Instituto Español de Estudios Estratégicos

02/2025 01/07/2025

Miguel Ángel Pérez Franco

Smart Deterrence to prevent 21st-century conflicts

Smart Deterrence to prevent 21st-century conflicts

Abstract:

The international situation has undergone significant changes, marked by ongoing competition between states that are redefining global dynamics. The way we wage war has also evolved, evidencing a return to high-intensity conventional conflicts. Combined with the proliferation of hybrid wars, the emergence of new domains of competition, and enormous technological development, this will forever change the practice of warfare. In this context, traditional deterrence remains a fundamental tool for preventing conflict, but it is insufficient in the face of this new operating environment and these new threats. Therefore, there is an urgent need to develop a new form of deterrence that integrates new domains of competition and innovative technological advances to address the new operating environment. Smart deterrence is the great challenge: designing innovative mechanisms that allow us to anticipate and avoid conflicts, ensuring international stability in an increasingly interconnected and volatile world.

Keywords:

Smart deterrence, operative environment, threat, conflict

Cómo citar este documento:

PÉREZ FRANCO, Miguel Angel. *Smart Deterrence to prevent 21st-century conflicts.* Documento Marco IEEE 02/2025. enlace web IEEE y/o enlace bie[3] (consultado día/mes/año)

Deterrence is the art of producing,
in the mind of the enemy, the fear to attack.

Dr. Strangelove.
How I learned to stop worrying and love the bomb
Stanley Kubrick, 1964

Introduction

The world has changed in recent decades. After a brief unipolar period, China has emerged to challenge the United States for global leadership. The resurgence of Russia, the emergence of aspiring regional powers, and the renewed role of supranational organizations are characteristics of our new and changing world. These changes have always occurred throughout our history, but the difference is that they are now happening at breakneck speed, driven by the exponential advancement of new technologies. As a result, warfare and its modus operandi have also evolved.

The renewed nature of warfare has many facets and dimensions. Today's warfare is characterized by a strong and enhanced conventional nature, but also by many other nuances. Added to this conventional temperament are the characteristics of fourth-generation warfare defined by Frank Hoffman[1], where images, communication, and the use of social media are used indiscriminately in the battle of narratives. On the other hand, the profuse use of hybrid warfare, the presence of militias, paramilitary groups, and non-state actors, with their asymmetrical nature, join this dizzying combination[2].

In this sense, it could be argued that all these characteristics are based on the solid foundation of an operating environment known as VUCA[3], where the establishment of the grey zone is seen as the path to preparing for war[4]. In light of these considerations,

---

[1] HOFFMAN, Frank. Conflict in the 21st Century: The rise of hybrid wars. Potomac Institute for policy studies, 2007, Virginia.

[2] BAQUÉS, Josep. De la guerra de Ucrania al debate sobre la naturaleza de la guerra. Global Strategy Report. 2023.

[3] Volatility, uncertainty, complexity, and ambiguity. As established in our joint operational documentation, there are other evolved models of VUCA, such as BANI (Brittle, Anxious, Nonlinear, Incomprehensible) or VI2RCA2S (volatility, uncertainty, immediacy, noise, complexity, ambiguity, acceleration, and simultaneity), but in this text we will stick with the VUCA model to keep things consistent with other national strategy documents and our current joint doctrine. CENTRO CONJUNTO DE DESARROLLOS DE CONCEPTOS (EMAD). Entorno Operativo 2035. Estado Mayor de la Defensa. Madrid, 2022.

[4] Ibídem.

it is imperative to anticipate trends and developments that are likely to play a significant role in future conflicts. This enables us to identify the tools necessary to either prevent such conflicts or, at the very least, ensure that we are equipped to deal with them effectively. However, what tools could be useful in preventing new conflicts?

The 2021 National Security Strategy indicates a potential solution, emphasising the necessity of a credible and effective deterrent capability to prevent any form of aggression, ranging from hybrid strategies to conventional conflicts[5]. However, the credibility of the current deterrence strategies must be assessed. In light of the prevailing uncertainty, it is essential to assess the efficacy of them. The following solutions are provided for each of the aforementioned questions, thus answering the established question: Smart deterrence is key to preventing conflict. This is our challenge...

Conceptual Approach

According to our joint doctrine, the military defense of Spain continues to be the “raison d'être” of our Armed Forces, which emerge as an essential tool for deterrence[6]. However, what is deterrence?

According to André Beaufre, deterrence is defined as the set of actions that seek to prevent an adversary power from deciding to use its weapons to change or alter the status quo. The French general understood deterrence to be an essential tool for avoiding conflict through the use of the threat of force. However, Beaufre specified that this set of actions or deterrence was diametrically opposed to those of war, since its ultimate goal was to prevent or avoid the decision to use weapons. As previously stated, this is the psychological result of the threat[7]. Therefore, deterrence implies a defensive stance with a strong determination to prevent aggression. Implementing a deterrence strategy involves clearly and directly communicating to potential opponents the vital interests that are at stake and it worth it to fight for them[8].

[5] GOBIERNO DE ESPAÑA. Estrategia de Seguridad Nacional. Real Decreto 1150/2021. Madrid, 2021.

[6] CONJUNTO DE DESARROLLOS DE CONCEPTOS (EMAD). Doctrina para el Empleo de las FAS – PDC-01 (B). Doctrina. Estado Mayor de la Defensa. Madrid, 2024.

[7] BEAUFRE, André. Disuasión y Estrategia. Editorial Pleamar. Buenos Aires, 1978.

[8] FREEDMAN, Lawrence. Beyond Deterrence and its limits in the Russo-Ukrainian War. Polity. Beyond Deterrence - by Lawrence Freedman - Comment is Freed 2024.

Professor Javier Jordán's analysis states that deterrence is defined as a process of influence, structured through a series of meticulously designed actions, whose objective is to prevent a certain actor from carrying out an armed action that would otherwise be carried out. Jordán asserts that this process of influence constitutes a component of a defensive strategy, the objective of which is to circumvent the potential for conflict. This strategy is focused on calculating the costs and benefits for our potential adversary[9]. This definition aligns with the formulation of American doctor and scholar Colin Spencer Gray, who adds that the deterred party would choose not to take military action because they would consider the costs of implementation to be too high. For both sides, it is of the utmost importance to influence the perception of the potential adversary[10].

In short, deterrence consists of preventing a potential adversary from considering the use of force as an acceptable option for imposing their will[11]. It could therefore be inferred that deterrence is a preventive strategy of influence, the purpose of which is to avoid conflict. And, how is this achieved? By attacking the perception of the potential adversary, or more specifically, by influencing their cost/benefit analysis when they are assessing whether or not to initiate armed action[12]. In short, by influencing their decision-making process. However, in order to be able to initiate this mechanism, it is necessary to answer a question of utmost importance: what influences the adversary's decision-making process? Finding the answer to this intriguing question is essential, because if we know in advance what influences this process, the necessary mechanism of influence and deterrence to alter it can be applied.

Deterrence or how to influence the decision-maker

As we have seen, deterrence aims to influence the adversary's decision-making through a process of influence: attacking their perception is key to any deterrence strategy. Its objective is to prevent conflict by influencing the adversary's decision-making and the

[9] JORDÁN, Javier. Qué es la disuasión y cómo funciona», Estrategia podcast 40, Global Strategy: https://global-strategy.org/que-es-la-disuasion-y-como-funciona-estrategia-podcast-40/, 2023.

[10] GRAY, Colin. The Definitions and Assumptions of Deterrence: Questions of Theory and Practice. Journal of Strategic Studies 13, nº 4, 1990.

[11] THAUBY, Fernando. Disuasión y Defensa. Revista de Marina nº 2. Valparaiso, 1999.

