or within the framework of the Alliance or a multinational coalition already included in a contingency plan (COP) or occur without warning or unexpectedly. They are embodied in the development of an operations plan (OPLAN)."

[4] bid. p. 52. "Permanent operations are those that are continuously active or are activated periodically or repeatedly. They are embodied in the development of permanent plans (PP)."

[5] National Security Strategy (NSS) 2017. The President of the Government. Preamble. "In addition to global challenges, there are other, internal threats to our territorial integrity and constitutional values."

[6] Ibid. p. 26.

[7] Ibid. pp.59-60

94 From the viewpoint of possible internal challenges to Spain's national sovereignty, constitutional order or territorial integrity[8], the construction of narratives that contradict the real situation in Spain is one of the most important that Spain will confront in the coming years.

95 To counter **external aggression**, the Armed Forces could act autonomously or with the International Security and Defence Organizations of which Spain is a member, which are committed to intervening to support a member state when it is attacked. This principle of collective defence and, above all, the design of a credible military force, are the main elements of dissuasion to prevent an attack from outside[9].

96 The **geographical area** to which this operational scenario is limited is the national territory, our sovereign areas and those of primary interest. As a result of the existence of Spanish territories apart from the Iberian Peninsula, consideration shall be

[8] Ibid. "Spain faces a number of threats and challenges, both internal and external, including its demographic prospects, its limited energy interconnections, and its territorial cohesion issues. Challenges to the legal order and to the general interests of Spain require a response based on the rule of law in order to safeguard the rights and freedoms of all its citizens." p. 10

[9] National Security Strategy (2017). p. 60.

given to A2/AD scenarios, together with a total or partial interruption of land, sea and air communication lines.

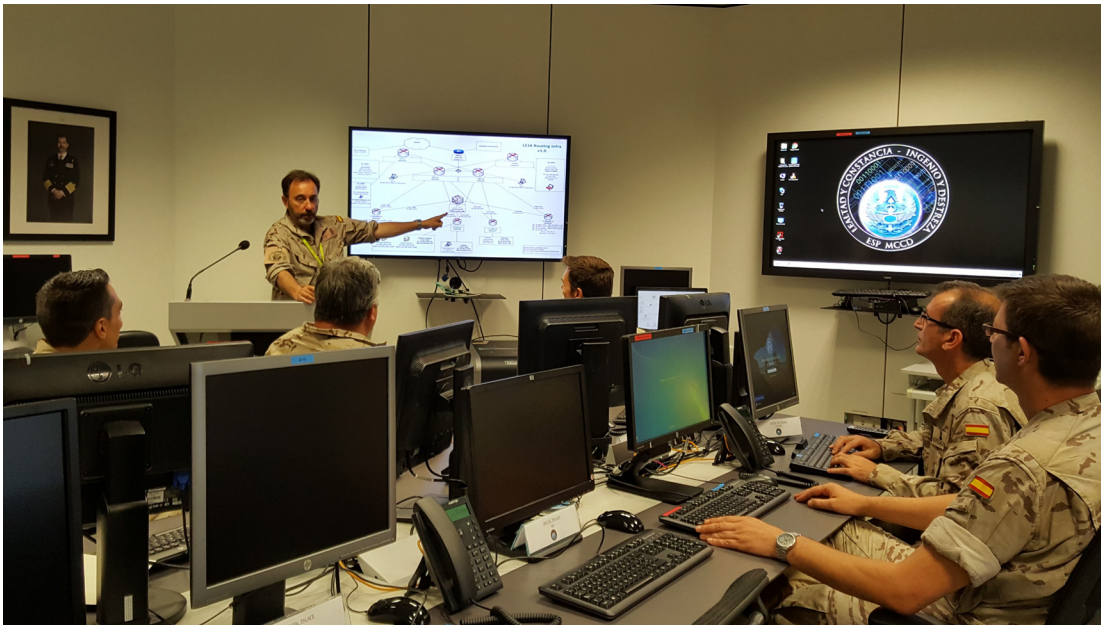
97 In addition to the traditional domains of land, sea and air, it is considered that, due to their probable use in the future, the prevailing domains in OS 1 will be **cyberspace and cognitive**[10].

98 **Cyberspace** cuts across the other domains, since it is present in all of them and acts as a multiplier or booster for other threats. This domain is already a reality today but increasing globalization and interconnection over the Internet foreshadows the huge importance of this domain in the future due to the dangers it may hide, cyber dependency of our societies and its discretion and sophistication.

99 Cyberattacks could be caused by three different actors: States, organized groups (terrorists, criminals and hacktivists) and isolated individuals. The targets of the cyberattacks will be the Armed Forces networks and systems, as well as those of government departments, critical infrastructure and services essential to the nation, with the aim of causing severe economic damage and creating instability and internal chaos.

100 Cyberspace could also be the medium used to broadcast politically motivated narratives using manipulation and disinformation campaigns. The Armed Forces must be capable of finding out about and countering the adversarial information broadcast and of carrying out information operations in cyberspace in order to ensure Spanish interests.

101 The **cognitive domain** also cuts across the other areas of operation, since information operations will take place at the same time as military operations in other areas, following the principle of unity of action.



[10] Ibid. p.60

102 The cognitive domain, in which the centre of gravity will not be the Armed Forces but the minds of individuals, will be the predominant one in 2035:

- *Firstly, because the political level requires credibility to justify the employment of the military instrument. The government will need to elicit the support of society through a greater communication effort, based on advance information "cleansing".*

  In the event of external aggression, the use of force in legitimate defence is a concept that exists in all legal systems and is also included in International Public Law and international custom[11].

  The Armed Forces, under the direction of the political hierarchy, must promote strategic communication at all levels.

- *Secondly, because our potential adversaries know the* **strategic value** *of identifying public perceptions and moulding them to their political objectives, and without investing large sums of money in sophisticated weapons systems and without being subject to rejection by the international community, because they are using less violent but more efficient methods.*

  To win the battle for the narratives, the Armed Forces, in close cooperation with other state powers, must be able to carry out information operations using several media, acting both autonomously and as part of multinational forces, in order to refute the adversary's narratives with their own.

103 Within OS 1, the Armed Forces will also carry out permanent operations of a dissuasive and preventive nature to ensure public safety. These will consist of the routine performance (24/7) of many surveillance, security and control activities throughout the national territory, and in military cyberspace, sovereign sea, air space and priority areas of interest[12]. The main purpose of the surveillance, security and monitoring activities is to prevent conflicts and, where necessary, act as an initial reaction to them, which is why they are included in OS 1.

104 Given the growing importance of cyberspace, cognitive domain and outer space[13], the Armed Forces will also monitor space and cyberspace and will contribute according to their capabilities to the security of the cognitive.

105 Attacks like 9-11 in the United States in 2001 or the 11-M attack in Spain, as well as the possibility of others of similar lethality, demonstrate the need to **prepare legislation, procedures and systems** so that the Armed Forces can respond to such attacks (e.g., RENEGADE)[14].

---

[11] Article 51 of the United Nations Charter states "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations..."

[12] Organic Law 5/2005 of 17 November on National Defence. Art. 16. A): The surveillance of maritime areas, as a contribution to state action on the sea, the surveillance of airspace and the control of national sovereign airspace….

[13] Outer space is deemed a part of the aerospace domain in the Spanish military doctrine

[14] An air defence operation, specially designed after 9-11 to combat terrorist attacks from the air.

106 The activity performed by the Armed Forces in OS 2 has to do with protecting universal security interests or the global commons. This means that, if there are values that are common to the majority of countries in the international community, it will be necessary to defend them against those who do not share them. For the same reason as the "**security and defence effort**" that nations are prepared to make for their own protection, these universal values end by becoming national security interests in a global environment.

107 Once nations have guaranteed their national security interests and those of the nation state, such as sovereignty and territoriality, it is other reasons, related to achieving a national order of peace, security and respect for human rights that move the respective governments to protect them. It is this "**responsibility to protect**", in clear opposition to the principle of the nation sovereignty emanated from The Peace of Westphalia, that moves the international community to intervene even in the internal affairs of nations when their governments do not protect their populations from "genocide, war crimes, ethnic cleansing and crimes against humanity".

108 To defend these universal values, nations can act autonomously or collectively.

109 Globalization, the emergence of new challenges and threats, a proactive attitude to face them and the inability to act autonomously and uncertain strategic security environment lead nations to strengthen **international cooperation**.

110 Spain belongs to four international organizations with powers over security matters: the UN, OSCE, EU and NATO. Membership in these organizations, and above all the design of a dissuasive military force, contributes to the protection of our strategic interests and their other security interests. Membership in NATO, for example, contributes to the defence of Spain's vital interests as a benefit of the principle of collective defence against external attacks on our sovereignty, and permits us to contribute to the effective prevention of conflict and to be actively involved in crisis management wherever there are risks or threats to international peace and security.

111 Spain's membership in these organizations gives us a privileged position since it permits us to influence security matters when these occur in our immediate environment. However, in turn, a committed effort in terms of human resources and materiel is required to bring about, as shown by the proliferation in recent years of overseas missions to defend the "collective interests" of these organizations. This trend of increased effort will grow in the future due to the emergence of new global challenges.

112 Membership in these organizations is not exempt from differences and friction with other member states. Firstly, owing to Nations' differing perceptions on how to employ military forces; secondly, because their geographical location and economic, demographic, cultural and other constraints make nations perceive the risks and threats very differently (e.g. northern European countries comprehend the situation in the Sahel differently than the south of Europe) and thirdly, because different countries have different views about which international organization is the most appropriate to confront the different challenges. It is therefore essential to **balance two principles:** satisfying national security interests of each member state and solidarity, to cope with the risks and threats perceived more by other partners or allies.

113 There will be **other security efforts** that must be addressed **autonomously and as a priority** when belonging to these security organizations does not guarantee that there will be a response. These efforts will mainly come from the historical Spanish context (Latin America) or because of our geographical situation (North Africa, Gulf of Guinea or Sahel), and they form part of defence diplomacy actions, under which cooperative security activities are included.

114 The Armed Forces will perform Cooperative Security activities bilaterally with countries that are a priority for Spain's foreign relations and will aim to strengthen the military capabilities of the countries supported so that they can be self-sufficient in the future[15]. These activities supplement the preventive measures implemented beyond Spain's borders to reduce the risk that threats from Africa will have a negative impact on the development and prosperity of this country.

---

15 Currently, at the operational level, related activities are taking place in the following countries: Tunisia, Cabo Verde, Senegal and Mauritania, in addition to weekly deployments of Spanish ships in the Gulf of Guinea. It is estimated that they will continue in the future due to the growing importance of the security and stability of these regions of Africa in preserving national interests.

115 The major challenges that the Armed Forces will have to confront in OS 2 will be related to so-called **fragile or failed states**. Recent experience shows that where there are power vacuums, due to poverty, social fragmentation or a lack or absence of democracy, risks are created that can easily become threats in the future.

116 **Radical groups** that use terrorism as a form of action and elements of transnational organized crime (piracy, people, weapons and drug trafficking, etc.) use these states to establish and have "safe havens" from which to operate. The tools provided by globalization (information, communications, finance, technology, etc.), plus the impunity guaranteed to them by the effective absence of any authority in those countries, are fertile ground for the planning, training and support of their terrorist or criminal activities.

117 These areas are also the main source of **mass migration**, encouraged by a widespread knowledge of the opportunities available in more developed societies and the existence of networks of people traffickers.

