CIVITAS, 2025, 15(1), 212-232
www.civitas.rs

Zoran M. Marjanović[*]
Marija Mićović[**]
Aleksandar Terzić[***]

UDC 327.54(4)
Review article
Received: 13/05./2024
Accepted: 12/11/2024

DETERRENCE INSTRUMENTS IN THE POST COLD WAR PERIOD

Abstract: Relying on conventional and/or nuclear armed forces of one or more states for deterrence[1] has represented a flawed approach to foreign policy implementation since the 1950s. In the West, even in the period following the Second World War, official policy—exemplified by Hoover's stance—held that it was necessary to "play dirty" in foreign relations. In the East, General Gerasimov's well-known statement that the

[1*] Doctor of Philosophy in Security Studies, Ministry of Defence of the Republic of Serbia, Belgrade, Republic of Serbia, ORCID number: 0009-0001-0087-3106; e-mail: marjanovic.cole.zoran@gmail.com
[**] Doctor of Philosophy in Security Studies, Research Associate, Criminalistics and Police University, Belgrade, Republic of Serbia; e-mail: marijablagojevic.bp@gmail.com
[***]Master of Political Science in International Relations, Belgrade, Republic of Serbia; e-mail: at.terzic.93@gmail.com

Deterrence, according to the Dictionary of Military and Associated Terms of the U.S. Armed Forces, is defined as "the prevention of action by the existence of a credible threat of unacceptable opposition and/or the belief that the costs of the action are greater than the perceived benefits." In the same dictionary, deterrence is also equated with the term strategic effect in the context of defining tasks and missions (e.g., deterrence, stabilization), where the list of strategic effects includes: "advance, secure, compel, compete, contain, deceive, defeat, degrade, delay, delegitimize, deny, destroy, deter, discredit, disable, discourage, disrupt, redirect, engage, enhance, integrate, isolate, kill, maintain, manage, neutralize, prevent, protect, stabilize, suppress, synchronize" (DoD Dictionary of Military and Associated Terms, 2021, pp. 2, 63). Deterrence, as defined here and practiced for more than three quarters of a century, has evolved in tandem with shifting strategic conditions that shape responses to contemporary threats.

engagement of armed forces is merely the final act of a conflict suggests that certain conflicts unfold in peacetime and may be more significant and effective than military ones. The actions of state authorities in deterring such and similar directions of the highest state leaders included a shift from "hard power" to "soft power" as dominant in the realization of foreign policy conflicts. The culmination of this practical transition was marked in the post–Cold War period with the emergence of "smart power," where the concept of deterrence was reshaped under the influence of new technologies. These developments dictated a modification of deterrence and its adaptation to the rapid information-technological changes in the life and work of individuals, and consequently, the countries in which they live (or stay).

Keywords: *deterrence, instruments, security services, cyber deterrence, concept of Israel.*

1. Introduction

This research begins with an examination of the conditions that have led to the emergence of a new concept of deterrence for contemporary states in the post–Cold War period. Special attention is given to the case of Israel, with the aim of providing a scientific account of deterrence through two complementary lenses: an analysis of Western theoretical studies on the subject, and a close reading of Israel's most significant strategic document regulating deterrence—recently disclosed and translated—which outlines the instruments available to the state for such engagements.

From the opening statements of Joseph S. Nye in the first chapter of his work, where the concept of deterrence is approached through the lens of power, it becomes clear that deterrence is not reducible to the use of armed force alone. The shift in the "center of gravity" from exclusive reliance on military power—so-called *hard power*—toward *soft* and increasingly *smart power* reflects the transformation of contemporary threats. These threats now operate primarily within the spheres of infor-

mation and telecommunications, cyberspace, and outer space, and they constitute not a future challenge but a present reality for states engaged in deterrence.

Coercive instruments traditionally associated with deterrence—tanks, planes, armored vehicles, and other combat assets—have largely migrated to new domains of conflict: drones (unmanned aerial vehicles), computers, media, and the virtual world. Within these domains, information operations have become among the most critical instruments of coercion. Deception, misinformation, and lies are now routinely employed by major powers in pursuit of strategic objectives. Cyber deterrence must be recognized as a necessary component of modern deterrence; however, the inertia of large, bureaucratic state security and intelligence systems raises questions about their capacity to adapt to the rapid pace of emerging threats. These threats, often invisible or covert, require swift integration into the organizational structures of entities tasked with countering them, particularly state security services[2].