[12] JORDÁN, Javier. Disuasión: fundamento de la estrategia defensiva. Global Strategy. ¿Qué es la disuasión? | Global Strategy, 2022.

cost/benefit assessment of their armed action[13]. Therefore, it seems clear that the target of deterrence is ultimately the decision-maker, the person who has the authority to decide, and, of course, their closest team[14].

In this regard, the decision-maker and their team bear responsibility for developing the decision-making process to determine whether armed action will ultimately be initiated. This assessment typically involves a process of reasoning based on assumptions of values, beliefs, culture, and objective data. The aim is to understand whether a given action will result in total victory, a Pyrrhic victory, a zero-sum cost, or even defeat. Glenn Herald Sdyner, a professor of political science from the United States, has stated that, from a military perspective, the cost/benefit ratio of armed actions is calculated using a combination of four factors[15]:

- The value of the military objective to be achieved.
- The political, human, economic, and material cost of achieving it.
- The probability of suffering a response from the attacked nation (the deterrent).
- The probability of achieving the objective with each response received.

The value of the objective and its political cost are intrinsic to the nature of the decision-maker (the aggressor) and will be based on their values, beliefs, and culture. At the same time, the human, economic, and material costs, as well as the probability of suffering a response and the probability of achieving the objective with each response received, are factors that, although they must be assessed by the aggressor, can be modulated by the deterrent (the one receiving the aggression)[16]. In short, the deterrent, who will receive the aggression, could influence these last three aspects, and it is here that the two models or strategies of deterrence emerge: punishment and denial.

[13] FREEDMAN, Lawrence. Deterrence. Polity. London, 2004.

[14] Ibídem.

[15] SNYDER, Glenn. Deterrence and power. Journal of Conflict Resolution. Volume 4, Issue 2. 1960.

[16] GRAY, Colin. Gaining compliance: the theory of deterrence and its modern application. Comparative Strategy, 29, Issue 3. 2010.

Deterrence strategies: punishment and denial

Deterrence by punishment is based on threatening or reacting against high-value targets belonging to the aggressor, even after an initial offensive strike has been launched. For this strategy to be effective, the punishment must be credible and unacceptable to the potential adversary (industries, facilities, and military forces, or directly to enemy leaders and decision-makers). Its ultimate expression is nuclear deterrence. Its objective is therefore to maximize and raise the aggressor's costs to unacceptable levels. Therefore, the following military capabilities are necessary to achieve this: high strategic mobility and a powerful offensive capability[17].

Deterrence by denial is based on the resilience of the victim (the deterrent), or, in other words, on their defensive capability, making the aggressor see that if they act, they will either fail to achieve their objective or it will be very costly to achieve it. Its objective is to minimize the aggressor's gains; or, in other words, to exacerbate their fear of failure. Therefore, in addition to space and time, which are basic conditions for defense, the following military capabilities are necessary to achieve this: accurate and timely intelligence, a powerful defensive capability, and a certain response/offensive capability to counterattack[18].

Both strategies are complementary, and in both cases, the deterrent, defender of the status quo, will always be at a disadvantage compared to the aggressor. So how could we combine both strategies to maximize their effects?

First, the punishment strategy involves knowledge and certainty of the purpose and actual capabilities of the nation exercising deterrence. That is, why it would be willing to go to war and what means it would use if it did. This fact would therefore generate a certain amount of respect from a potential aggressor. On the other hand, the denial model implies precisely the opposite: ignorance and uncertainty about the intentions and capabilities of the deterrent, a fact that instills fear of the unknown in the potential aggressor.

Both strategies can be combined with certain guarantees that mitigate the uncertainty of the potential aggressor, assuring them that they have nothing to lose if they respect

[17] DOWNS, George. The Limits of Deterrence Theory. Deterrence in the Middle East, JCSS Study No. 22, Westview Press, Colorado, 1993.

[18] Ibídem.

them[19]. As Professor Javier Jordán states, these guarantees are indispensable in any combination of both deterrence strategies, providing certainty and minimizing misinterpretations or miscommunications between both parties. These guarantee or safeguard measures could include political, diplomatic, and economic measures; in short, measures aimed at fostering mutual trust[20].

The optimal combination of these strategies, when complemented by appropriate safeguards, could be pivotal in averting potential conflict. However, deterrence is not an exact science; the decision-making process of potential aggressors is always influenced by their own norms and values, as well as by their political, religious, ideological, psychological, and cultural characteristics[21]. Therefore, it is essential that we analyse these subjective factors if the deterrence strategy is to be effective. In this regard, its own credibility will be a fundamental tool. However, it is not always easy to ascertain whether the deterrence is credible.

The importance of credibility and the effective communication of deterrence.

The credibility of a deterrence strategy is crucial and is closely linked to the potential aggressor's perception of the deterrent's commitment to using force. In this sense, to be truly effective, the aggressor must be convinced, beyond any reasonable doubt that the deterrent will carry out its threat of response if the aggression occurs. Similarly, this credibility must be taken to its ultimate consequences, with the deterrent able to maintain it at all costs, even when the costs of confrontation begin to rise[22]. In this regard, the credibility would be severely compromised if the political will were too hesitant to utilise military capabilities for the purpose of deterrence. Furthermore, if we consider the fact that the adversary makes full use of the deterrer’s laws, customs, and traditions, the deterrence would be greatly weakened[23].

[19] KNOPF, Jeffrey. Varieties of assurance. Journal of Strategic Studies, nº 35, Issue 3. 2012.

[20] JORDAN, J. Disuasión: fundamento de la estrategia defensiva. Op. Cit.

[21] PAYNE, Keith. 2011. Understanding deterrence. *Comparative Strategy*, nº 30, Issue 5. 2011.

[22] STEIN, Janice. Military deception, strategic surprise and conventional deterrence: A political analysis of Egypt and Israel. Journal of Strategic Studies, nº 5, Issue 1. 1982.

[23] Estas actividades se denominan Lawfare. CENTRO CONJUNTO DE DESARROLLO DE CONCEPTOS. Entorno Operativo 2035. Op. Cit.

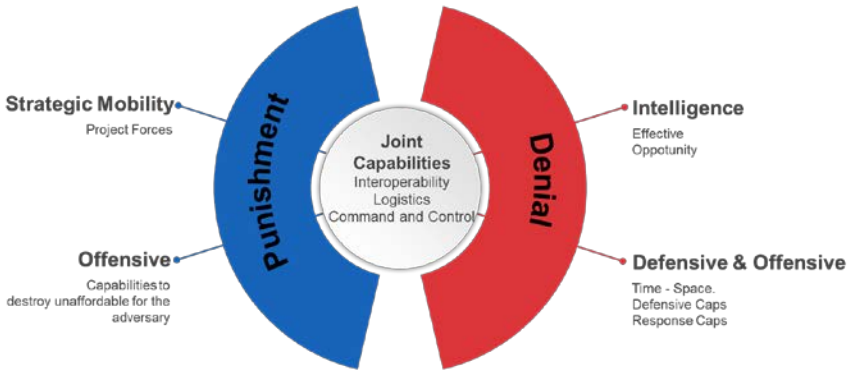
Therefore, for a deterrence strategy to be effective and credible, three factors must be in place: political determination; capacity, primarily military, economic, and diplomatic; and an effective communication strategy.

Political determination is based on the use of deterrent capabilities. In this regard, the political decision-maker responsible for deterrence must calculate the cost and benefit of defending vital interests and determine the value of fighting for them[24]. In this regard, it will be crucial for the political level to establish its red lines and the interests it will defend at all costs.