118 Due to its geographical location, Spain is particularly interested in the Maghreb, and the Mediterranean region in general, becoming stable areas. In addition, the unstable environments created in Sub-Saharan Africa -essentially because of migration and the establishment of organized crime routes- travel along the Western edge of Africa and enter the European continent through Spain. For this reason, we must undertake intensive, preventive efforts with our neighbours in the areas of diplomacy, economics, policing and the military to assist with the three factors considered essential for the stabilization and security of an area: **development aid, improved security and defence structures, and democratization and combating poverty**.

119 The Armed Forces activity in OS 2 is implemented by means of **peacekeeping operations and humanitarian aid and other stabilization and development aid operations** that may be required in certain areas to bring stabilization. They will be actions in low or medium intensity environments, related to peacekeeping and designed to bring about the end of hostilities in these countries, post-conflict reconstruction, a return to normality and governability. In regards to humanitarian aid, the intervention of the Armed Forces overseas where there have been catastrophes should also be mentioned (hurricane Mitch, the tsunami in Indonesia and earthquakes in a number of Latin American countries).

120 Although the operations listed so far for OS 2 are crisis response operations (CRO), OS 2 also includes **collective defence** operations, in which the Armed Forces has to intervene as a result of the aggression suffered by an ally, under the agreements and treaties signed by Spain and the organizations of which it is a member, coalitions that Spain could join to defend damage national security interests or because of requests for help from friendly countries.

121 As stated in Chapter 1, the need for global responses to future challenges, which would be multilateral and multi-dimensional, could lead us to exploit new opportunities for cooperation and collaboration, both at home with other instruments of state power and internationally with state and non-state actors. Because of its importance in this operational scenario, **cooperation between states** in security organizations has already been mentioned. It would also be appropriate to emphasize that transnational corporations, NGOs and even isolated individuals could have an influence on the international system.

122 Spain's geographical location, close to an area of great instability, and spread of security aspects as a result of globalization cause certain events that occur anywhere in the world, however remote, to have a direct influence on the security and well-being of the Spanish people. Therefore, the **defence of our national security interests** will also go **beyond our borders**.

123 Operations in OS 2 have constituted the major activity of the Armed Forces overseas during the last 25 years and it is **predictable that this trend will increase up to 2035**, together with operations in OS 3 to fight terrorism and provide cyber defence.

124 The positive perception held by Spanish society of its Armed Forces is in part recognition of their efforts abroad to contribute to a stable international order with peace, security and respect for human rights. For this reason, it is considered necessary for the population to continue to view these interests as being necessary, important and legitimate. And it is the responsibility of the institutions and their leaders to know how to explain and defend this stance to the public, by promoting specific measures that provide an appropriate awareness of defence.

8. OS 3. Public Security and Well-Being

125 Apart from permanent surveillance operations or the Spain-Morocco incident motivated by the Perejil Island, almost all the Armed Forces activity in recent years has

taken place under "OS 2: "Projection of stability abroad" and "OS 3: Public security and well-being".

126 The **contribution of the Armed Forces to internal security and well-being** is of particular importance. Together with other state and institutions and government departments, the Armed Forces must preserve public security and well-being when there is a serious risk, catastrophe, calamity or other public necessities.

127 To confront these challenges, the **National Security System** was created. It is the set of bodies, resources and procedures, integrated into one single structure, which permits national security relevant authorities to evaluate the factors involved in threats, gather and analyse information in order to make decisions regarding crisis situations, identify the needs and coordinate all the government departments.

128 Spain's geographical situation, globalization, climate change and a possible lack of territorial cohesion will determine many of the **challenges** that the country will surely face in the 2035 environment. These challenges will affect its internal security, the free exercise of citizens' rights and public freedoms, and its economic progress.

129 Under OS 3, the Armed Forces must be prepared, when required, to cooperate and use its capabilities with other instruments of state power to confront some of the following challenges that Spain could face:

- Demographic imbalance and the unequal distribution of wealth on both sides of the Straits of Gibraltar constitute significant **factors of migratory pressure** toward Spain, which could be aggravated by the lack of natural resources on the southern shore, caused by exceptional episodes of climate change;
- the possible lack of integration of immigrants into Spanish society, which could become a breeding ground for radicalisation;
- **Jihadist terrorism**, as in their imaginations Spain continues to be a part of the Caliphate[16];
- The proliferation of **weapons of mass destruction and their delivery systems**, especially those that could fall into the hands of non-state actors[17];
- **Organized crime[18]**;
- Dependence on **energy resources** and the vulnerability of the supply lines to actions by state and non-state actors, which would limit or interrupt the free flow of goods and people[19];
- **Attacks and cyberattacks** on critical infrastructure and services essential to the country, due to their ever increasing connectivity[20];

---

16 *National Security Strategy (2017)*. pp. 60-61.

17 Ibid, pp. 63-64.

18 Ibid, pp. 62-63.

19 *National Security Strategy (2017)*. pp. 73-74.

20 Ibid, pp. 67-68.

- **Emergencies and catastrophes**, some caused by mankind (fires, pandemics and environmental pollution, basically) and others with natural origins (droughts, pests, floods, earthquakes, for chemic or solar eruptions, etc.) and lastly,
- **The need to evacuate Spanish residents overseas**, when the instability in a country puts their lives or their interests at serious risk (NEO operations).

130. All these are challenges to national security that could hamper the social, economic and political life of the nation and harm the population.

131. Another important activity in which the Armed Forces has been engaged under OS 3 has to do with the **contribution to State Action** of its different departments and in non-combat military actions. It is foreseeable that these will continue in OE 2035. Among these activities are emergencies and catastrophes, oceanography, hydrography, cartography, aerial photography, calibration of radio navigation, fisheries inspection, protection of underwater heritage, environmental protection, collaboration with law enforcement agencies (LEA), customs surveillance, state transport[21], search and rescue, cooperation on defence in cyberspace, etc.

132. None of the operations or activities listed in OS 3 is an Armed Forces function or a responsibility specifically assigned solely to them, but they are carried out by them to **supplement the essential work** done by other instruments of state power. However, the magnificent level of professionalism, specialization and satisfaction with the Armed Forces´ performance on these missions could lead to their being tasked with new responsibilities and duties in the future.

[21] It includes transport for top state officials, law enforcement personnel, prisoners and immigrants, and medevac services in the events of pandemics overseas, when requested, etc.

133. Spanish society must be aware that the activities performed by the Armed Forces in OS 3 are provided 365 days a year for the public in peacetime. Undervaluing the performance of these tasks would be a serious "strategic communication" error, as by carrying out these missions the Armed Forces also legitimize and justify their actions to the rest of the population.

<table>
<tr><th></th><th colspan="2">OS 1:
Defence: Dissuasion, Surveillance, Prevention and Response</th><th colspan="2">OS 2:
Projection of stability abroad</th><th colspan="2">OS 3:
Public security and well-being</th></tr>
<tr><td>NATIONAL SECURITY INTERESTS PROTECTED</td><td colspan="2"><u>Vital</u>:
Sovereignty and independence, territorial integrity and constitutional order</td><td colspan="2"><u>Strategic and other interests:</u>
Stable international order with peace, security and respect for human rights</td><td colspan="2"><u>Vital</u>:
Lives, security, well-being and prosperity of the Spanish people</td></tr>
<tr><td>TYPES OF MISSIONS/</td><td colspan="2">Reaction</td><td rowspan="2">Reaction</td><td>Crisis response (CRO)</td><td colspan="2">Reaction</td></tr>
<tr><td>OPERATIONS</td><td colspan="2">Permanent</td><td>Collective defence
Permanent</td><td colspan="2">Permanent</td></tr>
<tr><td rowspan="3">POSSIBLE CHALLENGES FACED</td><td rowspan="2">Attacks from outside</td><td>Conventional military conflict</td><td colspan="2" rowspan="3">Fragile or failed states and the challenges posed by them:
• Terrorism
• Organized crime
• Mass migrations</td><td rowspan="2">External challenges</td><td>Migratory pressure toward Spain, radicalization and violent demonstrations by immigrants, Jihadi terrorism, the proliferation of WMD, organized crime, the vulnerability of external supply lines, attacks and cyberattacks on critical infrastructure and essential services, environmental catastrophes, NEO operations, etc.</td></tr>
<tr><td>Proxy wars, using:
• State actors
• Non-state actors
• Foreigners
• Nationals
(non-conventional and hybrid strategies)</td></tr>
<tr><td>Domestic challenges</td><td>Territorial cohesion issues</td><td>State action</td><td>Emergencies and catastrophes, oceanography, hydrography, cartography, aerial photography, calibration of radio navigation, fisheries inspection, protection of underwater heritage, environmental protection, collaboration with LEAs, customs surveillance, state transport, search and rescue, cooperation on defence in cyberspace, etc.</td></tr>
<tr><td rowspan="3">METHOD OF ACTION</td><td colspan="2">Autonomous</td><td colspan="2">Autonomous</td><td colspan="2" rowspan="3">Cooperation with other instruments of state power (LEAs, civil defence, etc.)</td></tr>
<tr><td colspan="2" rowspan="2">International cooperation (ISDOs, coalitions, etc.)</td><td rowspan="2">International cooperation</td><td>State actors (ISDOs, coalitions, etc.)</td></tr>
<tr><td>Non-state actors (financial corporations, NGOs, individuals, etc.)</td></tr>
<tr><td>GEOGRAPHICAL AREA</td><td colspan="2">National territory, sovereign airspace A2/AD</td><td colspan="2">Overseas</td><td colspan="2">National territory overseas</td></tr>
<tr><td rowspan="3">OPERATING AREAS</td><td colspan="6">Land, sea and aerospace</td></tr>
<tr><td colspan="6">Cyberspace</td></tr>
<tr><td colspan="6">Cognitive domain</td></tr>
</table>

Summary of Chapter 2

AIM: "**To determine the situations in which the Armed Forces will operate to protect national security interests".**

SUMMARY:

4. NATIONAL SECURITY INTERESTS vs. OPERATIONAL SCENARIOS BY THE ARMED FORCES. In 2035 the Armed Forces will continue to be one of the main instruments of the state to protect national interests:

- Interests of national sovereignty and territorial integrity.
- Interest in a stable international order with peace, security and respect for human rights.
- Interests that affect the lives, security, well-being and prosperity of the Spanish people.

5. Operational Scenario (OS) 1. Defence: Deterrence, Surveillance, Prevention and Response The Armed Forces will continue to have the mission of guaranteeing the sovereignty and independence of Spain and defending its territorial integrity and constitutional order in the face of all types of aggression. This does not preclude the fact that this mission will be performed in any of the traditional domains of land, sea and aerospace. It is considered, however, that, due to their probable use in the future, the prevailing domains for OS 1 will be cyberspace and cognitive..

6. Operational Scenario (OS) 2. Projection of stability abroad. The major challenges that the Armed Forces will have to confront in OS 2 will be related to the so-called fragile or failed states, and with some of their consequences, such as terrorism, illegal immigrations and organized crime. Special mention should also be made of the operations that might take place to contribute to the collective defence of the ISDOs to which Spain belongs. Operations in OS 2 have constituted the major overseas activity of the Armed Forces during the last 25 years and it is predictable that this tendency will increase by 2035.

7. Operational Scenario (OS) 3. Public security and well-being. The all-encompassing, multi-dimensional nature of security will require more and closer cooperation between the various instruments of state power, and even national power. Spain's geographical location, globalization, climate change, problems of territorial cohesion, etc. will decide many of the challenges that this country will surely face in the 2035 environment, such as pressure from illegal immigration, terrorism, the proliferation of WMDs, organized crime, vulnerable supply lines, attacks and cyberattacks on critical infrastructure and services essential to the nation, emergencies and environmental catastrophes and NEO operations. The contribution of the Armed Forces to state action will also be essential in OS 3.