When discussing deterrence and the engagement of the state sector, we refer to the designated actors responsible for specific operations. Yet the non-state sector is also deeply embedded in this sphere, and its obligations should be codified in the state's highest strategic documents. Secret threats typically involve a high degree of concealment during both the planning and execution phases of an operation. These actions often include deliberate efforts to obscure the identity of the true perpetrators, employing deception to ensure that the actual actors remain unknown. Security services represent the "extended arm" of politics. In addition to providing information—through intelligence, counterintelligence, and

[2] In this research, the term *security services* refers to all state entities engaged in counterintelligence, intelligence, non-intelligence, and security-related activities—functions that most commonly involve covert operations. These services form part of a country's integrated security-intelligence system. In the Republic of Serbia, the scope and composition of the security services are defined by the Law on the Basics of the Organization of the Security Services of the Republic of Serbia. In other countries, comparable entities may be referred to as elements, offices, administrations, agencies, or state services. To avoid terminological inconsistencies across jurisdictions, this study adopts the unified term security services.

security activities—to the political leadership concerning national security, they function as both defensive and offensive instruments. Beyond these core activities, they also undertake non-intelligence operations and engage a wide range of other entities, institutions, firms, companies, and similar actors, particularly in the application of coercion within deterrence, most notably by great powers. By observing threats on a daily basis, due to the speed at which they evolve, it becomes clear that only through timely and high-quality deterrence is it possible to act preventively against specific threats.

2. Instruments of Deterrence in the Post-Cold War Period

The creator of the term *soft power* in foreign policy, Joseph S. Nye, an American theorist, highlights a changed understanding of the nature of power in the modern world. He considers the state's ability to influence others and impose its will through the promotion of democracy (both internal and external policy), mass culture, and similar means—not through military and economic force, which would constitute *hard power*. Nye emphasizes that *soft power* alone is insufficient to achieve strategic objectives. For this reason, he introduces another term into international relations theory: *smart power*, which combines coercion, economic pressure, and persuasion.

Nye states that information has always meant power, and that modern information technology disseminates information more widely and rapidly than at any previous point in history. As a result, the importance of information as a component of power has significantly increased. Nye notes that the nature of power has changed over the past fifty years, particularly following the most recent information revolution, which has rendered computers and the Internet indispensable across all spheres of life.

While Nye acknowledges that nuclear deterrence, domestic armed forces, and the stationing of troops abroad will remain relevant even in the information age, he asserts that these instruments alone will no longer suffice to ensure national security (Putnik, 2012). It is worth noting that as early as 1990, Nye hinted at the transformation of deterrence

strategy, an evolution that today may be compared to cyber deterrence and the ongoing search for new instruments of deterrence.

In his research, Sten Rynning identifies the renewed strategic competition between the Russian Federation (RF) and NATO as a key factor in the development of deterrence strategies, shaped by the diversity of strategic perspectives among NATO member states. NATO perceives and responds to the Russian Federation's new generation warfare, which essentially represents a strategy of coercion, often directed at the adversary's information space. New generation conflicts employ a range of tools to persuade and deter unwanted political developments, and most importantly, they erase the traditional distinction between war and peace.

NATO has observed several new conceptual approaches adopted by the Russian Federation across various political domains, particularly in relation to societal resilience, enhanced cooperation among security services, cyber security, and the need for rapid decision-making. In 2014, NATO established the Joint Intelligence and Security Division, one of the instruments designed for early detection of Russian intentions. However, a key shortcoming remains – NATO's political-military headquarters do not integrate the security services of member states, but merely coordinate them, and the intelligence that member states provide is incorporated into a collective assessment of Russian policy and actions.

In the context of hybrid threats, this coordination proves particularly contentious, as it introduces ambiguity and potential confusion within the information spaces of allied states. NATO has improved its cyber defense capabilities and the coordination of security services, and since 2016, cooperation with the European Union in addressing hybrid threats has been notably strengthened. That year, a joint declaration was adopted, leading to a shared work program with the Centre of Excellence for Countering Hybrid Threats, located in Helsinki.

In response to the annexation of Crimea by the Russian Federation in 2014, NATO has introduced a combination of *deterrence by denial*—including grey zone conflict management, societal resilience, and deployment of forces to counter a limited land grab—and *deterrence by*

punishment, involving a full spectrum of responsive capabilities, from conventional to nuclear. NATO remains largely committed to deterring the Russian Federation through punitive measures. During the Cold War, NATO's flexible response strategy reflected a political compromise (Rynning 2021).