With regard to the military aspect, the effectiveness of the deterrent capability is contingent upon the sufficient potency of its coercive element to halt the potential aggressor in their tracks. Therefore, depending on the weight of the deterrence strategy to be adopted (punishment or denial), certain capabilities must be made available.

In this regard, it will be necessary to take into account not only the number and quantity of military forces and resources, but also their ability to operate effectively in different domains, their logistical support, their command and control capabilities, their interoperability, their supply and replenishment capabilities, etc. It is also vital to take into account the human factor, which includes superior strategy and tactics, the training and morale of the forces, and individual capabilities such as having leaders who are particularly gifted at making the right decisions in accordance with a higher purpose (Mission-Oriented Command).

Capabilities of Deterrence Strategies



Source: Author's Own Work

[24] JORDAN, J. Disuasión: fundamento de la estrategia defensiva. Op. Cit.

Finally, it will be necessary to implement a timely and effective communication strategy. This communication should be based on: 1) the ability to communicate to the aggressor, in no uncertain terms, what action is considered unacceptable (red lines and vital interests that will be defended at all costs) and what response will be provided, if any; 2) the commitment to carry out the threat; and 3) the ability to carry it out[25].

Likewise, an important consideration when communicating the deterrent threat is to ensure that it is not perceived as aggressive intent. In this regard, there are numerous examples of how to communicate the ability to carry out a threat: military exercises, demonstrations of force, or participation in military missions in peacetime. In short, by developing preparedness and training the forces, as well as effectively communicating this to the target audience (the potential adversary).

Deterrence to prevent 21st-century conflict, but what kind of conflict?

As has been seen, if a credible and effective deterrent effect is to be achieved, it is necessary not only to integrate both deterrence strategies, but also to coordinate them with other political, economic, and cultural policies, etc., capable of reaching the values and perceptions of the potential opponent. However, this approach to deterrence has not always been developed in accordance with this practice.

During the Cold War, deterrence was based on the defensive strategies of the two great nuclear powers, where the nuclear orientation prevailed, which is fundamentally based on the strategy of punishment. However, the complexity of using nuclear weapons, the dilemma of mutually assured destruction, and the moral aspects of their use provided a certain rationality in the control of nuclear arsenals and the definition of other strategic options to achieve the political objectives set[26]. This fact, coupled with major advances in conventional capabilities, specifically in intelligence gathering capabilities, as well as precision munitions and delivery systems, led to the emergence of what is known as north American conventional dominance[27].

[25] KAUFMANN, William. The Requirements of deterrence. Center for International Studies. Princeton University. 1954.

[26] COLOM, Guillem. Teoría y práctica de la disuasión en el mundo globalizado. Revista Ejército, nº 954. Madrid, octubre 2020.

[27] ALLAN, Charles. Extended Conventional Deterrence: In from the Cold and Out of the Nuclear Fire? The Washington Quarterly, nº 17, Issue 3. 1994.

It should also be noted that conventional weapons have a lesser deterrent effect, as they are easier to use. This factor, combined with the fact that, from a political point of view, their use will always be more acceptable, makes them a more credible threat. This means that conventional weapons have greater deterrent power.

In this sense, these conventional capabilities, and mainly long-range precision weapons, have two major advantages. First, they limit collateral damage and the resulting moral dilemmas associated with the loss of civilian lives. Second, their use reduces the likelihood of friendly casualties. Therefore, conventional deterrence has emerged as a consequence of the evolution of nuclear deterrence and the need to find alternatives to achieve similar effects in order to avoid conflict. However, in recent decades, the emergence of non-state actors, such as Hezbollah or Da'esh, often motivated by religious reasons; the emergence of asymmetric conflict and hybrid warfare; and the proliferation of gray areas seem to render the concept of deterrence unviable. Could a deterrence strategy work effectively in this new environment? To answer this thought-provoking question, we must first wonder: What does this new operational environment look like? What are its characteristics? By analyzing its nature, we may be able to identify the vulnerabilities of the classic deterrence strategies, with the aim of complementing it to make it truly effective and credible.

The new operating environment

The operating environment is understood to be the set of fixed and variable conditions that affect decision-making and the use of military capabilities in relation to a given operation[28]. In this sense, conducting a rigorous analysis of these conditions will provide decision-makers with comprehensive and detailed knowledge of the situation, facilitating appropriate decision-making and an understanding of its potential effects and consequences[29].

In this regard, following the bipolarity of the post-war period, the unipolar world led by the United States seems to be coming to an end. The rise of China as a new economic and military power, together with Russia's desire to remain a relevant international player,

[28] CENTRO CONJUNTO DE DESARROLLOS DE CONCEPTOS (EMAD). PDC-00: Glosario de Terminología de uso conjunto. Estado Mayor de la Defensa. Madrid, 2020.

[29] CENTRO CONJUNTO DE DESARROLLO DE CONCEPTOS (EMAD). Entorno Operativo 2035. Op. Cit.

have led to a transition to a scenario of continuous competition. We are therefore facing a multipolar world tending towards the formation of two competing blocs. Likewise, the emergence of non-state actors, outside the scope of international law, has filled the existing power vacuums. As a result, many of today's conflicts feature terrorist groups, tribal militias, or private paramilitary security groups as the main protagonists. However, these actors are at a clear technological and military disadvantage compared to sovereign states. In this sense, and to mitigate this disadvantage, their operational and tactical praxis focuses on the use of asymmetric mechanisms of confrontation in order to compensate for and reduce their technological gap. Likewise, in this competitive environment, the clash of interests between state and non-state actors has led to an increase in actions framed in the gray zone and the use of hybrid strategies[30]. These forms of action, supported by global interconnection, international law, and the use of emerging technologies, will be those of conflict in the coming decades. Likewise, cyberspace, outer space, and the cognitive realm, together with the use of innovative technologies such as robotics, artificial intelligence, 5G, and massive data management, are already changing the way war is waged and hypothetical conflicts are addressed[31]. The combination of all these conditions and factors defines an operational environment characterized by volatility, uncertainty, complexity, and ambiguity. In this sense, these characteristics are defined by the following factors[32]:

- Volatility, due to the speed and rapid evolution of scenarios.
- Uncertainty, as the effects of actions—particularly in the cognitive domain—are increasingly unpredictable.
- Complexity, stemming from the multitude of factors involved (domains, actors, threats, cultural variables, etc.), and the cross-domain impact of their interactions.
- Ambiguity, due to the difficulty in attributing hostile actions, especially in the cyber and cognitive domains.

[30] Ibídem.

[31] Ibídem.

[32] CENTRO CONJUNTO DE DESARROLLOS DE CONCEPTOS (EMAD). Evolución de la Fuerza Conjunta hacia las Operaciones Multidominio. Concepto Exploratorio. Estado Mayor de la Defensa. Madrid, 2023.

This evolving environment challenges the traditional concept of deterrence, which can no longer be viewed as a universal, mechanical, or purely rational construct. Indeed, deterrence strategies reveal critical vulnerabilities when confronted with this dynamic and multifaceted reality. However, what are these specific vulnerabilities and limitations? By identifying them, we could tailor the deterrence strategy to align with both the operational environment and the nature of potential adversaries.

The Operational Environment: A Challenge to Contemporary Deterrence

The current operational environment poses a significant challenge to existing deterrence strategies. Numerous empirical studies yield conflicting conclusions regarding the effectiveness of both punishment-based and denial-based deterrence approaches in a VUCA (Volatile, Uncertain, Complex, and Ambiguous) environment.