CHAPTER 3
NEED FOR CHANGES IN THE ARMED FOCED TO ADAPT TO OE 2035

"The greatest fortune is made hours in advance.
For the prepared, there are no bad contingencies,
nor for the qualified are there predicaments."

Baltasar Garcián

9. Characteristics of the Armed Forces in 2035

134. Having described the main trends that will shape the global security environment, the key characteristics of the operating environment in 2035 and the contexts or situations in which the Armed Forces will foreseeably operate to protect our national security interests, this study must end with the characteristics that the Armed Forces must have in the future and the implications or consequences of the changes that must be implemented in the different areas of **DOTMLPF-I** (Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, Facilities - Interoperability), so that the Armed Forces can successfully perform the tasks assigned to it in the future environment.

135. It is probable that future operations will be conducted on evermore complex, populated terrain, so that it will be necessary to adjust the capabilities for operations in urban and coastal environments. The fact that military operations will take place in populated areas will mean that, in many cases, the troops involved will seek to control the population rather than destroy or neutralize armies. This will mean that the effectiveness of military operations will increasingly depend on having an adequate information management capability (command and control, JISR, cyber defence and use of cognitive domain), without neglecting the power and performance of the weapons systems. Information operations will become one of the essential tools for operations.

136. In the future, the tenuous line between conventional and non-conventional conflict, regular and irregular warfare, combat zone and rear-guard, and combatant and non-combatant will become blurred. The concepts of "grey area" and "hybrid threat" will end by imposing themselves on and monopolizing the debate about conflicts. This situation will have the following implications: firstly, greater participation by the Armed Forces in affairs that traditionally are not defence but security, and, therefore, greater cooperation between the services and the other instruments

of state power (governmental and non-governmental organizations) and more interweaving of the Armed Forces with society; secondly, the use of military force will be subject to many legal and ethical limitations, so that it will be necessary for the Armed Forces´ standards and procedures to adapt to the legislative changes that will be implemented, so as to guarantee effective action within this restrictive framework.

Figure 11. Characteristics of the Armed Forces in the 2035 operating environment

137. Technological superiority will continue to be one of the most important factors in the 2035 operating environment but due to its proliferation and foreseeably easy access to it by our potential enemies, it will be less decisive and vital than in the wars of the "industrial era". However, it will be necessary to continue to compete with our possible adversaries for the technological advantage in areas such as non-lethal capabilities (information management), aerospace systems, directed energy weapons, operational integration of manned and unmanned vehicles, cyber weapons, etc., even if the adversaries' supposed technological inferiority, plus the appearance of disruptive technologies, could cause conventional capabilities to be less effective than in the past. It will therefore be in our vital interests to adapt to new technologies if in OE 2035 we want to continue to be effective. At risk is, being left behind technologically which increasingly decreases our capability to interoperability with our partners and allies. However, we also need to keep in mind that technology alone, although important, is not decisive if it is not integrated into the evolution of the doctrine and the training.

138. The unstoppable technological evolution affecting current weapon systems, even if it does considerably increase their efficiency, also leads to a significant increase in the cost of their procurement, upkeep and operation. It will therefore be necessary to abide by the principles of feasibility, sustainability and efficiency to properly plan the weapons systems and resources that the Armed Forces will really need to be able to deal with future challenges:

- **Feasibility** will allow the design of the Armed Forces to fit the economic possibilities of the nation.
- **Sustainability** will ensure the maintenance and upkeep of effective, properly equipped and trained Armed Forces.
- **Efficiency** will ensure that the Services perform their duties with the strength and the capabilities that are strictly necessary to attain the desired effects.

139. However, to counter the characteristics of the future, which will be determined by its volatility, uncertainty, complexity and ambiguity (i.e., VUCA environments), which cause confusion and instability and hamper the anticipation of threats and opportunities, in addition to appropriate decision-making, **agility** is considered the main characteristic required of the Armed Forces in 2035. It is therefore no exaggeration to state that the only way that the Armed Forces will be in a position to deal with this challenging future is to be agile, so that what is required is an understanding of the situation and rapid execution.

140. Both of the **organization** and its **personnel** require the same agility. For the organization, it would be necessary to optimize the structures by making them flatter and allowing decentralization of some resources and decision-making, to have "uncommitted" resources in case of the unexpected. In the case of the personnel, it would be necessary to change their mentality so that they can anticipate unexpected situations, which will be achieved by greater investment in their preparation.

141. The main characteristic that must drive the design of the Armed Forces so as to improve its agility will be boosting others that result from agility:

- **Response capability**, to recognize and respond to changes in unexpected circumstances, which, in military terms, is associated with the state of readiness of all units, understood as the level or degree of operational readiness that enable units to operate in the shortest notice to move possible.
- **Versatility**, to achieve an acceptable level of performance or effectiveness when taking on new duties or missions that have been altered by changes in the situation.
- **Flexibility**, to provide more than one alternative way of adapting to the new situation, when the planned response to that situation cannot be implemented, does not work or does provide the appropriate response. The variety of operational scenarios of action and the variety of duties to be performed in each of them will mean that this characteristic is particularly necessary for the Armed Forces.
- **Resilience**, to overcome unfavourable situations and maintain their ability to act in degraded environments.

- **Innovation**, to create or develop new capabilities, doctrines, training, etc., that will make it easy to carry out the duties assigned.
- **Adaptability**, to allow the different services to continuously change, by adapting their organization, processes, structure etc. so as to be better prepared to face the new challenges.

142. The characteristics of the future Armed Forces analysed up till now are generic and applicable to the three operational scenarios. The following study looks more specifically at the characteristics that must take priority in each of the different contexts of OE 2035, with the provision that none of them excludes any of the others.

9.1. Characteristics in OS 1. Defence: Dissuasion, Surveillance, Prevention and Response

143. Defending national security interests affecting sovereignty will require, where necessary, the use of all the nation's human resources and materiel. We must therefore be able to respond to the innumerable challenges that the future could bring in this context. This response must be exercised preventively, by using dissuasion, or reactively, by using coercion, contention or intervention. In all cases, it will be necessary to have **credibility** in the eyes of the adversary and the society that is being defended.

144. Three factors come together in this characteristic, which, according to Clausewitz[1], interact in a conflict. There will be no credibility without deciding on the political level at which military force is to be used, if necessary; when there is no cohesion in or unconditional support from society; or, obviously, when the military does not have the necessary capability. Regardless of the first two factors, we will have a proper military capability when the Armed Forces are properly equipped in both quantity and quality. To do so will require supporting modernization, adequate training, a willingness to act autonomously but in close coordination: firstly, with the other instruments of state power so as to have other coercive options (diplomatic, economic sanctions, etc.) and, secondly, with our partners and allies so as to have a multiplier effect.

[1] Prussian officer and one of the most influential historians and theoreticians of modern military science (1780-1831)

145. Closely linked with agility, resilience will be imperative in OS 1, even if it is not exclusive. The destruction, interruption or breakdown of the Armed Forces capabilities could be a result of action by the adversary, an act of nature, an internal vulnerability or limitation, or the inevitable result of the complexity of the situation. The factors that could contribute to the resilience of the Armed Forces would be: redundant capabilities, the availability of reserves or a national industry that is part of the country's defence structure. Such defence industry must be capable of supplying the Armed Forces and LEAs with the systems required at the time they are needed, in order to react to adverse situations, by minimizing their impact, overcoming them on the shortest possible notice, whilst continuing to achieve their mission. Since feasibility, sustainability and efficiency are the principles that must guide capability planning, the need for agile Armed Forces is emphasized once again, by increasing other characteristics of agility that require fewer resources.

9.2. Characteristics in OS 2: Projection of stability abroad

146. The characteristics of the Armed Forces in OS 2 have to do with its expeditionary nature, in other words, the ability to operate outside national territory, either autonomously or with partners and allies on multinational operations. The characteristic of strategic mobility is the result of the meeting of the other three characteristics:

- **Availability**, which means being ready to be employed at the required time and in the required place. This characteristic is a priority for the employment of the Armed Forces. All units must therefore be in a suitable state of readiness and in a position to operate within the timeframe set, as a result of completing the established training programmes, and properly operating and supporting the different weapons systems on inventory.
- **Deployability or projection capability**, which involves being able to be deployed to any scenario, so that it will be necessary always to have the means of transport available that match the effort required. The increasing rise in instability outside our borders will counsel increasing the rapid deployment capability of contingents of varying sizes.
- **Support** or the ability to provide adequate supplies, maintenance and healthcare to the forces wherever they are operating, during the time the deployment continues. Different planning, coordination and control processes must be undertaken, therefore, to achieve the greatest efficiency with the least use of resources and to implement information systems and procedures that will improve logistical command and control, shorten the supply line and reduce the logistical footprint.

147. Since the Armed Forces will join multinational contingents (ISDOs, coalitions, etc.), interoperability with our allies and partners will be an indispensable requirement, not only for the equipment but also education, training and procedures.

9.3. Characteristics in OS 3: Public Safety and Well-Being

148. The numerous and diverse duties that the Armed Forces will need to carry out in OS 3, some of which are far from traditional defence duties, mean it is advisable to design the future Armed Forces using the criteria of **flexibility**.

Given that limited resources could prevent their having the specific capabilities for each task, it should be necessary to prioritize the procurement of multipurpose or polyvalent capabilities and the development of modular units that will permit their use in any of the operations assigned, with only slight modifications.

149. As stated in chapter 2, threats to national security, which not only involve the instruments of state power but also affect all areas of society as a whole, require extremely complex management. The need to interact with all the instruments of the national security system will require **interoperability** between them and the Armed Forces to facilitate their integration and cooperation. It will also be necessary for the Armed Forces to follow the basic principles of that system (unified action, pre-emption, prevention, efficiency, sustainable use of resources, ability to resist and recover, coordination and cooperation[2]).

10. About Change

10.1. The need to confront change

150. The new types of conflict will transcend our traditional understanding of what until now we have considered regular and irregular military activity. The conflict paradigm is changing and, if we wish to triumph, we must also **change our mind-set, both as individuals and as an organization**. Some indicators show a worrying tendency for the West to be losing its initiative in terms of dictating the way in which the conflicts of the future will be waged and, therefore, we must be prepared for the new reality ahead.

151. The complexity and uncertainty of the future operating environment and the number and variety of missions that the Armed Forces must perform in the operational scenarios of action analysed above and, as a result, the different characteristics that they must have to be useful, mean **difficulties when designing the Armed Forces of the year 2035**.

152. The difficulty of such task is understandably even greater, taking into account the uncertain economic scenario, together with the competition that will take place in the coming years between investment in defence and other items of the national budget.

153. The challenge posed requires making decisions about the design of the Armed Forces that we want to have in the year 2035, in the sense that OS 1 is the *raison d'être* of all armies and legitimizes their existence. The demands of the society that we serve can also not be ignored. All these factors will oblige us to carry out a realistic prioritization exercise and start the in-depth process of change demanded by the future operating environment.

154. Conventional forces respond magnificently to classical military missions, as they are well prepared and equipped for them. However, they have difficulty

[2] Law 36/2015, of 28 September, on National Security, Art. 4.2. 66

adapting when confronted with non-conventional missions, because it is not possible to anticipate the evolution of events and since their actions may have unforeseeable consequences. Such difficulties do not quite derive from the adversary's ability to surprise - something classical and normal in conflicts - but precisely from the future operating environment characteristics described in this document. Faced with this situation, the best approximation that can be made is to continue to improve agility.

155. Because of the uncertainty, **the human factor and effective leadership** will be essential for achieving decisive results. Under the current scenarios, leaders are vital for preventing a fear of change and avoiding organizational paralysis.