National security can be threatened not only by armed forces, but also by governments, groups, individuals, and other non-state actors—or those posing as such. Namely, in the era of new technological development, the primary dimension of conflict is no longer land, air, or sea. A few years ago, it shifted decisively to cyberspace. The great powers—the United States of America (USA), the Russian Federation, and others—have long since established forces and centers dedicated to both protection and conflict in the cyber domain. In 2018, NATO Secretary General Jens Stoltenberg issued a statement regarding the interpretation of Article 5 of the NATO Founding Treaty in the context of cyber attacks originating from the territory of the Russian Federation. The Secretary General of the Alliance, which is led by the USA, affirmed that cyber attacks may be treated as attacks on NATO members. Depending on the nature of the attack, NATO may invoke Article 5, thereby alerting all member states. However, this provision will not be applied automatically to every cyber incident. Stoltenberg deliberately refrained from specifying the conditions under which Article 5 would be activated. In recent years, cyber attacks have been accompanied by public accusations, primarily from senior officials in the USA, France, and Great Britain, against presumed perpetrators from the Russian Federation. These accusations have been met with consistent denials from Russian officials, resulting in a persistent stream of contradictory statements from both Western and Eastern sources. Just a few years later, in 2021, NATO expanded its strategic framework by introducing a fifth dimension of conflict: space. This addition may also serve as grounds for activating Article 5. NATO declared that its members would be prepared to respond to attacks *in* space and *from* space, recognizing that such attacks could pose threats comparable to conventional military aggression (Stoltenberg, 2018; 2021). .

Soesanto and Smeets view cyber deterrence through a military lens and argue that the concept carries at least three distinct meanings. It

may refer to the deterrence of a (military) attack, the use of (military) means to deter (military) cyber-attacks, or the use of (military) cyber means to deter by means of a (military) cyber-attack. Scholars currently disagree on the extent to which hostile cyber-attacks can be effectively deterred—perhaps due to the observation that cyberspace hosts a multitude of actors with access to offensive cyber capabilities. Some researchers believe that the strategic value of damage caused by cyber-attacks is generally limited, which in turn reduces the opportunities for effective deterrence. Proponents of cyber deterrence typically refer to four logics: *deterrence by denial* (synonymous with cyber security), *deterrence by punishment* (where costs outweigh benefits), *deterrence by entanglement* (where interdependence disincentivizes aggression), and *deterrence by delegitimization* (which seeks to restrict the battlefield to military actors only). Although cyberspace is increasingly recognized as a new domain of warfare, its utility for deterrence, particularly outside the military sphere, remains uncertain. Politically motivated cyber-attacks with strategic impact are relatively rare, most relevant documents are highly classified, and access to cyber operators is limited. Moreover, existing military cyber organizations are still in the process of development.

Thus, Soesanto and Smeets propose four future research directions for cyber deterrence: its integration into broader deterrence postures within multi-domain strategic competition; a deeper focus on technical aspects at operational and tactical levels; greater emphasis on competence; and the development of strategies to curb and blunt hostile aggression in cyberspace (Soesanto & Smeets, 2021). As of now, there is no consensus among scholars on the viability of cyber deterrence as a strategic concept.

Since the attacks of September 11, 2001, counterterrorism studies have increasingly focused on the question of whether non-state actors can deter. Eitan Shamir identifies a link between deterrence and violent non-state actors in the context of preventing terrorist threats. Shamir argues that Israel has developed a concept of deterrence specifically aimed at violent non-state actors, which includes efforts to contain adversary capabilities. In addition to restraint, Shamir emphasizes that deterrence must be understood as a process-based approach—one that presupposes a continuous relationship between the deterrent and the deterred.

The prevailing view that terrorist groups, especially those motivated by religious ideology, are difficult to deter stems from several factors: they are rarely monolithic organizations, often operate through hidden networks and autonomous cells, and lack a centralized leadership with whom state representatives could engage. Moreover, their ideological frameworks typically exclude the possibility of diplomatic negotiation. Consequently, Shamir contends that full deterrence of violent non-state actors is not feasible, and that a restrictive approach is more appropriate. This implies that deterrence should not rely on symbolic attacks, but rather on repeated responses to norm violations, a strategy Shamir refers to as the "grass-cutting" approach. Restrictive and cumulative deterrence of violence by non-state actors draws more from criminological understandings than from Cold War models of absolute deterrence (Shamir, 2021). As in many areas of life, strategic experience and culture cannot simply be transferred from one entity to another. Shamir underscores that deterrence is shaped by a state's unique economic, military, and political capacities, and that it cannot be copied wholesale from one state or culture to another—though certain positive practices may be adapted.

Practically, the threat of sanctions will not yield the same results for economically independent states as it might for dependent ones. According to one definition, deterrence is never achieved through a single act, but through a series of coordinated activities—often involving security services—that serve the political goals of a society's elite, whether state-led or otherwise. Some theorists define hybrid warfare as a fusion of conventional deterrence and insurgent tactics. The broader question is whether hybrid warfare constitutes a new form of conflict, or a strategy employed by states to pursue political objectives in both war and peace—most often through subversive, non-intelligence activities. Hybrid warfare exploits nationalist identities, obscures the responsibility of perpetrators, and may even garner political support among foreign observers.

The strategy of the Russian Federation (RF) aims to weaken NATO's readiness to pursue its own deterrence threats and vice versa. Military strategists have long recognized that, in order to achieve victory, one side in a conflict must provoke rebellion or instability, thereby gaining

the ability to prevail more easily over its opponent. Direct military conflicts are generally avoided by states, as they tend to benefit only the great powers. Accordingly, more subtle and indirect techniques of problem-solving are considered more appropriate. These techniques include the use of propaganda to mobilize insurgent support, to demoralize enemy forces, and to target the weak points of opposing forces. Crisis situations, whether within a country or on a global scale, such as epidemics or pandemics, give rise to a new type of threat. Regardless of the priority engagement of, for example, the national health apparatus, such situations require the involvement of security services. This begins with the registration of threats, procurement of resources, equipment, and devices across the globe, and extends to the prevention of misinformation, defeatism, and panic, as well as other related activities (Marjanović & Mićović, 2022).

As one of the important instruments of deterrence, we cite *land power*, which—in the context of economic independence, both in terms of energy and agriculture, and with regard to other resources necessary for the functioning of companies, organizations, the population, the army, and the state—represents a form of power that nullifies all instruments of deterrence related to coercion in the economic sphere and sanctions in this area (Marjanović & Mićović, 2023). Thus, economic activities (sanctions) applied to the Federal Republic of Yugoslavia in 1999, and those used against the Russian Federation in the 21st century as an energy-independent country, cannot have the same effect on the leadership of the country and the population in general.

There are various instruments that can be applied in hybrid warfare: *propaganda*, which influences the attitudes of members of the target society and serves to hinder the ability of the target group to rely on public support in implementing its policies and mobilizing its resources; *espionage*, in which agents covertly gather intelligence in order to give the conflicting party an advantage in forced negotiations. Then, the use of agents in the targeted, intentional dissemination of *false information* among members of the public regarding the real intentions of certain organizations, or the creation of misunderstandings and discord (which do not yet exist) within the target society. The next instrument is criminal disruption, whereby agents of the parties to the conflict engage in

attacks, cyberattacks, sabotage, kidnapping, and other forms of subversion. The creation, training, and use of the *fifth column*[3] (individuals or groups who usually operate covertly and are embedded in a much larger population against which they operate), in the role of "unmarked soldiers," makes it possible to man checkpoints, occupy government buildings and other facilities, and detain persons of strategic importance for a time. A side in a conflict might initiate border skirmishes to unsettle the other side and test its weaknesses, then proceed to deplete forces and resources and disengage from the center of action using guerrillas. The USSR applied these techniques immediately after the Second World War, sponsoring communist movements in Europe and other locations to undermine the capitalist order. The modern military doctrine of the Russian Federation emphasizes the need to respond to both external and internal threats, not only from other great powers, but also from subversive organizations operating in areas controlled by the Russian Federation.

Military theorists recognized decades ago that the United States had gained a strategic advantage in precision strikes and in information and communication technologies, and that states could become targets of information warfare. The initial stages of such warfare typically involve disinformation campaigns. Information superiority has become indispensable in modern conflict (Lanoszka, 2016). Given that the theoretical definition of hybrid war remains fluid and that no comprehensive definition of the phenomenon has been established, the term is often used inconsistently—frequently to suggest that a hybrid war is underway, even when the situation may in fact involve covert operations or non-intelligence activities conducted by security services. When such activities are occurring, they should be properly identified as intelligence, counterintelligence, or non-intelligence operations—forms that

[3] The term *fifth column* dates back to the Spanish Civil War, when in 1936 Spanish General Emilio Mola declared in a radio announcement to the residents of Madrid that four nationalist columns were moving towards the capital, but that there was a fifth column in the city that would strike from within. The term was later widely used during the Second World War to describe collaborators who secretly acted in favor of the enemy, and it remained in use for decades thereafter.

have existed since the inception of security services, albeit with techniques adapted to technological advancement. When invoking the conceptual definition of war, one should begin with its theoretical, legal, and normative foundations, and assess whether the concept of hybrid war is adequately defined (Lanoszka, 2016).

Professor Ilija Kajtez[4] presented information indicating that, even in the aftermath of the Second World War, preparations for global surveillance by the United States had already begun. In 1970, the security services of the United States—CIA and NSA—and Germany's BND allegedly concluded a secret agreement to conduct illegal global wiretapping of a substantial portion of the planet, including 130 countries and the United Nations. The operation was code-named *Rubicon* by the BND—symbolically referencing Julius Caesar's irrevocable crossing of the Rubicon—although its original name was *Theasaurus*. The CIA reportedly referred to the same operation under the code name *Minerva*. Most of these activities were conducted through the Swiss company Krypto AG, allegedly founded by Boris Hagelein, a specialist in encryption. The company generated substantial profits, which were reportedly funneled into the black budgets of the U.S. and German security services and used to finance their economic operations. Krypto AG was allegedly established by the CIA and the BND. The BND is said to have sold its stake only in September 1993, following the arrest of Hans Biller in Tehran, where he was held for nine months. This event led to the loss of German governmental support for the operation, while the United States allegedly continued these activities until 2018.

In early 2020, Peter Müller produced a documentary on this operation for a German television program, in which the Socialist Federal Republic of Yugoslavia (SFRY) was mentioned as a purchaser of encryption devices as early as 1957 and 1978. The documentary was broadcast by German and Swiss public services ZDF and SRF, as well as the American *Washington Post*. Some countries, including Austria and the SFRY, discovered that these devices were readable by the other side.

[4] Professor Ilija Kajtez, a retired colonel of the Ministry of Defense of the Republic of Serbia, presented the above data during a guest appearance on a television program in Belgrade on August 21, 2022.

Given the global scope of the operation, caution is warranted in interpreting the data—particularly as it continues to be disseminated by the same institutional actors who have consistently participated in a series of non-intelligence activities conducted by the United States, Germany, and Switzerland. It remains unclear whether this reflects the preparation of a new operation or the revival of an older one.

Peter Viggo Jakobsen sees deterrence in a broader form, one that includes both state and non-state actors and is situated within the context of multinational operations. He examines this type of operation through the implementation of attacks on peacekeeping forces—primarily those composed of Western countries—that were deployed in the territory of the former Socialist Federal Republic of Yugoslavia (SFRY). The use of peacekeeping forces in foreign countries, according to Jakobsen, takes place within a changing context in which the strict demarcations between deterrence and coercion are collapsing.

Jakobsen interprets these collapsing boundaries through several interrelated factors: a coercive threat that demonstrates the ability to defeat an opponent quickly and at minimal cost; a compliance deadline that creates a sense of urgency; an assurance that no further demands will follow compliance; and the inclusion of positive incentives to reduce the cost of compliance. He further stresses the need to deter and coerce simultaneously the various participants both on and off the battlefield during multinational operations.

Jakobsen thus distinguishes four groups of deterrence participants—both positive and negative—in peacekeeping operations: fighters who use force on the battlefield; allies who provide material support to the fighters; supporters of fighters who block action in regional or global institutions; and other persons, bystanders, present on the battlefield at the global level who do not engage in combat. He concludes that for deterrence to be effective, participants cannot rely solely on threats and the use of force, which are insufficient. According to Jakobsen, it is necessary to supplement these measures with persuasion and encouragement, designing and implementing an influence strategy that fully integrates all three components: coercion, persuasion, and incentivization (Jakobsen, 2021).

In this research, Jakobsen confirms that the specific features of certain cultures, countries, and phenomena, particularly the activities in question, introduces distinct characteristics and factors that make each instance of deterrence unique. As a result, applying a uniform template across different cases is not an adequate approach. Nevertheless, effective solutions can be identified and selectively implemented. In the next chapter, we will examine how Israel regulates deterrence.

3. Specifics of Deterrence in the Strategy of the Israeli Defense Forces

An analysis of Israel's strategic document—the strategy of the Israel Defense Forces (IDF)—indicates that the strategic relationship between two states, that is, a state and a great power (Israel and the United States), plays an important dual role in Israeli deterrence, reflected in the following. Very close cooperation with the United States increases Israel's scope for political and operational maneuvering in response to aggression against it and enhances Israel's operational capabilities to inflict damage on its enemies—both through greater force buildup and through the threat of U.S. intervention on its behalf.

Adapting the concept of deterrence from 21st-century U.S. policy, modifying the nature of the American commitment within the extended deterrence model, developing Israeli deterrence in the 21st century, expanding the concept of deterrence to include non-military tools in strategic planning, and strengthening the link between defense and deterrence are the main features that characterize this strategy (Golov, 2016).

In August 2015, the Israel Defense Forces published their first-ever publicly disclosed strategic document, which was translated into English in August 2016 (*Israel Defense Forces Strategy 2016*). The seriousness with which one of the most endangered countries in the world approaches the role of its security services—as essential to national survival and the dignity of its citizens—can best be appreciated through a quote highlighted in the strategy itself. It is a reflection by Amos Yadlin,

former head of Israel's Military Intelligence Directorate, which reads: "Hamas and Hezbollah, we did not destroy, but we were able to establish deterrence. This is basically because we hit them hard, and because the terrorists, in a way, have become like incomplete state entities, but they are like semi-state entities. Terrorists have discovered that when they are responsible for their economy, for education, for the lives of their people, suddenly they don't dare to use terror all day long." (Graham 2016, p. 24). This statement speaks volumes about the practical effects of deterrence within a state framework.

Deterrence is created in perception, but it is also grounded in physical and concrete elements. Israeli deterrence relies on the superiority of its defense systems, with the important caveat that this superiority is more limited than in the past due to the evolving nature of threats. Deterrence must be specific and tailored to each adversary. At the same time, deterrence against any enemy must be generalized and cumulative over time to preserve the existing situation. It must also be crisis-specific and clearly defined, so that the adversary is compelled to act, or refrain from acting, in order to halt hostilities or prevent further deterioration of the situation.

According to this strategy, the components of deterrence include: a credible threat of heavy offensive operations based on force buildup; public perception of actions that signal a willingness to take risks; and limited offensive actions. It is essential that the armed forces maintain an image of deterrence and capability—one that portrays them as an unpredictable adversary capable of responding in a serious and decisive manner.

Israel periodically conducts airstrikes in Syria and Lebanon to enforce its 'red lines' against terrorist organizations—for example, the December 2015 airstrike targeting Samir Kuntar, a senior Hezbollah operative (Graham, 2016, p. 25). Such deterrent actions are carried out within the framework of the Campaign Between Wars (CBW). The rationale for employing force in the CBW context is multifaceted: to weaken the component of negative force, to minimize the enemy's capabilities and strengthen its own forces, to create optimal conditions for victory in the future war, to shape favorable conditions for future

conflict, to legitimize Israeli operations, and to delegitimize enemy actions. Operations conducted between wars require a multidisciplinary approach, encompassing military, economic, legal, media, and political spheres. The operational concept must be unified around a single strategic objective. Offensive measures may include a combination of covert and clandestine operations across all fronts and dimensions, extending beyond Israel's borders. Crucially, this policy is informed by intelligence gathered through the security services and is designed to disrupt enemy activities or intentions. It is important to note that this document outlines an overt deterrence strategy—one that underscores the limits of Israel's restraint and signals its readiness to act decisively when necessary.

The guiding principles for the use of force in the Campaign Between Wars (CBW), particularly in covert and clandestine operations, emphasize that such actions must be initiated, sustained, and tightly controlled. These operations typically involve short-term deployments of forces acting in a covert or clandestine manner and are marked by inter-organizational cooperation—both operational and intelligence-based—with the security services. They also rely on international collaboration to conduct intelligence work, disrupt enemy activities, and preserve the legitimacy of Israeli defense actions while undermining the legitimacy of the adversary. In addition to the military dimension, CBW operations extend into the public perception, economic, and legal spheres, all of which contribute to diminishing the enemy's capabilities and legitimacy. These efforts depend on accessible and accurate intelligence (Graham, 2016, p. 26). As Chief of General Staff Lt. Gen. Gadi Eisenkot articulates this strategic shift: "In the past, we had an army in one of two situations—it was either preparing for war or at war. But that is no longer the reality. We are not preparing for war, and we are not at war. We are in a different situation, one in which the entire campaign, shaped by evolving perceptions, relies on the security services and on both covert and overt capabilities to prevent our adversary from gaining strength, and to weaken the enemy in a way that does not provoke escalation." (Graham, 2016, p. 26). This perspective, echoed by Amos Yadlin and embedded in the broader strategy of the Israel Defense Forces, underscores that the cornerstone of CBW doctrine is the activity of the security services. From this segment of Israel's strategic framework, analysts worldwide

can draw significant insights from a country that arguably possesses unparalleled experience in countering threats to national security.

It is extremely important to emphasize that, within the theoretical concept of deterrence, Israel may have achieved the most through its strategic efforts. It immediately proposes the construction of CBW forces, where the process should unfold as follows: first, by establishing a coordination center for CBW operations, which includes inter-organizational and inter-ministerial elements; and second, by developing capabilities for covert and clandestine CBW operations (Graham, 2016, p. 44). Given that such operations typically involve a wide array of national experts who are not concentrated within a single institution, the proposed coordination center constitutes a foundational step in force development. The development of covert and clandestine capabilities thus reflects the 'artisan' dimension of security professions, those whose craft and discretion are essential to the successful execution of such operations.

One of the key professions involved in such operations is the domain of expertise in current trends in information and telecommunication systems (ITS). The cyber sphere represents one of the principal areas of defense in which offensive activities and intelligence gathering are conducted. The process of building forces in this domain is structured around several core actions. First, the establishment of a cyber branch directly subordinated to the office of the Chief of the General Staff of the Israeli Armed Forces, tasked with the development and operationalization of cyber capabilities. This branch is responsible for planning, organizing, and executing conflicts in cyberspace. In addition to these duties, it bears a specific obligation: the development of technological capabilities for the cyber defense of all operational systems, as well as the protection of support systems such as manpower and logistics (Graham, 2016, p. 44).

In order to improve working conditions and build potential capacities, it is necessary to develop a unified command-and-control language across all headquarters of the Israel Defense Forces operating in the interwar spheres. This standardization is to be implemented through the establishment of dedicated command-and-control schools. Further-

more, it is essential to enhance the ability to utilize high-quality security services and their activities across all levels of operation—national, strategic, and operational.

Force-building in the field of security services is grounded in several key actions: developing and refining the capacity to integrate intelligence; enhancing the ability to hold adjacent territory based on actionable intelligence that enables rapid, high-precision targeting; monitoring enemy doctrines; and exploiting the outputs of security services—both their activities and data—through analysis and dissemination across all levels of command, from headquarters and district commands to tactical units and battalions. These efforts must also include the presentation of a comprehensive picture of enemy formations and the assessment of the effectiveness of Israeli offensive operations against them.

Maintaining baseline readiness is essential for sustaining credible deterrence, alongside mechanisms that accelerate necessary procurement processes. Capacity-building in this context will rely on the following activities: reinforcing strategic and tactical deterrence through cyber warfare; ensuring the availability of security service data as an early-warning mechanism to trigger preventive measures; and enabling preemptive strikes based on early-warning indicators to thwart potential attacks on Israel (Graham, 2016).

It is important to reiterate that the foundation of CBW operations lies in the actions and intelligence provided by security services. In Israel's first publicly released strategic document, the significance of non-intelligence activities and the broader role of security services is explicitly recognized as a cornerstone of its deterrence posture.

4. **Conclusion**

Western theory has qualitatively addressed most segments of deterrence in its conceptual and instrumental definitions. However, the role of security services in deterrence, particularly the application of non-intelligence activities in the pursuit of foreign policy objectives, has received minimal attention. This research has sought to partially clarify that gap.

When discussing the creation of strategies at the highest levels of state governance, which in recent times may have become more of a trend than a necessity, we must recognize that a document, regulation, or strategic paper holds little value if it is not adequately prescribed or implemented. The proliferation of strategic documents, when operationalized, can result in an excessive number of valid regulations. In complex professions, such as those involving deterrence, each within its own domain, this can lead to difficulties for practitioners in identifying, complying with, and applying their obligations effectively. The issue of coordination and the regulation of subordinate legal instruments becomes critical, as the strategic vision articulated by state leadership must be operationalized from the top down, reaching even the lowest-level executors.

Israel has modeled its approach after the United States and NATO. In recent years, both have implemented significant organizational reforms in the coordination of security services: the U.S. established centers to unify security and counterintelligence components, and in 2016 NATO created a center for countering non-intelligence activities and improving inter-service coordination. Israel has gone a step further. The strategy of the Israel Defense Forces (IDF) not only specifies the instruments of deterrence involving non-intelligence activities but also envisions the construction of dedicated forces for such operations—namely, the Campaign Between Wars (CBW). These campaigns include obligations assigned at the highest levels of government, including ministerial responsibilities, organizational adjustments, and the training of personnel for planning, participating in, and executing covert and clandestine CBW operations.

The strategy's emphasis on cyber deterrence, and the creation of a structure for countering cyber threats directly subordinated to the IDF, clearly identifies the instruments to be used against such threats and underscores the role of security services in deterrence during CBW. As a strategic document, the IDF strategy stands out for its clarity and depth. It includes direct quotations from the Chief of the General Staff of the Israeli Armed Forces and the former head of Israeli Military Intelligence, and it offers concrete proposals for solving deterrence-related challenges—through the formation of state units, the development of

operational forces, and the designation of participants with personal involvement from leading experts in the field. This makes the document arguably unique on a global scale, and as such, it may serve as a model from which adaptable elements can be drawn for use in other national contexts.

The vast volume and rapid circulation of information in daily use facilitates the spread of disinformation and deception targeting specific groups, creating fertile ground for poor decision-making by state leaders in the application of deterrence instruments. A new threat has emerged: the extremely short time available for verifying information. This phenomenon poses serious risks to national security. When credible intelligence about a threat is available and no preventive action is taken, the consequences may be as severe—or even worse—than if the information had not existed at all. The events of September 11 in the United States and their aftermath serve as a stark example.

References

1. DoD Dictionary of Military and Associated Terms, (2021). *Standard US military and associated terminology to encompass the joint activity of the Armed Forces of the United State, Department of Defense (DoD)*.
2. Golov, A. (2016). *Israeli Deterrence in the 21st Century*, (Arms Control and Strategic Stability in the Middle East and Europe. Emily B. Landau and Anat Kurz, editors. Tel-Aviv: Institute for National Security Studies, p. 83-97.
3. Graham, A. (2016). Deterring Terror, English Translation of the Official Strategy of the Israel Defense Forces (*Israel Defense Forces Strategy* 2016), Belfer Center for Science and International Affairs, Harvard Kennedy School.
4. Jakobsen, V. P. (2021). Deterrence in Peace Operations: Look Beyond the Battlefield and Expand the Number of Targets and Influence Mechanisms, Denmark (In: Osinga, F. & Sweijs, T. 2021. Deterrence in the 21st Century-Insights from Theory and Practice, Annual Review of Military Studies 2020, NL Arms Netherlands, T.M.C. Asser Press, Hague, Netherlands, p. 327-345).

5. Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe. *International Affairs*, 92(1), University of London, p. 175-195.
6. Rynning, S. (2021). Deterrence Rediscovered: NATO and Russia, *Annual Review of Military Studies* 2020, NL ARMS Netherlands, T.M.C. ASSER PRESS, The Hague, The Netherlands.
7. Shamir, E. (2021). Deterring Violent Non-state Actors, Political Science Department, The Begin Sadat Center for Strategic Studies (BESA Center), Bar Ilan University, Ramat Gan, Israel (In: Osinga, F. & Sweijs, T. (2021). Deterrence in the 21st Century-Insights from Theory and Practice, *Annual Review of Military Studies* 2020, NL Arms Netherlands, T.M.C. Asser Press, Hague, Netherlands, p. 263-286).
8. Soesanto, S., & Smeets, M. (2021). Cyber Deterrence: The Past, Present, and Future, Center for Security Studies (CSS), ETH Zurich, Zurich, Switzerland (In: Osinga, F. & Sweijs, T. (2021). Deterrence in the 21st Century-Insights from Theory and Practice, *Annual Review of Military Studies* 2020, NL Arms Netherlands, T.M.C. Asser Press, Hague, Netherlands, p. 385-399).
9. Stoltenberg, J. (2018). „*Stoltenberg: NATO može da iskoristi član 5. Povelje u slučaju ruskog sajber-napada*“, Preuzeto 10.04.2022. sa adrese https://Vostok.rs, i Stoltenberg, J. (2021). „*Svi za jednog, jedan za sve: NATO uvodi promjenu*“, Preuzeto 10.04.2022. sa adrese https://rtvbn.com.
10. Bajagić, M. (2010). **Š***pijunaža u 21. veku-Savremeni obaveštajno-bezbednosni sistemi*, drugo dopunjeno izdanje. Beograd: MARSO.
11. Bajagić, M. (2013). Obaveštajna aktivnost u funkciji izgradnje sistema nacionalne bezbednosti. *Politika nacionalne bezbednosti* broj 1/2013, str. 61-86.
12. Bajagić, M. (2015). *Metodika obaveštajnog rada*. Drugo, izmenjeno i dopunjeno izdanje, Beograd: Kriminalističko policijska akademija.
13. Marjanović, Z. i Mićović, M. (2022). Uticaj krizne situacije izazvane epidemijom i pandemijom (kovid 19) na korporativnu bezbednost, **Časopis** *Bezbednost*, 3/2022, LXIV, Beograd, str. 100-119.
14. Marjanović, Z. i Mićović, M. (2023). Geografski vektor nacionalne odbrane-Kopnena moć, **Časopis** *Politička revija*, broj 1/2023, Beograd, 183-209.
15. Mijalković, S. (2011). Obaveštajno-bezbednosne službe i nacionalna bezbednost. *Časopis Bezbednost*, 1/2011, Beograd, str. 74-92.
16. Mijalkovski, M. i Konatar, V. (2010). *Neobaveštajna rovarenja obaveštajaca u lavirintima specijalnih operacija*. Novi Sad: Prometej.

17. Milošević, M. (2005). *Odbrana od terorizma*. Beograd: Edicija, Nauka, Svet knjige.
18. Putnik, N. (2012). Kiber ratovanje-novi oblik savremenih društvenih konflikata. (*Doktorska disertacija*). Beograd: Fakultet bezbednosti.
19. Trbojević, M. (2017). Neobaveštajni oblik delovanja obaveštajnih službi. *Srpska politička misao* broj 4/2017., god. 24.,Vol. 58., str. 319-334.