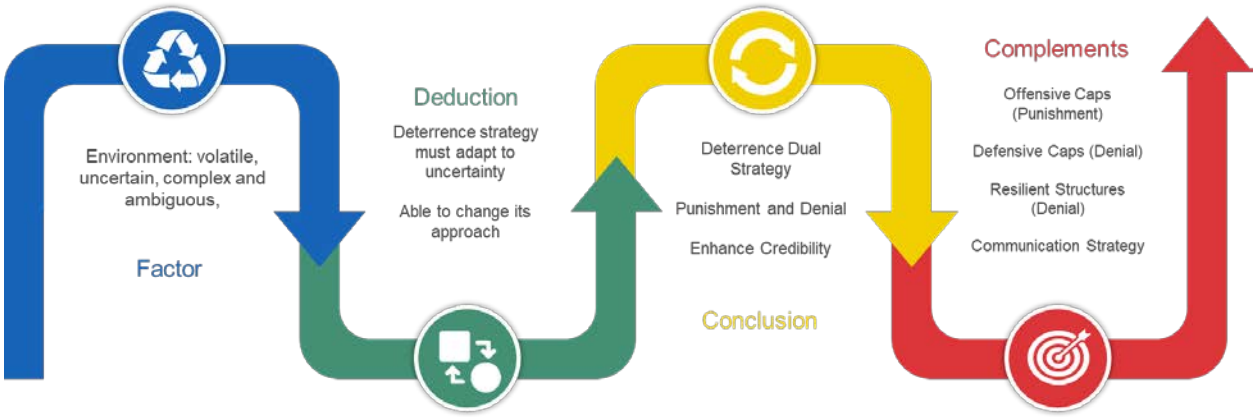
An analysis of the aforementioned characteristics reveals that force flexibility and versatility are critical tools for adapting to the evolving operational environment and its potential crises and escalation phases. A force structure and organization capable of establishing deterrence from the earliest indicators of crisis emerges as the optimal solution. Such a force must be well-balanced, with the capacity to conduct pre-emptive strikes (deterrence by punishment) and to establish a robust defense posture (deterrence by denial) across all operational domains[33].

In terms of force structure, it is feasible to develop an organization that is optimized for significant deterrent effect through a punishment strategy (with extensive offensive capabilities) while simultaneously maintaining strong defensive capacities (enabling a denial strategy). However, the inverse is not possible: a force based solely on defense cannot credibly support a strategy of punishment. Therefore, establishing a force structure with a strong offensive component, complemented by dual-capable (offensive-defensive) systems, is paramount to effectively supporting a denial-based strategy[34].

[33] SNYDER, Glenn. Deterrence and defense. Vol. 2168. Princeton Legacy Library. 1961.

[34] KLIEMAN, Aharon y LEVITE, Ariel. Deterrence in the Middle East: Where Theory and Practice Converge. JCSS Study, nº 22. Softcover. Tel Aviv. 1991.

Deductive Analysis on Operational Environment Characteristics



Source: Author's Own Work

To further reinforce a denial strategy, the force's structure and organization must also be highly resilient. Military deterrence must be grounded in balanced and resilient forces capable of operating across the full spectrum of conflict. In this regard, enhancing cyber defense and strategic communication capabilities is essential.

On the other hand, deterrence by denial must not rely solely on the sum of defensive and offensive capabilities. The adversary's perception is a decisive factor. Thus, credibility becomes central—and with it, the importance of a strategic communication posture[35]. In this operational context, any potential aggressor must weigh two critical considerations prior to initiating an attack: 1) the probability of success of their military action; and 2) the cost of inaction[36]. Therefore, if we—as defenders—successfully communicate both our defensive capacity and our resolve to respond to aggression in order to prevent it, we will establish an effective deterrence by denial strategy.

Asymmetric Conflict: The Battle of Narratives and Resilience

In asymmetric environments, traditional deterrence—whether based on punishment or denial—is often ineffective. This is particularly true when dealing with non-state actors, terrorist groups, and militias, which typically do not adhere to rational patterns of behavior.

[35] SNYDER, G. Deterrence and Defense. Op. Cit.

[36] LIEBERMAN, Ellie. The Rational Deterrence Theory Debate: Is the Dependent Variable Elusive? Security Studies, Paper 3, Issue 3. 1993.

Instead, their strength often lies in deeply rooted ideological or religious narratives, which are inherently resistant to conventional deterrence mechanisms.

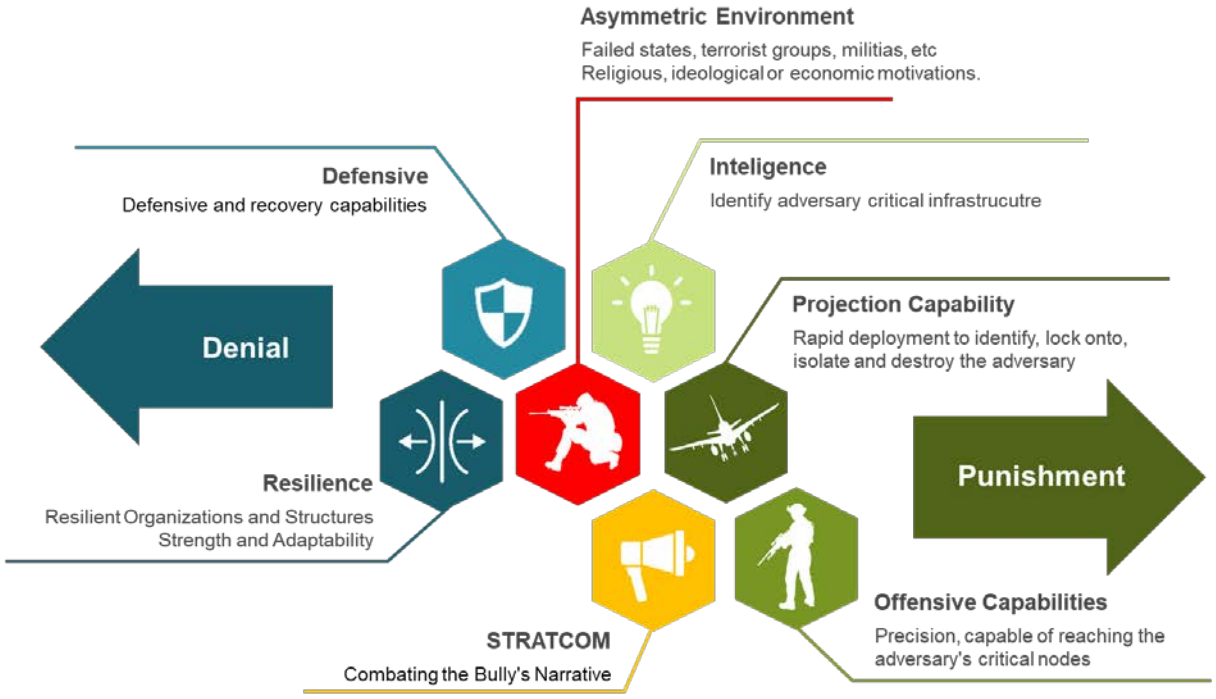
In this context, deterrence by punishment alone is generally insufficient, and must therefore be reinforced with denial measures (defensive actions) and a robust strategic communication plan. From the punishment perspective, precision offensive capabilities are required—capable of targeting operational nodes while minimizing collateral damage. This necessitates on-the-ground intelligence to gather actionable information about enemy forces and their support infrastructure. Additionally, the capacity to rapidly project forces and conduct decisive operations against both the enemy and its support structures is vital. The purpose of these punitive actions is to identify, fix, isolate, and destroy enemy assets and command-and-control, financial, and logistical infrastructures—thereby depriving the adversary of the initiative[37].