10.2. The difficulty of undertaking change

156. All complex organizations have a certain reticence when dealing with the changes that must be made to respond to the challenges that the future, ever uncertain, will bring:

157. There are certain **subjective factors** in leaders of organizations that determine whether their stance regarding changing that organization is positive or negative:

- Leaders with very **open minds** are better prepared to handle contradictory situations. Not only are they more imaginative but they also request alternative viewpoints and are comfortable in discussions with people whose opinions differ from theirs. They are generally more receptive to change. Therefore, open-mindedness will affect the way in which people build their frames of reference and their predisposition to challenging and altering those frames.
- Another factor to be analysed is impact. The careers of leaders reflect the posts that they have had in the past. Their impact leaves a mark that is difficult to change and has considerable influence on the decisions made in subsequent stages. Therefore, when commanders at the strategic level face new situations, they must be aware of the natural tendency to return to the frames of reference that were laid down in the past and have possibly remained fixed.
- In addition, it is necessary to talk about **experience**. Experience is both a gift and a burden. No leader at a strategic level would be successful without trusting in the experience accumulated during his or her career. However, experience can blind us and produce a false sensation that we know what in fact we do not know; it can make us not pay attention to the evidence because we believe it does not have the importance that it really does have. But experience has undoubtedly been and always will be a good counsellor, although in the envisaged operating environment it has to be assessed cautiously, precisely because it is based on past events whose validity in new circumstances could be doubtful.
- Established beliefs and prejudices are also difficult to change. People pay particular attention to information that supports their beliefs and tend to ignore the value of evidence that contradicts them. They also tend to spend the greater part of their lives trying to confirm prior beliefs, instead of seeking information or

contradictory signals that challenge their perceptions. This attitude has been called the **confirmation bias**.

- The **generation gap** is another factor to be taken into account when evaluating a person's attitude to change. The younger generations, educated in the latest technologies "digital natives" generally show themselves to be more open to the changes offered by technology. In contrast, the older generations "digital immigrants" are more reactive and need greater motivation and impetus. The problem can be that the top leadership roles belong to the latter.

158. Not all obstacles to change are found in the individual. There are also organizational factors that can contribute to obstructing action that will change the organization. The organizational culture, corporatism, the traditions and interests of organizations very often lead to innovation being rejected.

10.3. How to implement change? Transformation or adaptation?

159. The Greek philosopher Heraclitus said that the only constant is change. And, as we have seen, it will come **increasingly quickly**. We must anticipate it and drive it, or let it come and have to react in order to manage it.

160. There are two basic ways of **implementing change.** The first comes when there is an overwhelming need to change an organization so that it remains relevant. In this case, speed and pressure can lead to wanting to fix what is not working immediately and make radical changes that at times are not necessarily suited to the new situation. The second way is based on the need for constant renovation, applying gradual, intentional adjustments that are considered necessary in order to fit the context. The first case can be associated with **transformation** and the second with **adaptation**.

161. After the Fall of the Berlin Wall, NATO and most of the armies around us began a process of change, which is still continuing, under the name of "transformation", as if these organizations had to become something different instead of adapting in order to continue being useful in the new operating environment that had arisen after the breakup of the Soviet Union. It should therefore be asked, are we really using the word "transformation" appropriately?

162. There is a palpable **difference between transformation and adaptation,** similar to the one between revolution and evolution. The natural course is evolution; revolutions serve to abruptly change the course of evolution, giving rise to something totally different from the starting point. With evolution, on the other hand, we do not lose contact with the past, rather we gradually abandon the starting point, reach out towards the future in increments.

163. Living innovation and organizational creativity do not refer to transformation but to adaptation. Organizations are in an on-going process of change and we are obliged to adapt naturally to the environment if we want to remain in it. **Adaptability** is, in fact, the ability to change in order to continue advancing towards a different environment.

164. If the **final aim of adaptation** is not change itself but survival in the new environment, why do we continue to talk about transformation? The reason could be that instinct propels us to reject something that does not work and replace it with

something new. But this is not the objective sought; the objective is to continue being useful and effective in the new context.

165. At times transformation will be indispensable in order to make progress but transforming is not necessarily the solution. In the present case, it is precisely an on-going process of adaptation that will permit the Armed Forces to take advantage of the opportunities and confront all the challenges of OE 2035 without losing the essence or the values that inspire our actions.

11. A model of innovative change

166. Designing the military Force for 2035, considering the operational scenarios and the tasks envisaged, will need to take into account the **principles of feasibility and sustainability**, whilst ensuring anyway that the model contains a proper balance of military capabilities.

167. As part of the Defence Planning framework, this premise will make it necessary to **adapt the Armed Forces gradually to the new times and situations** with the required adjustments that Colonel John Boyd (USAF) considered a key factor for a force. These were, in order, "people, ideas and tools".

168. The "**people**" are the human resources (R) the training (T) and the organization (O) of DOTMLPF-I. These are the "people" who define how the "ideas" and the "tools" are combined and interact in order to adapt to the environment. The way in which the "people" are organized, through legislation, regulations and organization, determines which "ideas" and "tools" are developed and flourish, and which fade or disappear. Organizations therefore act efficiently when they achieve synergies, making it possible to link the strengths of the individuals with the common goals. It will therefore be necessary to give the people the skills that allow them to empathize with the viewpoints and positions of other organizations and that train them for cooperation and leadership as part of interdisciplinary teams.

169. Although we could find a certain parallel between the "ideas" and the doctrine (D) of DOTMLPF-I, ideas have a greater scope since they are the foundation of the theoretical debate about how organizations or groups (people) are formed, how they operate and how the "tools" are designed and planned. Ideas therefore form the context for what is done with the "tools" and drives the training and modification of the groups. Special mention should be made of the Concept Development Joint Centre (CCDC) accomplishments in creating innovative ideas in the realms of prospection, concepts and doctrine as drivers of change in the SAF. Among the "ideas", the principles and values by which any organization is governed could also be included.

170. The "tools" could be the materiel (M) and facilities (F) of DOTMLPF-I. The changing nature of conflicts is due to sociocultural factors, motivated in great part by technological advances in the "tools". The "tools" come from the "ideas" but sometimes, and this is occurring recently, it is the unstoppable development of technology that is giving rise to new "ideas" and new group structures (people). For Colonel John Boyd, however, the "tools" are not the important element of the whole as they "do not fight" wars by themselves but through "people", who also use their minds.

171. **We create strategic agility when we innovate or make changes, adjustments or improvements in the three areas** mentioned above and when we seek new possibilities in each specific area that will help us to release all the potential of the others. We also achieve agility by exploring several alternatives in each area, creating the adaptability needed to respond to future challenges, which we will not be able to completely anticipate, however.

172. The ideal situation would be that innovations in these three areas occurred simultaneously; that the interaction between them would provide us with synergies to increase the efficiency and effectiveness of the organization; and that this on-going process of adaptation to new environments (from version 1 to version 2) would extend gradually and uninterruptedly over time (Figure 12).

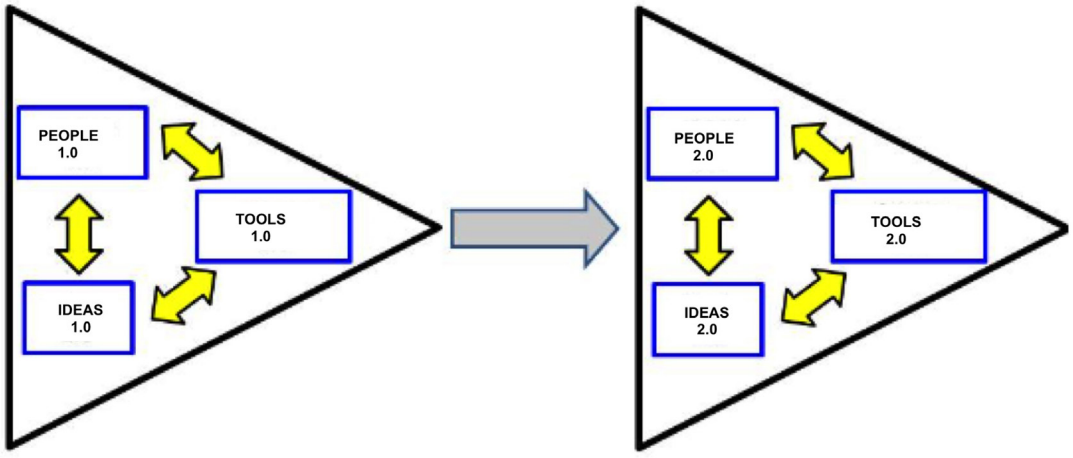


Figure 12. Balanced innovation among People, ideas and tools

173. However, advances often emerge in one area without similar advances in the other areas, creating an imbalance that frequently leads to unpredictable and undesirable results. Therefore, the result is that we have designed "Tools 3.0" but we continue to be stuck with the old ways of thinking ("Ideas" 1.5) or with obsolete, antiquated bureaucratic structures ("People" 1.0) (Figure 13).

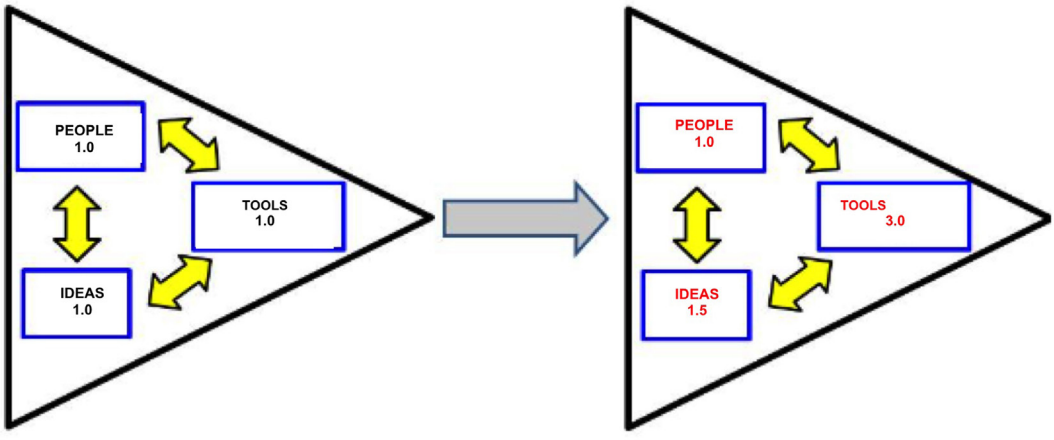


Figure 13. Unbalanced innovation among People, ideas and tools

174. Increasingly rapid technological change will require leaders who understand its implications and the new operating environment and its realities. Imagination and intellectual qualities are as important as the specific technical and tactical details of warfare. The great challenge here will be how to inculcate these qualities into the Armed Forces personnel.

175. Based on the characteristics of the future operating environment, the following section will synthesize the main consequences or implications for the various aspects of DOTMLPF-I, so that the Armed Forces can gradually adapt to this environment.

12. Changes in the "people"

12.1. Human resources

176. The main capability of the Armed Forces, on which its effectiveness is based, is their personnel. Below are some **characteristics** that the personnel will foreseeably have in the 2035 environment:

- There will be a sufficient number of troops for the missions entrusted to them by the policy makers, in which the **quality and preparation of their members will take priority over the quantity**. The demographic situation and the sociological structure of the Spanish population makes it possible to foresee certain difficulties in recruiting troops, so that decisions will need to be made to compete with other sectors for human resources. Technology and process automation will permit a reduction in personnel numbers. In addition, as it will no longer be possible to ensure technological superiority over other competitors, the qualitative advantage must reside in the talent and preparation of the personnel.
- To **counteract the possibly limited number of troops**, actions the following ones could be encouraged:
  - Optimizing the distribution of military forces by improving the personnel management processes, which will permit the transfer of troops from one speciality or category to another, and increasing the quantity and quality of the personnel in greater demand.
  - Outsourcing services or duties that could be performed by civilians.
  - Improving the current Reservist model, in line with neighbouring countries.