On the defensive side, beyond the necessary protective and recovery measures against asymmetric attacks, deterrence strategies must include resilience-building measures to enhance the robustness of all the organizations and societal systems. These resilience efforts must extend across the entire society under protection, focusing particularly on cybersecurity, energy security and electoral security[38]. Simultaneously, the strategic communication effort must aim to directly counter the adversary's narrative, which often constitutes its center of gravity.

[37] REYNOLDS, John. Deterring and Responding to Asymmetrical Threats. United States Army Command and General Staff College. Fort Leavenworth, Kansas. 2003.

[38] BEAULIEU, Brittany y SALVO, David. NATO and Asymmetric Threats: A Blueprint for Defense and Deterrence. Policy Brief. Number 31. Alliance for Securing Democracy. July, 2018.

Confrontation: Deterrence vs. Asymmetric Environment



Source: Author's Own Work

Furthermore, many of these actors will employ lawfare—the exploitation of legal systems, norms, and customs of democratic states to undermine them from within. To counter this, a successful deterrence strategy requires the full backing of all state instruments of power, with a critical role played by political, diplomatic, and especially economic measures aimed at isolating and exhausting the aggressor[39].

Operating in the Grey Zone: Tailored Deterrence and Strategic Communication

When dealing with hybrid threats and grey zone conflict, conventional deterrence strategies—grounded in classical theory—are often poorly suited. To address this, it is essential to develop a tailored deterrence strategy, specifically designed to counter hybrid strategies and prevent escalation into open conflict. According to national conceptual frameworks, such a strategy should encompass, at least, four core components: 1) Prevention; 2) Detection and communication of the threat to the adversary; 3) Deterrence proper; and 4) Response articulation, if necessary.

[39] CENTRO CONJUNTO DE DESARROLLOS DE CONCEPTOS (EMAD). Entorno Operativo 2035. Op. Cit.

The inherent ambiguity of the grey zone—its blurred attribution, and the potential for both escalation and de-escalation—makes prevention and detection particularly difficult[40]. Therefore, early detection of hybrid strategies demands specialized efforts, including distinct indicators beyond those used in conventional military deterrence. This necessitates a multidimensional approach incorporating diplomatic, political, economic, legal, social, and informational dimensions, among others.

Moreover, ambiguity complicates information gathering, assessment, and communication, which undermines the deterring party's confidence in understanding the true intent and motivation of the aggressor[41]. So, what constitutes the most effective deterrence strategy in the grey zone? The answer is multifaceted: the optimal approach involves a dual-track deterrence strategy, reinforced by complementary instruments of national power.

On the one hand, denial-based deterrence is often less effective in the grey zone than punishment-based strategies (which rely on threats of retaliation). This is because adversaries will likely test and exploit vulnerabilities in our defensive posture through trial-and-error tactics. Therefore, denial strategies must include proactive efforts to publicly expose and condemn violations of international norms by the aggressor at the earliest possible stage.

On the other hand, a punishment-based deterrence strategy must rest on a credible threat of retaliation[42], backed by the political will to follow through. However, since the primary objective of deterrence is conflict prevention, mechanisms must be in place to avoid uncontrolled escalation. In this regard, and according to Professor Javier Jordán, military capabilities must be used in a way that maintains escalation below the threshold of open conflict in order to remain both credible and effective. Additionally, a tailored communication strategy is essential—one that focuses on the adversary's value system and normative structure, with the goal of identifying levers that may compel a shift in behavior or maintenance of the status quo.

[40] The aggressor in the gray zone will always try to conceal his responsibility by resorting to operations in virtual environments, such as cyberspace or the cognitive realm, by using third parties, or by outright denying his responsibility or involvement. In doing so, he seeks to avoid the victim's response, delegitimizing his response.

[41] ALLAN, C. Op. Cit.

[42] FREEDMAN, L. Op. Cit.

Finally, the credibility of the deterrence strategy must be bolstered through the application of confidence-building and guarantee measures, carefully aligned with broader political, diplomatic, and economic efforts. These actions aim to influence the adversary's cost-benefit calculus, deterring them from engaging in hostile activities within the grey zone[43].

Multidomain Operations: The Imperative of Technological Superiority

Multidomain operations as those conducted in a highly complex operational environment encompassing all domains of warfare—both physical and non-physical—characterized by strong interdependence and interaction across them. As such, these operations demand robust interoperability and connectivity, enabling distributed control of assets to optimize the concentration and integration of all capabilities at the right time and place, thereby generating effects in and from any operational domain[44].

The emergence and evolution of multidomain operations signify a paradigm shift—one that redefines the battlespace as an integrated whole, where success hinges on precise knowledge of one's own capabilities, the effects they can generate, and the technological means to achieve them, especially through emerging and disruptive technologies[45]. Emerging technologies contrast with traditional ones by introducing a degree of decision-making uncertainty within organizations. Their development is focused on new employment options and potential. Disruptive technologies exceed user and organizational expectations, offering a qualitative leap and significant added value through continuous innovation, rapid evolution, and adaptability to changing environments. As such, these new deterrence strategies must actively incorporate these technologies[46].

Similar to operations in the grey zone, actions related to prevention, detection, deterrence, and response offer more reliability in physical domains than in non-physical ones, where attribution is more difficult. In these intangible spaces, the adversary may

[43] JORDÁN, Javier. La Disuasión en la Zona Gris: una exploración teórica. Revista Española de Ciencia Política. Granada, 2022.

[44] CENTRO CONJUNTO DE DESARROLLOS DE CONCEPTOS (EMAD). PDC-00: Glosario de Terminología de uso conjunto. Op. Cit.

[45] In addition to the land, maritime and air domains, it is imperative to add the non-physic domains, such as cyberspace, cognitive and space. CENTRO CONJUNTO DE DESARROLLOS DE CONCEPTOS (EMAD). Evolución de la Fuerza Conjunta hacia las Operaciones Multidominio. Concepto Exploratorio.

[46] EJÉRCITO DE TIERRA. Tecnologías Emergentes y Disruptivas en el ET. Documento Blanco.

choose when and where to strike. Therefore, an adequate deterrence posture must include clear early warning indicators in all domains—particularly cyberspace, the cognitive domain, and outer space, all of which are gaining increasing relevance.

Therefore, the effectiveness of this new deterrence strategy will depend on the following key considerations:

- The absence of a legal framework governing new domains such as cyberspace, the cognitive domain, and outer space;
- The ethical use of artificial intelligence and other autonomous systems in decision-making, especially where human intervention is excluded;
- The integration of emerging and disruptive technologies.

These factors, along with legal and ethical considerations regarding human-machine autonomy, demand that the deterrence strategy be restructured around three core lines of effort:

- Capability to operate in cyberspace, the cognitive domain, and outer space;
- Technological superiority across the full spectrum of operations.
- Development of ethical and legal frameworks for AI and autonomous systems.

All of this must be integrated with the broader instruments of national power—diplomatic, political, economic, and informational—to ensure the credibility and viability of deterrence in a multidomain context.

Smart deterrence: A new approach

As has become clear, the traditional deterrence model (punishment and denial) is increasingly inadequate in facing the challenges of the future operational environment and the rise of new conflict types. Consequently, our bet for this new deterrence strategy must evolve into a “smart deterrence” model—a unified and tailored dual approach that combines punishment and denial, with the capacity to strike the adversary’s center of gravity while simultaneously preventing the achievement of their objectives, through resilience and adaptability.