- Competing in the labour market for scarce personnel resources will mean **effectively motivating** commanding officers. To do this it will be necessary to:
  - Increase the efficiency of human resource management by improving the definition of the duties for differing positions, avoiding overload or unnecessary overlapping.
  - Improve trust at the intermediate and basic levels, by delegating and assigning responsibilities to suitable personnel so that they can take them on with guarantees.
  - Take advantage of and maximize all the talent in the organization, regardless of the service or rank, to prevent the disaffection of its members.
  - Improve the visibility and transparency of promotion processes.
  - Improve the socio-economic conditions and quality of life of members of the Armed Forces.
  - Implement models, similar to those in neighbouring countries, for the transition between the Armed Forces and civilian life (other parts of the public sector, companies in the defence sector, etc.), for personnel who have no career expectations but could still contribute valuable knowledge and professional experience.
- The selection and promotion of talent, a better definition of the career models and an on-going, exacting selection process essentially based on the criteria of merit and ability will guarantee that there are solidly prepared leaders on whom the future of the Institution will depend in an uncertain and complex environment.
- The diversity and complexity of the Armed Forces´ duties will demand, in parallel, the diversification and specialization of career paths.

12.2. Training

177. Preparation, a commitment to serving Spain and overall intellectual development will help the Armed Forces adapt to the future operating environment. Therefore, the following need to be promoted:

- Education and military training that do not consist only of merely transmitting knowledge and skills but of **thinking differently** in a world with different possibilities. In the new conflicts, leadership must be oriented to on-going adaptation to the growing complexity of operations, which are executed at a fast pace by geographically scattered units that will act in a decentralized manner fit for dynamic environments. In these conflicts, the services will demand ever more innovative, adaptable and secure commanders. The leaders must be mentally agile and prepared to make decisions in chaotic situations, without having to wait for detailed guidelines from headquarters.
- Continuing education in military moral values to act effectively and in accordance with national and international law in an environment with many legal and ethical limitations; to **maintain a high degree of commitment, motivation, excellence, discipline and permanent availability**; and to reach a high degree of cohesion, without making discriminations of any kind.

- Proper **training in the new technologies**, as without these it will be impossible to interoperate with partners and allies or to counter technologically advanced threats.
- Proper **knowledge management**, which will determine the learning processes and greater understanding of the environment with which they are interacting.
- **Improved interoperability** with our partners and allies, and with other instruments of state power, which will mean merging training and using the "same language".
- Appropriate **physical ability** for **combatants** for the activity to be undertaken, which will require a clear definition of the staffing needs with the determining factors of the age and physical characteristics demanded for each post.
- **Education** and training in the new domains, such as **cyberspace** and cognitive.
- A **change of mentality** in the culture and organization that will make it possible for leaders to help their subordinates to implement instructional and training activities that foster innovation and problem-solving in combat.
- **Strengthening leadership training** which requires:
  - Imbuing them with greater "broad-mindedness" by encouraging them to compare their frames of reference with others that focus on efficiency.
  - Taking them out of the hierarchical environment in which they feel comfortable, questioning their frames of reference and testing out their suppositions so that they realize the difference between the processes of shaping the will and exercising command.

12.3. Organization

178. With the arrival of the "Information Age", fighting between groups, and even within a group, no longer occurs over the possession of information, as it did in the

"Industrial Age", since technological evolution allows access to and the dissemination of information to all levels of an organization. The problem that must be solved now is to determine **which information is of real interest** to each member of the organization and how to make it available to this person in the shortest time possible, in an accessible, understandable, manageable way, as an excess of unfiltered information could overwhelm the organization.

179. The **current organizational structures** are too bureaucratic, vertical and hierarchical; they slow down the information flow and do not have the agility needed to respond to a constantly changing environment. It is therefore necessary to consider the possibility of implementing more appropriate organizational and management models that would help reduce the time and implementation costs.

180. The "Information Age" makes it possible to create an interconnected world and a new operating environment, cyberspace, in which huge amounts of information exchanges are taking place. Operating in this environment means an enormous challenge for organizations with structures that are too rigid and hierarchical. Interconnectivity will however offer more opportunities for gaining a better situational awareness, through better ISR capabilities, and gathering more accurate information, which is available as never before. It will therefore be possible to stay ahead of the opponent's decision cycle and increase the **speed of command**.

181. The speed of command and the need to respond in real-time will need changing the classic **concept of battle rhythm** as it would be very difficult to deal with new situations. It will be therefore necessary to consider making changes of this kind in the joint doctrine of employment of the Armed Forces.

182. **Increasing the available bandwidth and redundancy of communication systems and improving information dissemination** will allow the Armed Forces of 2035 to carry out actions that were previously impossible. Increasing the bandwidth will help to increase the information flow. The greater reliability of the CIS systems will make it possible to improve connectivity even in the most demanding conditions, and the greater redundancy of systems will prevent their being neutralized in degraded environments, permitting a rapid advance to network centric operations (NCO). In this way, greater systems resilience will be achieved, guaranteeing them greater survival rates.

183. In the future, most operations will **require coordinated action by the Armed Forces** with other state and non-state actors, whether international or not. This will make those responsible for planning to face uncertainties regarding what they are supposed to be prepared for, i.e. to perform more complex tasks and to have less room for error. The quality and accuracy of information will be much more important when it is necessary to act under the premises of "zero casualties" and "zero collateral damage".

184. **Shared information systems** will allow commanders to obtain the intelligence needed directly from the data repositories, in many cases eliminating the need to have intermediate ranks to channel and handle the information. This will permit a "thinner, flatter" structure, which will allow commanders in the lower ranks to better support decision-making.

185. The new scenarios will introduce an ever-increasing Chaos, making decision processes less and less linear. It will gradually become more necessary to handle larger quantities of information more rapidly, by adding an increasing number of information sources obtained by an expanding constellation of sensors. It will therefore be necessary to adapt our response capability to a **distributed environment**.

186. Converting the enormous amount of information into "knowledge of the situation" requires systems that support this process and a large amount of experience. It is necessary to go beyond what "is happening" or what "could happen" and see **what "can be done"**. This will involve creating options, anticipating the actions and reactions of the adversary and understanding the effects of each of the possible lines of action.

187. In the future, it will be necessary to add to the traditional duties of "Command and Control" (C2) others that are more related with leadership, such as **inspiration, motivation and the creation of trust**. These duties can be performed in different ways but in the end it all comes down to determining what the "interaction patterns" between the different actors are, how they are distributed throughout the structure that has come to be called "decision rights", and how information flows and the knowledge of the situation is shared. These three factors are vital when studying the different approaches that can be made to OS 2 (Figure 14).

Figure 14: Summary of the Future Command and Control

	Industrial Age (past)	Information Age (future)
Decision rights	• Centralization • Ranked vertical structures • The leader directs, plans and controls	• Flat, decentralized organizations • The leader provides a consistent, clear intent
Interaction patterns	• The originator of the information is responsible for deciding which information to share, how to organize it, who to send it to, and how often to update it	• It is the users who configure their own information depending on their needs, starting from the fact that they have access to all they need and the authority to do so
Distribution of information	• Centralized systems • Limitation on the distribution of information, depending on the "need-to-know"	• All information is available to all entities. The limitations are linked to the need to implement the principles of guaranteeing information

188. It is foreseen that the dominant trend in military organizations will move away from a hierarchical structure toward the **assumptions of network centric operations**. However, it is somewhat improbable that hierarchical organizations will disappear, and it will be even more possible that both concepts will evolve and adapt in order to coexist. It will therefore be a question of obtaining greater combat capability from geographically disperse entities, sharing information and, where appropriate, transferring authority.

189. Network centric operations (NCO) are based on three factors: geographically **dispersed forces**, a high degree of training and experience and a robust, reliable network linking these forces. The dispersal of forces reduces vulnerability and therefore risk. At the same time, training and experience make it possible to reassign responsibilities dynamically so as to adapt to a constantly changing situation.

190. However, the general resistance to change in hierarchical structures could make the innovations brought about by the "Information Age" produce disagreements or friction during the implementation of strategies, tactics or procedures. To resolve these problems, it will be necessary to have coordinated management that maintains discipline and cohesion. It is therefore considered that **our organization must evolve** to adapt to the concepts of network centric operations.

191. This evolution will require the implementation of radical changes in the processes, mentality and culture of the organization, in addition to adapting to technological advances. But, above all, it will require a **new vision of leadership** that fosters the ability to delegate authority, take on and handle risks, act with initiative and adapt agilely to command intents.

192. In the year 2035, the Armed Forces will be characterized by their access to a huge volume of information, be totally interconnected and interact with all levels on the chain of command, and even with other actors outside the organization, and will need to develop a **more creative, collective leadership**. Each and every one of the individuals, even in the lowest ranks, must be leaders at that level and contribute their abilities to the overall, shared leadership of the organization.

13. Changes in the "ideas"

193. The "ideas" are **intimately related with the Armed Forces**, in the sense that the very nature and concept of the forces were the product of translating these same "ideas" for the real world. In other words, the structure, organization, resources, personnel, training, etc. are designed to be and are the practical manifestation of those "ideas" and not others.

194. In addition, the way the Armed Forces operations are codified in its doctrine, which acts as a **"bridge" between the theory of warfare and the practice**. The theory that inspires the doctrine (on warfare, combat, the way to win, etc.) usually stems from the experience gained in past conflicts, whose lessons learnt and conclusions are applied to the conflicts ahead, in order not to fall into the errors of the past. This is why at times it is said ironically that armies prepare for "past wars".

195. However, despite the difficulty in predicting future challenges exactly, the doctrine should also consider **proposals or solutions for the use of force** when new tactical concepts appear, possible disruptive technologies emerge and states change their strategies, the sociological nature of the armies alters, dominant ideologies appear in their societies based on their hierarchy of values, etc., in order to anticipate events and prevent outdated, reactive movements.

196. Consideration **should therefore be given to what capabilities**, for example, in densely populated urban areas or on the coast; what the future land, sea and aerospace capabilities should be like; what we are doing to counter some of the challenges and threats that lie ahead, such as demographic explosion and mass migration from Africa; how demographic decline and the ageing population will affect the Armed Forces; what systems will be necessary to operate over discontinuous fronts and areas; what the role of the Armed Forces will be in the fight against terrorism and organized crime; or how the legal and legislative frameworks that regulate armed conflicts will evolve.

197. There is a number of questions to be answered before implementing changes; to list only a few: Which new missions or operations will the SAF take on? What challenges will they face to confront a hybrid threat or how they will prepare to operate in the "grey area" in an armed conflict? What will be the role of special operations in an irregular conflict? How will the SAF operate in the five domains? What should be the human factor like? How should we manage talent? How can we better integrate all the elements of state power? What systems should we prioritize and to which should

we commit? What consequences will the militarization of outer space bring? How will emerging and disruptive technologies affect us? How can national resilience or support from the public for our missions be improved? What should the organization and structure of the SAF be like? What type of infrastructure should we have?

198. The permanent and unwavering military principles and values must continue to be the pillars on which the military institution rests and constitute the basis and foundation of our daily activities. In spite of changes brought about by OE 2035 in all aspects, the principles and values will remain unchanged.

14. Changes in the "tools"

14.1. Materiel

14.1.1. Disruptive technologies

199. Most nations are aware that technology is a differentiator. That is why prospective studies are made to anticipate technological changes that the future will bring and their impact, cost and benefits. The aim of such studies is to exploit opportunities and mitigate the risks inherent in deciding whether or not to introduce new technological discoveries.