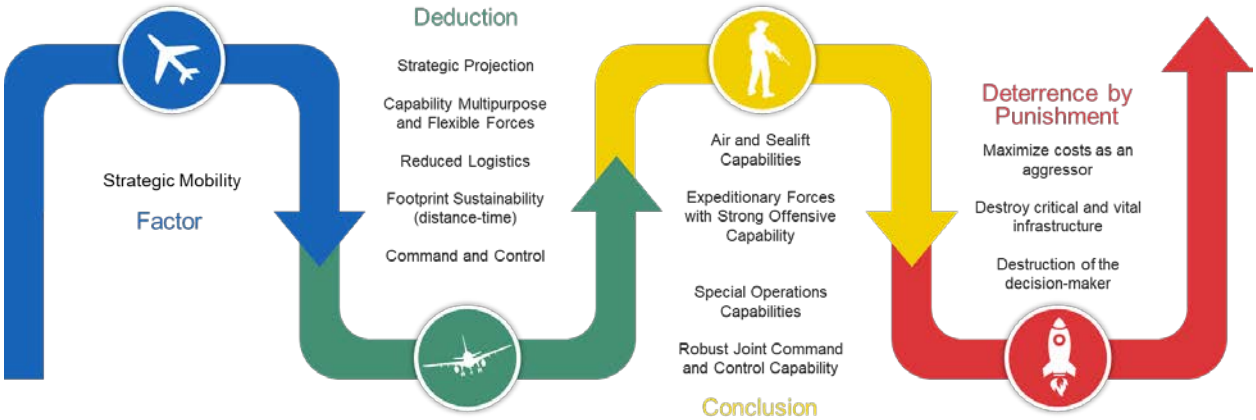
This smart approach must be built on a well-calibrated combination of deterrence by punishment (offensive) and deterrence by denial (defensive). Additionally, it must be supported by a credible communication strategy capable of clearly transmitting

to adversaries the red lines, as well as the coercive and guarantee-based levers that will be activated should the status quo be challenged. Looking forward, smart deterrence must encompass all capabilities needed to prevail in the multidomain operational environment—a setting defined by complexity, constant interaction, and mutual dependence between all domains, physical and non-physical alike. This tailored, dual, and future-ready approach—punishment (offensive) and denial (defensive)—must be grounded in both technological superiority and the resilience and readiness of the military forces. Based on these principles, we can now identify the military capabilities necessary to ensure that forces can execute a credible and effective deterrence strategy: a smart deterrence model.

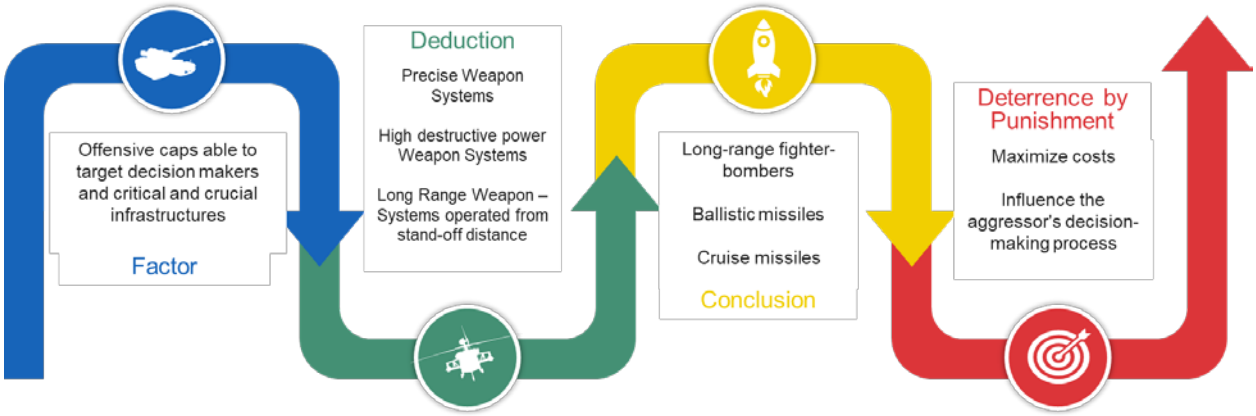
Deterrence by Punishment: Offensive Capabilities

Our analysis has clearly shown that the goal of deterrence by punishment is to escalate costs to unacceptable levels for the adversary. To this end, the following military capabilities are broadly required: High strategic mobility and robust offensive capabilities capable of striking decision-makers, critical infrastructures, and essential military assets—whose loss would impose a prohibitive cost on the adversary[47]. A deductive analysis of the previously outlined characteristics highlights the type of military capabilities that should support this offensive approach to punishment-based deterrence.

Deductive Analysis Table: Deterrence by Punishment – Offensive Dimension



[47] DOWNS, G. Op. Cit.



Source: Author's Own Work

In this context, effective strategic mobility is achieved through exceptional maritime and air capabilities capable of projecting versatile and flexible forces with high destructive capacity.

The speed of strategic projection will be conditioned by a reduced logistical footprint, a joint Command and Control system, and agile sustainment capable of maintaining and supporting projected forces over distance and time[48]. To this end, it will be essential to possess predictive sustainment capabilities, stock adjustment mechanisms, and standardized platforms, as well as energy generation and storage systems. All these elements aim to configure a more agile, simple, and efficient supply chain[49].

Likewise, a punitive strategy necessarily requires the acquiescence of forces that meet the following essential requirements: 1) capable of striking high-value targets; 2) capable of penetrating and breaking through the adversary's defensive system; and 3) sufficiently numerous to create the desired punitive effect (required level of destruction). In this sense, these characteristics are characteristic of air power, with its long-range fighter-bombers, ballistic missiles, and cruise missiles[50].

[48] METZ, Steven. Deterring Conflict Short of War. Strategic Review, Fall 1994.

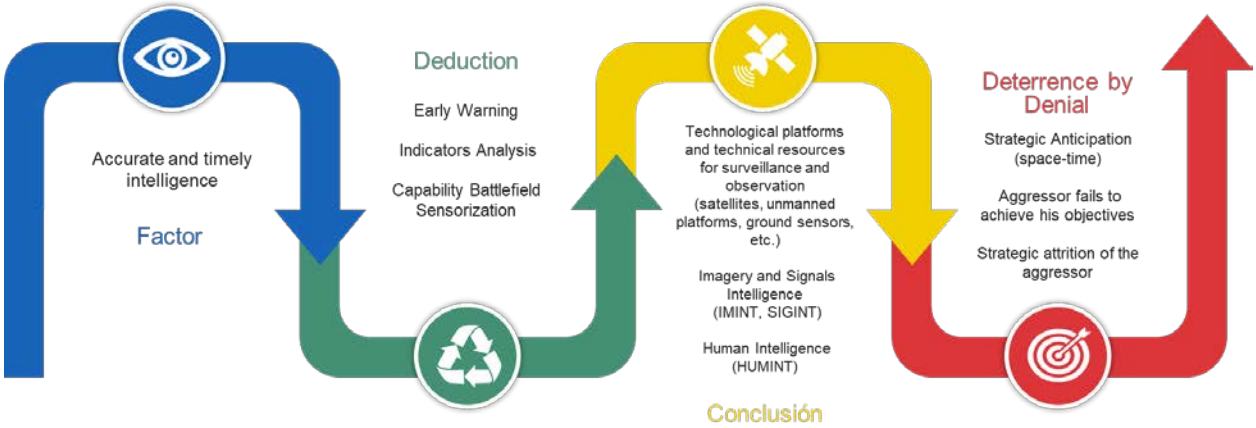
[49] CENTRO CONJUNTO DE DESARROLLOS DE CONCEPTOS (EMAD). Entorno Operativo 2035. Op. Cit.

[50] VALENZUELA, Joseph. Non-Nuclear Deterrence in US Strategic Policy: Incentives and Limitations. Austin, 1992.

Deterrence by Denial: Defensive Capabilities

Deterrence by denial is based on the capacity of the defender to resist, or in other words, on their defensive capability, making the aggressor understand that, should they act, they will either fail to achieve their objective or will find it exceedingly costly to do so. In this regard, in addition to space and time, which are the fundamental conditions of defense, the following capabilities become particularly important: the ability to obtain precise and timely intelligence; a robust defensive capacity; and a potent offensive/response capability[51]. If we delve deeper concerning the characteristics inherent to denial, military capabilities emerge that would support the defensive deterrence approach.

Deductive Analysis Framework: Deterrence by Denial – Defensive



Source: Author's Own Work

A timely and precise intelligence capability would require adequate technological capacity and the necessary technical resources to achieve the desired strategic anticipation. To this end, it would be necessary to enhance the analysis and surveillance capabilities, reinforcing information acquisition and processing. This deterrence strategy, combined with the complex operational environment, will demand superiority in information processing. Consequently, information acquisition and systematic observation (surveillance) or limited reconnaissance in space and time, using sensors and alert systems, along with the rapid processing and dissemination of the obtained information, will be decisive in conflict prevention.

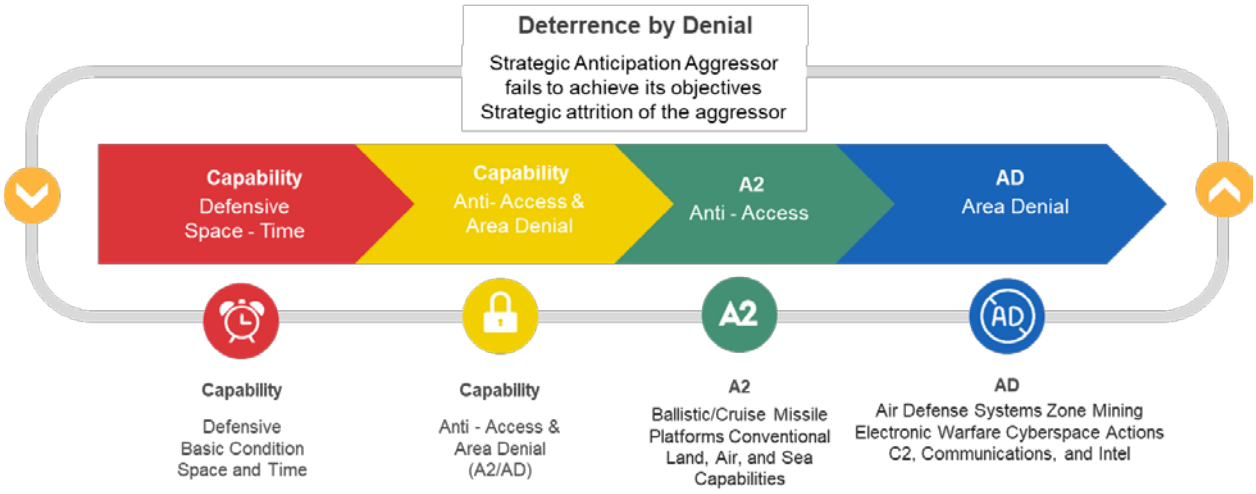
[51] DOWNS, G. Op. Cit.

The conclusion is clear: sensorize the battlefield into deterrer's favor. Therefore, enhancing joint Intelligence, Surveillance, and Reconnaissance (JISR) systems, both manned and unmanned, and processing systems that enable rapid and optimal intelligence generation should be an absolute priority for the denial strategy[52].

In addition to the aforementioned space and time, defensive capabilities would require anti-access and area denial (A2/AD) capabilities. The former pertains to actions taken at depth to prevent the mobility of adversary forces within the operational theater. In this regard, ballistic or cruise missile platforms, as well as robust conventional land, maritime, and air capabilities, would be necessary.

Area denial capabilities aim to limit the freedom of action of enemy forces within the operational theater. To achieve this, it would be essential to have land and maritime air defense systems, coastal mining/access denial to ports, electronic warfare capabilities, and the ability to conduct offensive/defensive actions in cyberspace, as well as operate a truly joint Command, Control, Communications, and Intelligence (C4I) system.

Deductive Analysis Framework: Deterrence by Denial – Defensive

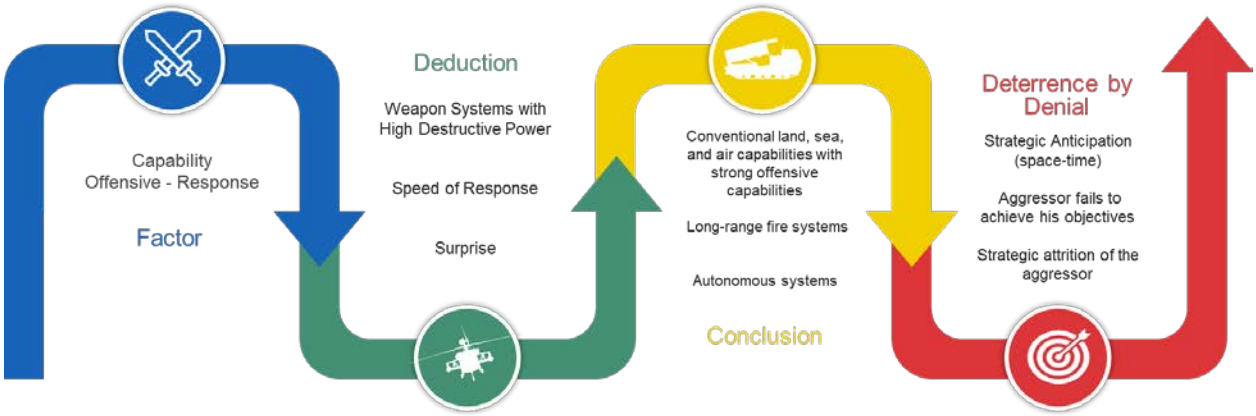


Source: Author's Own Work

A potent conventional land, maritime, and air capability would be necessary, in addition to the ability to respond in non-physical domains (cyberspace, cognitive, and outer space).

[52] Ibídem.

Deductive Analysis Framework: Deterrence by Denial – Defensive



Source: Author's Own Work

Strategic Communication: delivering on a threat

Credibility is the cornerstone of deterrence. To deter, one must be credible. Credibility is therefore essential for influencing the decision-making process of a potential aggressor. It is imperative to develop a timely and effective communication strategy, fully aligned with the political-level communication strategy. This communication should be based on: 1) The ability to unequivocally communicate to the aggressor what action is considered unacceptable and what response will be provided, if any; 2) the commitment to deliver the threat; and 3) the capability to deliver it[53]. While the first two aspects are the responsibility of the political level, a significant portion of the third—the capability to fulfill it—resides within the strictly military domain.

Effectively communicating the commitment to fulfill the threat means conveying that we possess the military capability to carry out the desired response in the event of aggression. Therefore, effectively communicating the punitive and the denial capabilities (both offensive and defensive) during training exercises would be of particular importance.

The purpose of these strategic communication actions would be to demonstrate that the deterrer is always prepared for any eventuality, as the contrary would encourage potential adversaries to use force and provoke conflict. In fact, communicating continuous preparedness to face a conflict is an essential part of deterrence. Thus, if the adversary

[53] KAUFMANN, W. Op. Cit.

is uncertain whether their aggression will succeed or is certain it will lead to a swift and vigorous response with an outcome contrary to their interests, they will refrain from acting. Consequently, effectively communicating the deterrer's capabilities and willingness to act is essential for effective deterrence and is the key to defense in peacetime[54].