200. Changes in technology have a major impact on the changes taking place in societies and, although they tend to be implemented gradually, at times the appearance of a particular technology or a new use for an existing one leads to a radical change in the scientific world, society as a whole and the way of dealing with conflicts. These are what are called **disruptive technologies**.

201. Not identifying a disruptive technology in time means that a factor that would help bring superiority has been ignored, increasing the technological gap between those who have adopted this technology and those who have not. Although it is difficult to pinpoint the **impact of** those **technologies** in a future scenario, undoubtedly, some of them will be pivotal for the design of a variety of systems.

202. In the military sphere, the **application of disruptive technologies** leads to operational changes, with consequences for the organization and also profound changes in the doctrine and strategies that will also be disruptive. History is full of examples: the military use of gunpowder, the introduction of tanks, the rise of military aviation, submarines, nuclear weapons, etc.

203. The appearance and use of disruptive technologies can pose **ethical issues and debates** about their application and possible consequences that at times are extremely intense. We only have to think of the debates arisen since the appearance of nuclear weapons.

204. Now we are seeing a debate about the use of **robots**, especially about whether they should be given a high degree of autonomy from human control. There is also a debate about using unmanned aerial vehicles (UAV) equipped with precision weapons to combat terrorism, due to the legal and ethical implications of their being used to execute terrorist leaders and the possible "collateral damage" that can be produced. We must also not forget the debate about the **use of cyber weapons** and

the type and magnitude of a response to a cyberattack owing to the difficulty of pinpointing its source.

205. There are countries that base their strategic culture on gaining **technological superiority** over their adversaries, although there is the perception that the technological superiority that has been shown to date is in danger, since the technologies on which it was based are, or soon will be, available to other actors.

206. The "US Defence Innovation Initiative-2014", in addition to proposing a need for significant changes in the organization of the Pentagon and expanding procurement procedures, focuses on the so-called *"Third Offset Strategy"*, which aims to adapt a new technological disruption that will permit the USA to maintain its broad military superiority over any possible competitor.

207. In September 2014, the "Center for Technology and National Security Policy" of the US National Defence University published a study that analysed the different areas in which **new disruptive technologies** would be developed. These areas were:

- Telecommunications and cyberspace.
- Energy.
- Autonomous and unmanned military systems.
- Directed energy weapons.
- Biotechnology.

And, in a series of appendices, it identified the **key emerging technologies**:

- Biology, biotechnology and medicine.
- Robotics, artificial intelligence and enhanced human capabilities.
- Telecommunications and cognitive science.
- Nanotechnology and advanced materials.
- Energy.

208. The "*Third Offset Strategy*" also identifies the **key technologies** that could maintain dissuasive supremacy and keep the peace in this new 20-year cycle. Among these technologies are robotics and autonomous systems, miniaturization, big data and the use of advanced manufacturing techniques 3D/4D printing, etc.).

209. This would further widen the **technological gap** between the USA and the European countries, which would lead to a decrease in the interoperability of their respective Armed Forces and the development of defence and technological industry base, which would be a cause for concern for the people of the United States and Europe.

210. Spain should not be left out of this innovative technological development process as this would not be appropriate either for our security and defence policy or industry. There are two approaches, which are not exclusive, that will permit our weapons systems not to miss out on the technological advantage that the **4th Industrial Revolution or "industry 4.0"** would provide.

211. On the one hand, at the national level, by having the ITDB become more involved in the design of the Forces right from the initial stages of designing the operational or functional needs, using the instruments and channels established at the department level, which would give us autonomy and freedom of action. In recent decades, procuring equipment and weapons systems from the Spanish defence industry has contributed to its development, the modernization of the Armed Forces and the wealth of the country, bringing a value added and substantial income for the public coffers. It is considered that this same strategy could continue or even be strengthened in the coming years.

212. If one looks at the speed at which changes are occurring in the world around us, some technological and industrial areas, of undoubtedly military origins, are developing more rapidly in the civilian sector. Apart from the duality of technologies and processes, it is the private sector that is exerting the "driving force" on the defence sector, so that it will be indispensable to count on it in the future. Disruptive technologies have their origins in two areas: public and private (or a combination of the two). These technologies do not appear on the market freely but are driven by public or private research resources, and therefore the Armed Forces should consider the need of contributing actively to the debate or prioritizing some technologies over others for operational reasons.

213. On the other hand, at the international level, by our participation in NATO, EU and EDA (European Defence Agency) forums and groups and ad hoc multinational initiatives. It is foreseeable that the most disruptive technologies will be developed for sophisticated, complex resources, which will only be acquired by Spain through these cooperation models. It will be these projects that will ensure that Spain has a competitive industrial base and a valuable geo-strategic position in the public environment. It will be essential for Spanish industry to be part of development programmes in cooperation with other European nations.

14.1.2. Future military applications of disruptive technologies

214. Following the initiative of the United States, despite the disparity in resources and geopolitical interests, it is considered that the following technological areas should be strengthened, due to their interest for defence:

14.1.2.1. Robotics and unmanned or autonomous systems:

215. In the world of unmanned vehicles (UV), despite the enormous growth in the demand for them and their employment in the air (UAV), and to a lesser extent on the sea (USV and UUV) and on land (UGV), their use is limited and restricted to very specific applications. In spite of the term "unmanned vehicle", it would be more correct to call them remotely piloted systems (RPAS).

216. There is a tendency to equip unmanned systems with greater intelligence and autonomy by applying robotic technologies that avoid having these systems piloted remotely. This paradigm of remote operation is changing and there is a wish to evolve to systems with greater decision-making ability and a greater degree of freedom. The next challenge will be to build **completely autonomous systems** that can interoperate with human beings in a natural way.

217. The situation on the battlefield changes instantly on dynamic environments. The human brain can operate in dynamic environments, rebuild paths and predict what the next movement will be adaptively in real-time. For this reason, autonomous systems that are deployed in an operation zone must be capable of doing the same thing, without requiring constant supervision by their human controllers.

218. This challenge involves enormous complexity. In the coming decades, the increase in the computing capability of new processes, the improvement in the possibility of sensor fusion and advances in the area of artificial intelligence will permit these systems to operate more and more autonomously on the battlefield.

219. **Potential military applications.** The duality of the technology used in the different UVs is absolute, making the transfer of technological advances from civilian to military applications easier.

220. In the air, UAVs are very useful for ISR operations, security and surveillance, target spotting, artillery support, communications relay, electronic warfare and combat (UCAV).

221. On the sea, UUV and USB are very useful for minesweeping and neutralization, in surface and submarine warfare (when equipped with weapons of various types or with targeting devices for ballistic attacks), electronic warfare etc.

222. On land, exo and endoskeletons are also under scrutiny. The most important applications in which terrestrial robotics have a sufficient degree of maturity are detecting improvised explosive devices (IED), measuring environmental conditions in environments with CBRN contamination, transporting loads, clearing routes, search and rescue in hard-to-access places, etc.

223. One relevant area of study, which offers controversies from the ethical, legal and political point of view, is the degree of autonomy that lethal autonomous robots (LAR) should have. The challenge is to define the limit of minimum human control required to enable the use of these systems in a reasonable context. The development of that autonomy is based on a "decision-making" algorithm that will be implemented in the systems. One of the great dangers in the future is that artificial intelligence can be corrupted by a cyberattack and that entire technological advantage used against those who developed it.

14.1.2.2. Power generation and storage

224. The development of new biofuels has important geostrategic and operational implications. A second generation is currently under development, based on bioengineering and the genetic modification of organisms, such as algae, to be used as a source of biomass or bacteria to synthesize biofuels. The application of technologies linked with decarbonisation should also be mentioned. They include electrifying transport and generating power using renewable resources.

225. **Potential military applications.** The financial and logistical costs of fuel pose one of the most important problems for the different forces. Any reduction in these costs could reduce the bill for operations by millions of euros per year. The availability of power is a key factor for both platform propulsion and the functioning of military installations.

226. Technologies that permit the development of light, flexible solar cells with greater efficiency than current, commercially available technologies, waste gasification systems, the use of renewable resources (wind power) or alternative non-conventional systems (fuel cells) will all be of interest to the Armed Forces.

227. Energy efficiency must be improved by developing new climate control systems (active and passive) and including systems that have already been proven

in the civilian world. This efficiency can drastically reduce energy consumption during operations.

14.1.2.3. Directed energy

228. Directed energy weapons use lasers to emit electromagnetic energy in different ranges of the spectrum (mainly visible and infrared) directed towards a precise target and do not launch any kind of projectile. This type of weapon only consumes electrical power (they transform the electrical energy into electromagnetic radiation), so that they do not require conventional ammunition.

229. Their generalized use, when adapted to defence applications, would imply a disruptive logistical change, as to use them only a source of electrical power would be needed, so that they could operate using photovoltaic solar energy. Without taking into account manufacturing and development costs, their hypothetical use would therefore be much more economical.

230. In addition, as the pulses emitted travel at the speed of light, no correction of the firing trajectory is required when aiming at targets, even when these are RPAS or missiles. No correction is required for wind or gravity either. Their precision is very high and, unless an error is made when discriminating the target, it is very difficult to create collateral damage. Obviously, laser weapons are not classified as weapons with "indiscriminate area affects".

231. High-power microwave weapons (HPM), which are grouped among non-lethal weapons (NLW), consist of generating and radiating a high-powered electromagnetic pulse (EMP) that prevents the use of, disables or even destroys electrical and electronic systems and equipment. The military has an obvious interest in possible weapons of this type and with the development of power generation technologies, above all on the fringes of microwave frequency, there is a growing concern in military circles about the operational use of such weapons, which exploit the vulnerability of electronic systems, the cornerstone of modern warfare in the 21st CENTURY.

232. **Potential military applications.** There are many: the most important are countermeasures against missiles or mortars; the destruction of aerial platforms, especially RPAS, and self-protection for ships, e.g., against suicide attacks using small boats. Due to their power and precision, HPM could also be used against personnel, although it would be necessary to take into account the possible legal and ethical issues.

233. The applications for electromagnetic weapons are varied. They include the integration of HPM measures into conventional weaponry, the protection of components and sensors to avoid their operation being disabled, systems to neutralize mines or immobilize vehicles, measures to reinforce components and make them more reliable against this kind of radiation, etc.

14.1.2.4. Metamaterials and advanced manufacturing techniques

234. An increasing number of materials and processes that were developed for civilian use are being used in the military sphere, such as the recent cases of graphene, 3-D printing and nanotechnology.

235. The properties of graphene, such as its high electrical conductivity, thermal conductivity, elasticity and mechanical resistance, have great potential for military applications.

236. Additive manufacturing (AM), or 3-D printing, describes manufacturing processes in which a machine lays down layers of material that then fuse to form an object of almost any shape. The best-known 3-D printers use plastic polymers in a process similar to the way a common ink injection printer works. However, they can also be used for a much wider variety of manufacturing processes, such as constructing buildings, printing metals and alloys and even creating human tissue.

237. With nanotechnology, new materials can be obtained that have superior electronic, magnetic, optical or mechanical properties to conventional materials.

238. **Potential military applications.** Graphene has applications in sectors such as electronics, to manufacture smaller devices with more features; energy, to be used as a component in long-lasting batteries, to improve the performance of power generation systems by making the same features provide greater autonomy to the systems supplied and increase the useful charge; and new, more resistant and lighter composite materials, to provide personal protection with great ballistic resistance, much less weight, and for possible use in composite armour.

239. Nanotechnology permits a great number of applications, such as nanomaterial in the form of particles, fibres or laminates, intended to increase the protection and safety of combatants and reduce weight and costs. It can also be used for armour for land, air and sea platforms, improving their structural resistance and reducing their weight.