To achieve this, it will be essential to communicate and make known a continuous preparation for the most demanding scenarios. It is not enough to communicate small training exercises or small activities. It is necessary to communicate training exercises with sufficient scale and ambition to cause doubt or at least sow the seed of uncertainty in the potential adversary. These training exercises should be joint, of an appropriate level of ambition, and showcase the full spectrum of the deterrence strategy: strategic projection, response capability, operational sustainment, A2/AD capabilities, precision platforms and vectors, etc.

Furthermore, considering that the decision-making process of one potential aggressor will always be conditioned by their own norms and values, as well as their nature, the communication strategy should incorporate a strong cultural approach aimed at the adversary, with the purpose of reaching their values and influencing their perception[55].

Multidomain Operations: Disruptive Technologies

Multidomain operations are based on the digital transformation of the forces, enabling them to confront challenges and threats arising from the digital era. To ensure adequate deterrence in the multidomain environment, the organizations and military structures must adopt more mature and collaborative command and control models than those previously used, to achieve superiority in the decision-making process. Additionally, to exercise credible and effective deterrence, it should be necessary to have, at least, capabilities that allow to:

- Operate and achieve superiority in cyberspace, the cognitive domain, and outer space.

[54] CENTRO CONJUNTO DE DESARROLLOS DE CONCEPTOS (EMAD). Entorno Operativo 2035. Op. Cit.

[55] PAYNE, K. Op. Cit.

- Establish an interconnected data and information exchange network within the battle space, where each platform contributes and receives essential information for situational awareness.
- Promote the development of future communication technologies, paying special attention to Artificial Intelligence and the Big Data in order to speed up the decision making process.

Emerging and disruptive technologies have arrived to revolutionize the operational landscape, particularly those related to connectivity, information management, and automation; aspects that will notably impact on situational awareness, ethical and legal considerations, and decision-making. In this regard, this deterrence strategy must possess this technology, in both quality and quantity, to be truly effective and provide an adequate response. Specifically, it could have disruptive capabilities in the following fields:

- Autonomous combat systems (aerial drones, autonomous land and naval combat systems, etc.) that would complement our offensive and reconnaissance capabilities;
- Quantum technology applied to sensing, supporting battlefield monitoring;
- Offensive and defensive space capabilities to dominate outer space;
- Hypersonic systems (missiles), enhancing the offensive capabilities and thereby complementing the punitive strategy;
- Sixth and seventh-generation communication systems, providing efficiency, reliability, and robustness to the Command and Control system, and improving its resilience[56].

In this regard, the lack of availability or delays in acquiring these technologies could undermine the deterrence strategy and result in a loss of interoperability with the allies. This, in turn, may enable strategic surprise in favor of the adversary—who may already possess such capabilities—and ultimately lead to defeat in conflict[57]. It is therefore

[56] NATO. Emerging and disruptive technologies. Topic of NATO Headquarters. 2024.

[57] CENTRO CONJUNTO DE DESARROLLOS DE CONCEPTOS (EMAD). Entorno Operativo 2035. Op. Cit.

evident that possessing these emerging technologies will provide a decisive advantage over potential adversaries, significantly enhancing the deterrent posture[58].

Resilience: Adapting to Adversity

We have established that military deterrence must be based on balanced and resilient forces capable of operating across the full spectrum of conflict. We have also emphasized the need to enhance capabilities in cyber defense and strategic communication. In this context, it is paramount to optimize structures, making them more horizontal and less hierarchical; enabling decentralization in decision-making and simplifying processes. This approach will allow to operate in a networked manner, maintaining an appropriate dispersion of forces, which must be connected through a reliable and robust command and control system. Furthermore, structures and organizations should have alternative systems in place to continue operations in degraded environments or in the event of the destruction of primary systems. The combination of these actions will provide adequate resilience to all command structures[59].

Our analysis has also highlighted that, to effectively contribute to deterrence, the resilience of these structures must focus on the cyber, cognitive, and outer space domains of the aerospace sector[60]. Therefore, that is compelled to strengthen these capabilities in these areas to generate deterrence, prevention, and an effective military response[61].

On the other hand, NATO has developed a political document aimed at reaching an agreement to improve the resilience of its members. Its purpose is for member states to commit to increasing their resilience in critical areas and military capabilities, enhancing civil protection, cyber defense, and defense against nuclear, biological, chemical, and radiological (CBRN) threats. Consequently, these fields should be also included into the denial side of the strategy (defensive posture)[62].

---

[58] CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL (CESEDEN). Panorama de Tendencias Geopolíticas. Horizonte 2040. Ministerio de Defensa. Madrid, 2021.

[59] CENTRO CONJUNTO DE DESARROLLOS DE CONCEPTOS (EMAD). Entorno Operativo 2035. Op. Cit.

[60] BEAULIEU, B. y SALVO, D. Op. Cit.

[61] CENTRO CONJUNTO DE DESARROLLOS DE CONCEPTOS (EMAD). Entorno Operativo 2035. Op. Cit.

[62] FREEDMAN, L. Op. Cit.

In this regard and focusing on areas not yet covered by our analysis, and with the aim of facing the conventional high intensity warfare, the new deterrence strategies will have to include an adequate number of military personnel and their corresponding replacement in the event of conflict. Therefore, it should be necessary to perform an integral analysis to identify deficiencies, costs, and activation methods of a reserve force. It is essential to review the reservist models so that it can adapt to the evolving pace of the military force and meet the needs of the new operational environment, effectively contributing to the deterrence strategy.

Smart Deterrence: The Deterrence of the Future?

As observed, the concept of deterrence is more relevant than ever and capable of preventing conflict. We have seen how deterrence strategies stabilize situations or maintain the status quo. The more stable a situation becomes, the more successful the implemented deterrence strategy is, and the easier it is to maintain over time. Conversely, as the situation becomes more volatile and unstable, the deterrence strategy becomes crucial but also more challenging to maintain and develop. In fact, we have observed that deterrence is not improvised and cannot be immediate. It is a strategy that requires a lengthy planning process aimed at influencing the decision-making of the adversary to be truly effective. This influence process requires time and strong political determination to establish the nation's vital interests and the red lines worth fighting for. Without a doubt, if we improvise a deterrence strategy, it is highly likely to fail, leading us into conflict.

Furthermore, we have observed that the concept of deterrence is insufficient to operate effectively in the new operational environment. The current deterrence strategies need to be complemented or reformulated to address this new environment, where fragility, volatility, uncertainty, emerging technologies, and continuous competition undoubtedly emerge as common denominators in the defense policies of most states.

Is a classic deterrence strategy credible? Are they effective in facing these new times of uncertainty? Our conceptual approach to deterrence and our analysis of the operational environment have led us to conclude that it is necessary to complement the traditional concept of deterrence for it to be truly effective. In this regard, we have identified the capabilities and components required to have a genuinely effective and credible deterrence strategy. It has been confirmed that we need to possess both punitive (offensive) and denial (defensive) capabilities. Additionally, this deterrence strategy must have adequate resilience across all structures and organizations and cannot

lag behind in multidomain operations. To achieve this, it is essential to equip them with emerging and disruptive technologies. Finally, this deterrence strategy must include an effective communication strategy, culturally focused on the potential adversary. Only then can it reach their values, perceptions, ideology, religious precepts, etc.

A successful deterrence means that nothing happens. Our deterrence strategy may be functioning correctly without our awareness. However, there are many reasons why nothing occurs: our adversary may have restrained itself upon assessing our denial and punishment capabilities; perhaps, after evaluating the risks, it has decided that changing the status quo is not worthwhile; or simply, some other factor led them to change plans. Therefore, a credible deterrence strategy is more necessary than ever. Smart deterrence, to avoid conflict.

*Miguel Ángel Pérez Franco**
LIEUTENANT COLONEL
WAR COLLEGE GRADUATED
DEFENSE JOINT STAFF