240. Nanotechnology will also permit new, more efficient, selective and sensitive sensors to be used to detect chemical, biological, nuclear, and explosive agents (CBNE) or for sensors that can be incorporated into the soldier's uniform or the structure of a platform and are capable of determining whether that soldier or structure is in a condition to take part in a mission.

241. In addition, miniaturization will affect drones, so that micro-drones and nano-drones equipped with weapons, sensors, video cameras, listening devices, etc. will emulate birds, insects and small animals so as to be used in surveillance applications on the streets, alleys and hidey-holes of urban environments. They could also act in swarms when equipped with explosives, and have a great lethal effect.

242. Other applications will be damping the ability to detect -by reducing the radar, infrared, acoustic, etc. signature-, improving the efficiency of power generation and storage systems, self-repairing, maintaining thermal comfort in extreme weather conditions, self-cleaning, etc.

243. 3-D printing is also of great interest to the military sector as it is a way to obtain a wide range of parts, replacement parts, etc. quickly and relatively cheaply. The articles that have been produced to date range from basic forms of small weapons to rocket motors, although there is concern about their possible use in nuclear weapons programmes, to produce centrifuges for uranium enrichment.

Where there will be a great potential impact is in the aeronautics and missile production industry.

14.1.2.5. Big data or macro data

244. Big data is a concept that refers to the fact that in the future such enormous datasets will be handled that traditional data processing applications and the procedures used to date to find repeated patterns in that data will not be capable of dealing with them. The most common difficulties linked to managing these huge quantities of data centre around collection, storage, searching, sharing, analysis and display.

245. The datasets will grow exponentially, due in part to mass data collection by a variety of sensors. Because of their diversity, there will very probably be infinite unrelated original tables. The next objective will be to collect the data in one place and format them. When the required data has been stored, using a variety of storage technologies, it will be necessary to analyse them using a variety of techniques. Lastly, it will be necessary to display the information in a well-structured presentation of the statistical results, in the form of graphs or maps, which are better than tables with numbers and conclusions. The display will necessarily be in simplified, entertaining and attractive formats.

246. **Potential military applications.** The information and communication technologies (ICT) are the sector responsible for handling big data. The two areas particularly affected will be: JISR devices or sensors generating heterogeneous data that will need to be stored, merged, analysed and presented at great speed, and the command control networks that will permit appropriate decisions to be made using these data. It will be necessary to pay special attention to the concept of the "combat cloud", to be understood as an interconnected network for distributing data and exchanging information within a battle space, in which every user, platform, or authorized node contributes to and receives essential information in a transparent manner and can use it for the entire range of military operations. The ability to compile data and include them in an open, adaptable information system will significantly improve the command and control capability and the operating agility of forces in combat.

247. The goal will be to provide the Armed Forces with a collaborative, instant and intuitive situational awareness at all levels of command, from the commander to the combatant. To do this, the relationship between man and machine, or human machine interface (HMI) technologies, will be fundamental. The data and information must be presented clearly, in a user-friendly, effective manner, so that it does not saturate the operator or omit any information of importance to the operation. Therefore, improving the technologies related with data processing algorithms, interface architectures, data merging, quantum computing, etc. will help to reduce the stress levels of the operators, which will be reflected in an improvement in the operation of the systems.

14.2. Facilities

248. The number of military properties and facilities has shrunk in recent years, although its reduction rate is less than for the personnel, and also less than cutbacks in military facilities of other neighbouring countries.

249. In addition, to prevent making significant **investment in** the future **maintenance**, both preventive and corrective, of military facilities, it would be appropriate to adopt measures either to maintain the current facilities adequately or to care properly for the facilities that are considered indispensable.

250. For these reasons, to meet the future needs of the Armed Forces, in terms of personnel efficiency and material and financial resources for facilities, the Armed Forces must consider the adoption of measures designed to improve its availability and use. These measures should include a more **joint use** of our resources, eliminating duplication and reducing common or functional services so as to have greater efficiency.

251. From the organisational design perspective, the facilities should also include the Armed Forces´ latest technological and organizational features. The facilities must therefore be intelligent, interactive, multiuse, modular and networked.

252. Climate change will require alterations to the facilities to reduce their environmental footprint and improve their energy efficiency. Climate-related criteria will need to be considered in the risk analysis and investment decisions and technical specifications for the infrastructure, so that they are also made resistant to climate change.

15. Interoperability

253. Interoperability is the "I" in DOTMLPF-I, and it is the quality or factor that cuts across the other components (DOTMLPF) of each capability so that they can operate together.

254. An increasingly integrated approach to security that offers comprehensive responses to future challenges, which will be multilateral and multidimensional, will demand that the Armed Forces have a greater capability for interaction within each other and with other actors. It will be necessary to look more closely, in the first place, at **joint action** in areas such as C2, CIS, JISR, cyber defence, strategic communications and personnel training.

255. It will also be necessary to seek closer **combined integration** during operations and through cooperation initiatives in the area of capability planning (e.g., Smart Defence, Pooling & Sharing, etc.), education and training, information exchange, procedures, etc.

256. Lastly, the Armed Forces must **combine its actions and coordinate its operations with other instruments of state power** and with non-state, domestic and foreign actors, such as multinationals, NGOs, local populations, individuals, etc.

PEOPLE			IDEAS	TOOLS		
				MATERIEL		
HUMAN RESOURCES	TRAINING	ORGANIZATION	DOCTRINE, ETC.	DISRUPTIVE TECHNOLOGIES	MILITARY APPLICATIONS	INFRASTRUCTURE
• Optimize the distribution of military forces by: ○ Improving personnel management processes, which will permit the transfer of troops from one specialty/category to another ○ Outsourcing services or duties that could be performed by civilians ○ Improving the current Reserve model • Compete in the labour market by efficiently increasing motivation to Avoid overloading and ○ verlapping positions ○ Increase the trust between commanders and subordinates to Optimize talent to Improve the visibility and transparency of promotion processes the visibility and transparency of promotion processes. ○ Improve socio-economic conditions and quality of life • Improve leadership by: ○ Optimizing talent or Defining career models or A rigorous selection process • Diversify and specialize career paths	• Determination, initiative, agility, flexibility, creativity and ability to adapt • Unwavering moral commitment • Familiarity with new technologies • Proper knowledge management • Improved interoperability • Adequate physical ability • Training in new operational domains (cyberspace and perceptions) • Greater responsibility for subordinates • Critical thinking	The C2 duties can be developed in different ways but in the end it all comes down to determining what the "interaction patterns" are between the different actors, how what have been called "decision rights" are distributed throughout the structure, and how information flows and a knowledge of the situation is shared. In the future it is considered that these functions will be characterized by: • Decision rights: ✓ Decentralized organizations / The leader provides a consistent, clear intent • Interaction patterns: ✓ The originator of the information is responsible for deciding which information to share, how to organize it, who to send it to, and how often to update it • Distribution of information ✓ All information is available to all entities. The limitations are linked to the need to implement the principles of guaranteeing information	• Improve the theoretical debate to match the doctrine to the characteristics of the future operating environment and not to the teachings of past wars • Permanent and unwavering military principles and values on which the military institution rests.	• Robotics and unmanned systems • Power generation and storage • Directed energy • Metamaterials (graphene, 3-D printing and nanotechnology) • Big Data	• ISR, security and surveillance, Target Acquisition, artillery support, communications relay, EW and combat (UCAV), • Mine sweeping and neutralization and surface and submarine naval warfare, • Detection of IEDs, measuring environmental conditions in CBRN environments, transporting loads, clearing routes, • More efficient technologies • Improved energy efficiency • Countermeasures against missiles and mortars, destruction of aerial platforms, self-protection for ships, against snipers and infantry troops, etc. • Improved protection for combatants and systems; more efficient sensors to detect CBN-E agents; miniaturization; reduced detectability • ICT sector, sensor information processing, C2 networks	• Improving the efficiency of personnel occupancy and the assignment of material and financial resources. • Including new technological and organizational features in the Armed Forces: intelligent, interactive, multiuse, modular, networked facilities, with a small environmental footprint and high energy efficiency.
INTEROPERABILITY						
- Between components of the Armed Forces - With partners and allies - With other instruments of state power						

Figure 15. Summary of the proposals for changes in DOTMLPF-I

16. Potential areas of change to adapt the Armed Forces to Operating Environment 2035

257. The ISDOs of which Spain is a member will keep their superior conventional capabilities and an effective nuclear deterrence, but this favourable military balance will not be static as our potential adversaries will develop asymmetrical strategies that circumvent the superiority of conventional forces and exploit our potential vulnerabilities, creating conditions that delay, deter or counter the application of superior military capabilities.

258. It is also to be expected that potential adversaries will **constantly adapt to our capabilities** as they evolve, with the aim of narrowing the technological and conventional divide.

259. This situation should encourage us to adapt our capabilities to the uncertain, complex, asymmetrical and cooperative operating environment of 2035, so that **the Armed Forces should:**

- **Improve its strategic agility.** In an uncertain environment, Armed Forces with big, inflexible units that require months to deploy cannot react sufficiently rapidly or face up to all the problems.
- **Reduce the logistical footprint.** Complex supply chains, platforms with high fuel consumption and the need for frequent and costly maintenance by specialized personnel are contrary to agility and make the forces more vulnerable. It is therefore necessary to invest in certain emerging technologies.
- **Optimize the costs of operations and supply.** Making systems universal, permitting the sharing of components and maintaining a broader range of units with the same amount of training, brings cost savings and contributes to reducing the logistical footprint.
- **Optimize the distribution of military forces.** The current demographic situation in Spain, process automation, effective weapons systems, the introduction of autonomous systems, the greater survival rate of combatants and better personnel management processes will allow troops to be transferred from one specialty or category to another.
- **Improve talent management.** The uncertainty of OE 2035 and the complexity of military operations will demand professionals with determination, initiative, agility, flexibility, creativity and adaptability. It will therefore be necessary to attract and retain those who best serve the interests of the institution and to facilitate the transfer of personnel to other civilian institutions when there is a surplus.
- **Commit to technological superiority.** Technological superiority and doctrinal innovation will be key factors in guaranteeing superiority in a confrontation. It will therefore be essential to develop a strong, innovative and sustainable national defence industry, have cooperation agreements with the ISODs of which Spain is a member and take part in joint European equipment and military systems development programmes.
- **Improve surveillance and analysis capabilities.** The complex and changing future environment, the great number of actors involved and their dispersal will necessitate the early identification of threats through on-going, global

surveillance, which will require the strengthening of autonomous and non-autonomous JISR systems.

- **Improve capabilities in cyberspace, cognitive domain and outer space.** It seems obvious that there is an increasing trend toward increased non-conventional and hybrid threats and strategies and toward increasing action by our potential adversaries in the "grey area". In addition, the economic use of outer space and its progressive militarization will require the development and strengthening of space systems.
- **Improve interoperability, with state and non-state actors, inside and outside our borders.** The complexity of the environment, the variety of challenges and the impossibility of taking on all of them autonomously will mean that polyvalent capabilities must be acquired and the education and training of the personnel must ensure that they act cooperatively. At the same time, it should not be forgotten that the first and most important challenge, which has not yet fully developed, is achieving the full, joint integration of all Armed Forces capabilities.
- Make **organizational and structural changes** to implement the above-mentioned proposals by simultaneously and efficiently assigning all resources (for personnel, materiel, financial and facilities).

260. The future is already here and **change is essential** for the evolution and advancement of society. Organizations that close themselves off from change are condemned to disappear, unlike those that introduce innovations in the various areas of social activity. Organizations, especially the more complex, continue to be strongly resistant to change and adapting to the new challenges and environments. For this reason, efforts and investment (both intellectual and tangible) to encourage innovation are essential in order to triumph in the new scenarios. This is also true in the areas of security and defence and, more specifically, the military.

261. What is needed is **Armed Forces that fit the new times**. The coming years will require an intense and continuing effort to change, which will lead to bold, imaginative decisions being taken in the various areas of DOTMLPF-I in order to be more useful to Spanish society and, at the same time, more effective and efficient. A decided struggle must be waged against their own vulnerabilities, which will mean an effort to modernize the Armed Forces and prevent their decapitalization.

262. The future is challenging and we must choose the path to follow now. Change is inevitable; we must choose to drive it, or be its victims. Our main partners and allies have already started out on a path with no return.

Summary of Chapter 3

AIM: **"To determine the characteristics that the Armed Forces needs in 2035 and the consequences or implications of change in the various areas of DOTMLPF-I so that they can adapt to the operating environment."**

SUMMARY

8. ABOUT CHANGE. Determine the way in which to bring about the change that is required of the Armed Forces

9. THE NEED TO CONFRONT CHANGE.

- The paradigm of conflict is changing
- Quantity and variety of the Armed Forces duties
- Budget-related factors
- Difficulty of designing the Armed Forces
- Armed Forces that fit the modern times

10. THE DIFFICULTY OF UNDERTAKING CHANGE

- Individual factors:
  - Little open-mindedness
  - Professional impact
  - Cumulative experience
  - Confirmation bias
  - Generation gap
- Organizational factors: Organizational culture, corporatism, traditions and interests

11. HOW TO MAKE IT? TRANSFORMATION OR ADAPTATION?

- Transformation vs. adaptation is like revolution vs. evolution
- Adaptability is the ability to change in order to continue advancing in a different environment

12. A MODEL OF INNOVATIVE CHANGE. Adapting the Armed Forces gradually to fit the new times and situations with the adjustments required in the "people, ideas and tools", keeping in mind for the model the principles of feasibility and sustainability.

13. CHANGES IN THE PEOPLE, IDEAS AND TOOLS. Deciding on possible changes that should be made to the Armed Forces before 2035, and synchronizing them with the different areas of DOTMLPF-I.

14, 15 and 16 POTENTIAL AREAS OF CHANGE TO ADAPT THE ARMED FORCES TO THE 2035 OPERATING ENVIRONMENT.

- Improved strategic agility.
- A smaller logistical footprint.
- Optimum operating and supply costs.
- Optimum number of military forces
- Improved talent management.
- Commitment to technological superiority.
- Better analysis and surveillance capabilities.
- Better capabilities in cyberspace and cognitive, and in outer space in the aerospace domain.
- Improved interoperability.
- On-going, flexible adaptation of the organization.

REFERENCES

- Spanish Constitution, 1978.
- Ministry of Defence, Defence White Paper, 2000.
- Ministry of Defence, Strategic Defence Review (Spanish initials, RED), 2003.
- 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.
- 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 2017.
- OPLAN "ARMED FORCES 2030". Proposal from JEMAD, 2017.
- Doctrine for the Employment of the ARMED FORCES, Joint Doctrine Publication (PDC)-01-(A), 2018.
- Panorama of Geopolitical Trends. Horizon 2040, drawn up by the Spanish Institute for Strategic Studies (IEEE).

BIBLIOGRAPHY

- EUROPEAN DEFENCE AGENCY (EDA). *Future Trends from the Capability Development Plan* (CDP) 2008.
- ALBERTS, D. S. (dir.) *et al. The Agility Advantage*. CCRP Publication Series, September 2003.
- ALBERTS, D. S. *The Information Age Anthology Volume III: The Information Age Military*. CCRP Publication Series, March 2001.
- BIALOS, J. P. & KOEHL, S. L. *What America's Big New Defense Plan Gets Wrong.* The National Interest, 2016.
- JOINT CENTRE FOR CONCEPTS, DOCTRINES AND EXPERIMENTATION (CICDE) France. *Conflicts in the Next 15 Years and Operating Consequences,* 2012.
- JOINT CENTRE FOR CONCEPTS, DOCTRINES AND EXPERIMENTATION (CICDE) France. *Environnement Opérationnel Futur 2035,* 2016.
- CENTRE FOR THE DEVELOPMENT OF CONCEPTS AND DOCTRINE (DCDC) UK. *UK Joint Concept Note 1/14, Defence Joint Operating Concept,* 2014.
- CENTRE FOR THE DEVELOPMENT OF CONCEPTS AND DOCTRINE (DCDC) UK. *Future Operating Environment 2035. Strategic Trends Programme*. 1st ed., 2014.
- CENTRE FOR THE DEVELOPMENT OF CONCEPTS AND DOCTRINE (DCDC) UK. *Global Strategic Trends (GST) out to 2045. Strategic Trends Programme*. 5th ed., 2014.
- COMMAND AND CONTROL CENTRE OF EXCELLENCE (C2COE), NATO. *Exploring Command and Control in an Information Age*. Information Age Seminar. Estonia, 2014.
- DEFENCE INNOVATION CENTRE (CID) Italy. *Military Implications of the Future Operating Environment,* 2012.
- MILITARY CENTRE FOR STRATEGIC STUDIES Italy. *The world in 2030. Regional Trends,* 2007.
- HIGHER SCHOOL OF NATIONAL DEFENCE STUDIES (CESEDEN). *Monograph no. 115,* April 2010.
- COLOM, G. *Transforming the Spanish military*. DEFENCE STUDIES. Vol. 16, no. 1. Seville: Universidad Pablo de Olavide 2016 pp. 1-19.

- NATIONAL INTELLIGENCE COUNCIL (NIC) United States. Global Trends: Paradox of Progress, 2017.
- DUBIK, J. M. Leadership beyond the Chain of Command. Army Magazine. Vol. 59, no. 12, 2009.
- DWORKIN, A. Drones and targeted killing. Definlng a European position. European Council on Foreign Relations, 2013.
- CHIEF OF THE DEFENCE FORCE Australia. Future Operating Environment 2035, 2016.
- FRÍAS C. J. 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, 2017.
- GRISSOM, A. The future of military innovation studies. Journal of Strategic Studies. 29, no. 5, 2006.
- HOROWITZ, M. and SCHARRE, P. Meaningful Human Control in Weapons Systems. Center for a New American Security, 2015.
- CHIEF OF FORCE DEVELOPMENT Canada. The Future Security Environment (FSE) 2013-2040, 2014.
- JORDAN, J. 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, 2017.
- JOINT CHIEFS OF STAFF United States. Joint Operating Environment 2035. The Joint Force in a Contested and Disordered World, 2016.
- JOINT CHIEFS OF STAFF United States. Mission Command White Paper, 2012.
- KADTKE, J. and WELLS II, L. Policy Challenges of Accelerating Technological Change. Security Policy and Strategy Implications of Parallel Scientific Revolutions. CTNSP at NDU, DTP 106, 2014.
- KEEGAN, J. A History of Warfare. Alfred Knopf (ed.), 2001.
- KOTTER, J. The Heart of change. 2002.
- LEVERINGHAUS, A. and GIACCA, G. Robot Wars. The Regulation of Robotic Weapons. Oxford Martin School. 2014.
- ALLIED COMMAND TRANSFORMATION (ACT), NATO. Strategic Foresight Analysis (SFA) Report, 2017.
- ALLIED COMMAND TRANSFORMATION (ACT), NATO. Framework for Future Alliance Operations (FFAO), 2018.
- MARSAL, J. Tecnologías disruptivas y sus efectos sobre la seguridad. (Disruptive technologies and their effects on security.) Annual Research Plan 2015. Working Document 12/2015. CESEDEN.
- MORALES, S. El futuro de la naturaleza de los conflictos armados. (The future of the nature of armed conflicts.) Framework Document 17/2017. IEEE, 2017.
- LÓPEZ, P. Tecnologías Disruptivas. Mirando el futuro Tecnológico. (Disruptive Technologies. Looking at the technological future.) Boletín de Observación Tecnológica en Defensa no. 25, 2009.

- POSEN, B. R. The Sources of Military Doctrine: France, Britain, and Germany between the World Wars. Ithaca: Cornell University Press 1986.
- PRICKETT, S. Developing Operating Leaders for the 21st Century. Joint Military Operations. Newport (USA): Department Naval War College 2003.
- RICHARDS Ch. A Swift, Elusive Sword: What If Sun Tzu and John Boyd Did a National Defense Review. Center for Defense Information, 2001.
- RIOLA, J. M. Tecnologías disruptivas y sus efectos sobre la seguridad. (Disruptive technologies and their effects on security.) Annual Research Plan Working Document 12/2015. CESEDEN, 2015.
- UN SECRETARY-GENERAL. A more secure world: our shared responsibility. Report of the High-level Panel on Threats, Challenges and Change, 2004.
- SERRA, J. 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, 2013.
- SIMON, L. The Third US Offset Strategy and Europe's Anti-Access Challenge. The Journal of Strategic Studies. Institute for European Studies. Vrije Universiteit Brussels, 2016.
- TOFFLER, A. & H. War and Anti-war. Survival at the Dawn of the 21st Century. Little, Brown and Company, 1993.
- VILLENA, C. 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, 2014.
- WORLD ECONOMIC FORUM. The Global Risks Report 2018. 13th edition, 2018.

GLOSSARY OF TERMS

A2/AD	Anti-Access/Area Denial
AM	Additive Manufacturing
C2	Command and Control
CBNE	Chemical, Biological, Nuclear, Explosive
CBRN	Chemical, Biological, Radiological, Nuclear
CCDC	Concepts Development Joint Centre
CESEDEN	National Defence Advanced Studies Centre
CG	Civil Guard
CIS	Communications and Information Systems
CRO	Crisis Response Operations
CTNSP	Center for Technology and National Security Policy
DOTMLPF-I	Doctrine, Organisation, Training, Materiel, Leadership and education, Personnel, Facilities - Interoperability
DTIB	Defence Technological and Industrial Base
EDA	European Defence Agency
EMP	Electromagnetic Pulse
EU	European Union
GO	Government Organizations
GPS	Global Positioning System
HMI	Human-Machine Interface
HPM	High Power Microwave Weapons
IADS	Integrated Air Defence System
ICT	Information and Communication Technologies

IED	Improvised Explosive Device
IEEE	Spanish Institute of Strategic Studies
ISDO	International Security and Defence Organizations
ISR	Intelligence, Surveillance and Reconnaissance
JISR	Joint Intelligence, Surveillance and Reconnaissance
LAR	Lethal Autonomous Robotics
LEA	Law Enforcement Agencies
NATO	North Atlantic Treaty Organization
NCO	Network Centric Operations
NDU	National Defence University
NEO	Non-combatant Evacuation Operation
NGO	Non-Governmental Organizations
NLW	Non-Lethal Weapons
NSS	National Security Strategy
OE	Operating Environment
OS	Operational Scenarios
OSCE	Organisation for Security and Cooperation in Europe
PESCO	Permanent Structured Cooperation
RFW	Radio Frequency Weapons
RPAS	Remotely Piloted Aircraft System
SAF	Spanish Armed Forces
SAR	Search and Rescue
SBSS	Space-Based Surveillance Systems
UAV	Unmanned Aircraft Vehicle
UCAV	Unmanned Combat Aircraft
UGV	Unmanned Ground Vehicle
UN	United Nations
US	United States
USV	Unmanned Surface Vessel or Vehicle
UUV	Unmanned Underwater Vehicle
UV	Unmanned Vehicle
VUCA	Volatility, Uncertainty, Complexity and Ambiguity
WMD	Weapons of Mass Destruction

PUBLICACIONES
Pd
DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL