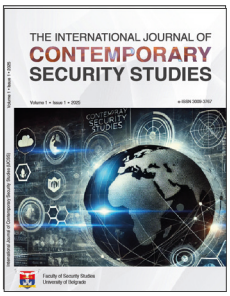
Volume 2 • Issue 1 • 2026 https://doi.org/10.18485/fb_ijcss.2026.2.1.3

Faculty of Security Studies, University of Belgrade
International Journal of Contemporary Security Studies (IJCSS)



Review article

Multi-Actor Deterrence of Small States: The Case of the Republic of Serbia

Aleksandar Pavić[1*], Hatidža Beriša[1]

[1] Military Academy, University of Defense, Belgrade, Serbia, Veljka Lukića Kurjaka 33, 11042, Belgrade, Serbia; aleksandar.pavic@mod.gov.rs (A.P.); hatidza.berisa@mod.gov.rs (H.B.)

* Correspondence: aleksandar.pavic@mod.gov.rs

Received: 1 January 2026; Revised: 15 February 2026; Accepted: 25 February 2026; Published: 1 March 2026.

ABSTRACT

The contemporary security context of small states requires a reexamination of classical concepts of deterrence, based on the symmetry of military capabilities and bilateral relations. The paper analyzes multi-actor deterrence as an expanded analytical framework for understanding how small, militarily neutral states manage security risks amid geopolitical uncertainty and hybrid threats. The paper hypothesizes that deterrence in hybrid environments can no longer be understood as a state-centered mechanism, but as a multi-actor system shaped by state, non-state, and corporate actors in multiple domains. The aim of the paper is to develop an analytical framework of multi-actor deterrence applicable to small states. Through a case study of the Republic of Serbia, the paper shows that the deterrent effect does not primarily arise from the threat of force, but from the potential for networking among different actors and multi-domain synergy, which increases the costs and uncertainty of potential aggression. The paper also identifies key challenges to implementing this model, including institutional fragmentation, capacity asymmetry, and external pressures, highlighting the importance of continued management of multi-actor deterrence mechanisms to preserve the strategic autonomy of small states.

KEYWORDS

Multi-actor deterrence, small states, Serbia, military neutrality.

1. Introduction

The contemporary international security environment is characterized by a profound transformation of the nature of threats, actors, and forms of confrontation. Classical models of deterrence, developed in the context of the bipolar Cold War order, were based on relatively clear assumptions. States were perceived as dominant and rational actors. The lines between peace and war were clearly demarcated, as was the primary role of military power, especially nuclear potential, in deterring aggression. However, in the conditions of the post-bipolar and increasingly multipolar system, these assumptions have significantly eroded. Hybrid threats mark today's security environment, actions below the threshold of armed conflict, multi-domain warfare, and, most importantly, the diffusion of actors involved in deterrence and coercion. This transformation is further accelerated by the penetration of artificial intelligence and cyberspace into the domain of risk management and security

Academic Editor:
Prof. Dr. Vladimir M. Cvetković

Pavic, A., & Beripa, H. (2026). Multi-Actor Deterrence of Small States: The Case of the Republic of Serbia. *International Journal of Contemporary Security Studies*, 2(1), 29-42.

planning (Beriša, Cvetković, & Pavić, 2024; Cvetković et al., 2025; Cvetković et al., 2023; Cvetković et al., 2021; Cvetković, Čvorović, & Beriša, 2023a; Cvetković, Renner, & Jakovljević, 2024).

In such a context, deterrence is no longer exclusively a bilateral relationship between two states. However, it increasingly takes the form of a complex network of interactions involving various state and non-state actors. This phenomenon is described in contemporary literature as multi-actor deterrence, a form of deterrence in which multiple actors, capacities, and domains of action simultaneously influence a potential aggressor's calculation. In addition to the armed forces and classical instruments of state power, this process also involves international institutions, military alliances, economic and technological actors, the media, legal regimes, and even social resilience and the public's cognitive perception. As Milenković et al., points out, this understanding of resilience relies on integrated institutional mechanisms of risk management (Milenković, 2025; Milenković & Cvetković, 2025; Nikolić et al., 2025; Cvetković & Šišović, 2024; Cvetković et al., 2024) Recent research indicates that deterrence in the modern security environment is conceptualized as a distributed and networked process, in which responsibility for the deterrent effect is not concentrated in a single actor, but is distributed among multiple institutions and actors of different levels of power (Baev, Marsh, & Martins, 2025).

A particular analytical challenge is applying the concept of deterrence to small states. Traditional theories of deterrence, based on symmetry or at least on the relative priority of capabilities, are difficult to apply to states that lack significant military or economic power. In this sense, small states are often viewed in classical theory as passive objects of deterrence, as beneficiaries of protection by great powers and alliances, or as actors with limited opportunities to influence security dynamics independently. However, the modern multi-actor environment opens the space to reconsider this approach. It is precisely the complexity, fragmentation, and networking of modern security relations that allow small states, despite limited resources, to achieve a relevant deterrent effect through a combination of different actors, domains, and instruments of action.

The Republic of Serbia can be considered a very interesting case in this regard. As a small state with formally proclaimed military neutrality, Serbia is located in the geopolitically sensitive Balkans, which is also a zone of overlapping interests among several major and regional powers. Surrounded by NATO members (the North Atlantic Treaty Organization) and strongly connected to the European Union (EU), while maintaining developed relations with the Russian Federation, the People's Republic of China, and other actors, Serbia is exposed to various political, economic, informational, and security pressures. These pressures rarely manifest as a direct military threat. However, they are mostly expressed through hybrid instruments of action, including strategic communications, legal and institutional mechanisms, economic leverage, and influence in the information space. A special place in this spectrum is occupied by cyberattacks such as ransomware operations that can produce systemic economic and security consequences (Vidović, Cvetković, Beriša, & Milašinović, 2025).

In such an environment, classical deterrence, based on the threat of punishment, proves insufficient and difficult to sustain. Serbia does not have the capacity to impose unacceptable costs on a potential aggressor through direct military escalation, nor can it rely fully on collective deterrence mechanisms given its specific foreign policy position. However, this does not mean that Serbia is deprived of deterrence potential. On the contrary, in its case, deterrence is increasingly achieved through a combination of deterrence by deprivation, the increasing complexity of the security environment, and strategic pragmatism in foreign policy (Pavić & Beriša, 2025).

The starting assumption of this paper is that small states such as Serbia already employ elements of multi-actor deterrence. However, they are not always explicitly articulated in strategic and doctrinal documents. State institutions, armed forces, diplomatic activity, economic ties, legal and normative frameworks, as well as non-state actors such as the media, academia, the information sector, and the diaspora, together contribute to creating a deterrence effect that is not based on the threat of force, but on increasing costs, uncertainty, and political risk for potential sources of pressure. In this sense, Serbia can be seen not as a front or buffer zone, but as a strategic node in a wider network of security relations. The contribution of this paper is reflected in the conceptualization of multi-actor deterrence as an analytical framework applicable to small states, which bridges the gap between classical deterrence theory and contemporary hybrid security challenges.

The authors will present, through theoretical analysis and a case study of the Republic of Serbia, an analytical framework of multi-actor deterrence applicable to small and militarily neutral states. The paper uses a combined methodological approach that includes a theoretical analysis of the concept of multi-actor deterrence and a case study of the Republic of Serbia, with a focus on institutional and non-state actors. A qualitative approach to the case study of the Republic of Serbia is applied, based on the analysis of strategic documents, laws, official statements, reports, and academic publications. The sources were selected for their relevance to multi-actor and multi-domain deterrence to identify specific mechanisms and instruments of deterrence.

While the existing literature mainly analyses multi-domain and integrated deterrence from the perspective of great powers and alliances, this paper shows that multi-actor deterrence is a key mechanism of security adaptation of small and militarily neutral states, which bases deterrence not on superior force, but on managing complexity and risk perception. In the "multi-actor deterrence" model, military neutrality is treated as a supporting, but not necessary, factor. It shapes the framework in which Serbia maneuvers, providing an additional signal of independence and minimizing the risk of confrontation with great powers. However, the concept of multi-actor deterrence itself can also function in the context of small allied states, with less flexibility in signaling and greater dependence on collective security mechanisms. Neutrality is not the driver of the model, but a factor that strengthens the credibility and consistency of deterrence in a complex multi-actor environment.

2. Theoretical framework: from classical to multi-actor deterrence

The classical theory of deterrence was developed within the realist paradigm of international relations. Deterrence was defined as the ability of a state to dissuade an adversary from taking a particular action by threatening unacceptable costs, either through deterrence by punishment or denial of success (Mazarr, 2018). Such an approach implied a relatively clear link between capacity, intent, and credibility. However, the end of the bipolar system and the emergence of new security challenges have led to an expansion and re-examination of this concept. Continued low-intensity conflicts, hybrid threats, cyber operations, and information warfare point to the limitations of a model that relies exclusively on military force and state actors. Instead of symmetrical relations, asymmetry dominates, and actors' rationality becomes contextual and culturally conditioned.

In such an environment, deterrence is no longer a one-time act of signaling, but a continuous process of interaction. It encompasses not only preventing an armed attack but also managing the behavior of actors in "gray zones," where the boundaries between peace and war are blurred (Fukuda, 2024). This transformation opens space for conceptualizing multi-actor deterrence as a broader analytical framework.

Multi-actor deterrence is not treated in this paper as a normative model that states should adopt, but rather as an analytical framework for understanding how deterrence is actually achieved in a complex and multi-domain security environment. This approach is in line with recent work suggesting that deterrence can be understood less as a linear relationship between threat and response, and more as the result of the interaction among multiple actors, domains, and institutional mechanisms within a complex security system.

2.1. Classical deterrence theory: assumptions

Deterrence theory is one of the fundamental concepts of security and strategic studies in the second half of the 20th century. Its classical form was developed in the context of the nuclear confrontation between the United States of America (USA) and the Soviet Union and rested on a relatively stable set of assumptions: states are rational and unitary actors, security interactions are primarily bilateral, and decisions about the use of force are made based on cost-benefit calculations. In such a framework, deterrence is defined as preventing an adversary from taking undesirable action by threatening unacceptable punishment or denying the opportunity to succeed in aggression.

A key contribution to this understanding of deterrence was made by Thomas Schelling, who understood deterrence as a special form of influencing an adversary's behavior, based not on the direct use of force but on the threat of its use and the management of expectations and perceptions (Schelling, 1960). In this sense, deterrence is primarily a psychological and communicative process, not exclusively a material demonstration of power. Later authors, such as Glenn Snyder, have further elaborated on the distinction between deterrence and coercion, as well as the role of credibility and interest in the sustainability of deterrent relationships (Snyder, 1961).

Within the classical theory, the division into deterrence by punishment and deterrence by denial is particularly significant (Freedman, 2004). The first form involves the ability and willingness to impose unacceptable costs on the aggressor after the aggression has been committed, while the second aims to make aggression unprofitable or infeasible in advance by strengthening defenses and reducing the probability of success of the attack. However, both forms are present in classical theory; deterrence by punishment dominated during the Cold War, primarily in the nuclear domain.

2.2. Limitations of classical theory in the modern security environment

With the end of the Cold War and the transformation of the international system, it has become increasingly clear that the classical theory of deterrence has significant limitations. Contemporary conflicts rarely unfold as open, high-intensity interstate wars. They are increasingly realized through a complex network of interactions that take the form of protracted, fragmented, and hybrid confrontations below the threshold of formal war. In such conditions, the clear lines between peace and war, as well as between military and non-military instruments, become blurred.

One of the key challenges to classical deterrence is the emergence of multi-domain warfare, in which actions take place simultaneously in land, sea, air, cyber, and information space (Hew, 2013). In addition, the rise of non-state actors plays a significant role, whose behavior often does not fit the rationalist models on which classical deterrence theory is based. These actors may have diffuse decision-making structures, asymmetric goals, and limited sensitivity to classical forms of punishment.

Additionally, contemporary "gray zone" strategies allow actors to avoid activating classical deterrence mechanisms through gradual and incremental action. As Michael J. Mazarr points out, such activities are designed to fall below the threshold that would justify a strong response, thereby undermining the credibility of traditional deterrence threats (Mazarr, 2015). In this sense, deterrence can no longer be understood as a stable state, but as a dynamic and contextually conditioned process.

2.3. Multi-Actor Deterrence as an Expanded Analytical Framework

In response to these changes, attempts to expand the concept of deterrence beyond the narrow state-centric framework are increasingly appearing in contemporary literature. Multi-actor deterrence is based on the assumption that the decisions of a potential aggressor are not influenced exclusively by a single state actor, but by a network of different actors and domains of action whose effects intertwine and multiply.

In this sense, deterrence can be viewed as a network phenomenon in which states, alliances, international institutions, economic and technological actors, as well as social and cognitive factors, jointly shape the perception of risk and costs. This understanding of deterrence is close to the concepts of "integrated deterrence" and "cross-domain deterrence", which emphasize the need for coordination among different instruments of power and actors to achieve a cumulative effect (Ochmanek et al., 2017).

Unlike the classical model, multi-actor deterrence does not necessarily imply a clearly articulated threat or centralized control over all actors. On the contrary, its effectiveness often stems from the very complexity and uncertainty it creates for a potential aggressor. This characteristic makes multi-actor deterrence particularly relevant for small states. Which, rather than relying on the limited

capacities of classical military force, may seek to network different actors and domains in order to increase the costs and risks of aggressive action against them.

Modern deterrence cannot be understood without insight into the multi-domain environment in which it is implemented. The military, political, economic, informational, and cognitive domains are intertwined, meaning that actions in one domain produce effects in others. This inter-domain dynamic further complicates the deterrence process and increases the importance of coordinating different instruments of power. Modern research indicates that the application of artificial intelligence significantly improves the coordination of responses in complex crises (Ocal & Torun, 2025). Of particular importance is the information domain, in which perceptions, legitimacy, and interpretations of actor behavior are shaped. In this sense, strategic communications and information operations become the central element of multi-actor deterrence, rather than its accompanying segment.

Table 1. Actors and effects in multi-domain deterrence

Actor Type	Examples of actors	Key Domain	Basic instrument	Deterrence effect
State	Government, armed forces, diplomacy	Political / Legal	Diplomatic and legal mechanisms	Increase in political costs
Non-State	Media, NGOs, academia, diaspora	Informational	Narratives and public visibility	Perceived increase in costs
Corporate	Companies, technology platforms	Economic / Technological	Investments, institutional decisions	Increase in economic costs
International	UN, EU, OSCE	Normative	Institutional pressure	Increase in legitimacy costs

Table 1 presents multi-actor deterrence as an analytical framework in which different categories of actors, through different domains of action, cumulatively produce political, perceptual, and economic and legitimacy costs of escalation. Essentially, it shows the categories of actors in multi-domain deterrence and their cumulative impact on the costs and risk perception of potential aggressors. Deterrence effects on the listed categories of actors are produced through a cause-and-effect logic: actions in a specific domain (political, economic, informational, or normative) activate mechanisms that increase the costs, uncertainty, or risk of a potential aggressor. For example, political-legal instruments of state actors signal international legitimacy and legal consequences; informational instruments of non-state actors shape public perception; and economic-technological instruments of corporate actors increase the material and operational costs of undesirable actions.

The uniqueness of the concept of multi-actor deterrence in this paper emphasizes the plurality of actors (state, non-state, and corporate) and the diffusion of responsibilities across multiple domains, to shape the risk perception of a potential aggressor. Unlike integrated or cross-domain deterrence, the focus is not only on the coordination of instruments or the networking of domains, but on the interaction of multiple actors, which produces a cumulative deterrent effect. The concept begins with the identification of relevant actors and domains and ends with an increase in uncertainty, costs, and political risk, without the direct use of force.

3. Small states and the logic of multi-actor deterrence

The importance of adaptive and unconventional models of deterrence for small states has been confirmed in recent academic debates, including the international conference Defense Strategies of Small States and Smaller Forces held in 2025, which emphasized that limited resources encourage the development of innovative, multi-domain, and multi-actor approaches to defense (SSU, 2025). In addition to the above, special discussions were held on the contemporary defense adaptations of small states, which support the thesis that they develop innovative models of deterrence in the absence of military force dominance. However, before we consider this concept through the lens of small states, it is necessary to formalize it. Namely, multi-actor deterrence is the process of strategically shaping the behavior of potential adversaries in a complex security environment. In which multiple state and non-state actors of different levels of power and rationality participate, through the coordinated use of military, political, economic, informational, and normative instruments, to

prevent undesirable actions below and above the threshold of armed conflict (Black & Obradovic, 2022). Key features of this concept are the plurality of actors, the diffusion of responsibility, the multi-domain nature of action, and the primacy of perception over material capacities. Unlike classical deterrence, where the relationship between the deterrent and the deterred is relatively clear, multi-actor deterrence operates as a network of interactions in which roles are often fluid.

A particular challenge with this concept is identifying actors. Within multi-actor deterrence, three basic categories of actors can be identified: primary state actors and alliances, secondary non-state and proxy actors, and structural actors that shape the normative and informational context. This typology indicates that deterrence does not operate exclusively through direct power relations, but also through indirect mechanisms of influence.

In addition to the above, it is necessary to define appropriate mechanisms and instruments of action. In addition to the classic mechanisms of punishment and deprivation, multi-actor deterrence also includes deterrence through interdependence, legitimacy, and strategic ambiguity. Economic connectivity, legal regimes, and dominant narratives become means of increasing the costs of undesirable behavior for potential adversaries. The three previously mentioned segments related to the definition, selection of actors, mechanisms, and instruments are also a starting point for further analysis in the context of small states.

3.1. Structural constraints of small states in classical deterrence

In international relations theory, small states are traditionally defined primarily by their limited material capacities and limited influence on the structure of the international system. In the context of classical deterrence theory, these characteristics produce clear structural limitations: an inability to impose unacceptable costs on a potential aggressor, limited ability to escalate dominance, and dependence on external security guarantees (Keohane, 1969). As a consequence, small states are most often treated in classical models of deterrence as objects of deterrence, rather than as autonomous subjects that actively shape relations in the deterrence process.

Maria Keinonen argues that small states can strengthen their deterrence through national factors, such as strong defense and societal resilience, as well as international factors, such as military and political alliances. Limited resources and low international status can translate into national deterrent advantages, while the political intentions and historical practices of potential aggressors act as international deterrent factors that shape decisions and enhance the deterrent effect (Keinonen, 2024).

In addition to material constraints, small states also face significant political and strategic risks. Any reliance on deterrence through punishment carries the risk of uncontrolled escalation, in which the small state lacks the capacity to manage the conflict's dynamics. As a result, classical deterrence strategies are often either unavailable or strategically unsustainable for small states, further reinforcing the importance of alternative approaches.

3.2. From deterrence by force to deterrence by complexity

The contemporary security environment, marked by hybrid threats and gray-area operations, opens space for a different logic of deterrence for small states. Instead of relying on the threat of punishment, deterrence by deprivation, which aims to make aggression slow, costly, and uncertain, is gaining increasing importance (Freedman, 2004). This form of deterrence does not require symmetry of capacity, but the ability to deny the adversary a quick and clear success.

In this context, the concept of "deterrence through complexity" emerges, which implies a deliberate increase in the institutional, social, legal, and operational complexity of the environment in which potential aggression would have to be implemented. As Lawrence Freedman points out, contemporary deterrence relies less and less on a single dominant threat, more and more on the cumulative effect of various, often indirect, mechanisms of influence (Freedman, 2013). For small states,

this logic represents a rational strategic adaptation, as it allows them to maximize the deterrent effect while minimizing confrontation.

One of the significant factors shaping and complicating contemporary concepts of deterrence is the development of technology such as artificial intelligence. Dingil (Hurşit Dingil) shows that artificial intelligence transforms traditional, state-centric models of deterrence, extending them to a multi-actor environment in which non-state and corporate actors play a significant role (Dingil, 2025). Artificial intelligence acts as a strategic power multiplier, but it also increases the risk of destabilization and miscalculations. Therefore, effective deterrence increasingly relies on multilateral governance mechanisms and institutional coordination between different actors.

3.3. Network logic and multi-actor deterrence

Multi-actor deterrence is a logical continuation of this evolution. Instead of a centralized, state-exclusive model, deterrence is viewed as the result of the interaction among multiple actors deployed across different domains. Among other things, the modern security ecosystem is characterized by the growing role of private military actors (Vračević, 2025). These actors do not have to act in sync or under a unified command to produce a deterrent effect; it suffices that their mere existence and potential actions increase a potential aggressor's perception of risk and uncertainty.

The literature on small states suggests that networking with alliances, international institutions, economic and technological partners, and non-state actors is a key mechanism for compensating for structural weaknesses (Thorhallsson, 2012). In this sense, a small state can function as a "node" in a wider network of security relations, the significance of which does not derive from the concentration of force, but from position and connectivity.

Contemporary conflicts increasingly involve military actors in roles beyond classic combat tasks (Popović Mančević, 2025). More recent analytical models of non-kinetic deterrence suggest that instruments such as institutional signals, economic interdependencies, and normative positioning can have a stabilizing deterrent effect, especially in environments where the use of military force is limited or politically risky (Meng, 2025).

3.4. Comparative insights: experiences of small states

Empirical insights from the practice of several small states further support the relevance of multi-actor deterrence. Finland and Estonia have developed concepts of comprehensive and total defense, which integrate military, civilian, economic, and information capabilities into a single resilience system (Järvenpää, Major, & Sakkov, 2019). Singapore, on the other hand, combines limited territorial depth with highly developed institutional and technological complexity, thereby significantly increasing the costs of any external pressure (Matthews & Timur, 2023).

The common characteristic of these examples is not the size of the armed forces, but rather the state's ability to mobilize and coordinate a wide range of actors and domains of action. This is precisely the essence of multi-actor deterrence of small states: deterrence is not achieved with a single blow or a single threat, but through the permanent creation of an environment in which aggression becomes politically, operationally, and socially unprofitable.

These insights provide a necessary analytical bridge to the case of the Republic of Serbia. An analysis of Serbia's strategic and security context is a prerequisite for understanding how the logic of multi-actor deterrence can be, and to some extent is, applied within its specific geopolitical and normative framework.

4. Case study: Republic of Serbia

Serbia's geopolitical position, historical experience of multi-layered foreign policy pressures, and commitment to military neutrality position it as a pivotal actor in a multi-actor deterrence system (Glišin, 2025). As a state located at the intersection of the interests of several major and regional powers, Serbia simultaneously receives, interprets, and sends signals to various centers of power, without formal allied obligations that would define its behavior in advance (Gajić, 2023). In this sense, its role is not passive but mediating and adaptive, with deterrence achieved through the management of perceptions, uncertainty, and spaces for maneuver in a complex security environment.

The concept of deterrence of the Republic of Serbia relies on a combination of limited but credible military capabilities, active and balanced diplomacy, normative legalism, and controlled information-narrative strategies. Unlike the classical logic of deterrence based on the threat of force, the Serbian deterrence model focuses on the production of political, perceptual, and legal costs for actors who would opt for escalation. Of particular importance is the consistent emphasis on respect for international law and the status quo, which is a key element of national security strategies that thoroughly analyze military neutrality and cooperation as instruments for achieving the national interests of the Republic of Serbia (Ćurčić & Dinić, 2024). This expanded understanding of deterrence shifts the focus from the narrow military domain to the broader political and social space.

At the same time, the implementation of this approach is accompanied by significant structural challenges and paradoxes of military neutrality. Although neutrality reduces the risk of automatic involvement in great-power conflicts, it increases the need for sophisticated signal management, credibility, and alignment with external actors' expectations. In a multi-actor environment, Serbia's deterrence does not rest on superior force, but on the ability to influence the calculations of others through a combination of strategic restraint, selective assertiveness, and sustained diplomatic activity, which makes this model sensitive, but also potentially effective in conditions of limited resources (Lekić, 2017).

Viewed in light of the modern concept of deterrence, as well as the multi-actor deterrence in question, Serbia's position can be interpreted as an example of a small state that deters not by concentrating force but by managing a network of relationships, expectations, and institutional constraints. Military neutrality can be considered as a starting point. Serbia officially practices military neutrality as the basis of its foreign and security policy. Military neutrality has a normative aspect, grounded in national legal acts and international law, and a political aspect, as it allows Serbia to maneuver among different global actors and blocs.

From Serbia's perspective, as well as that of other small countries, it is important to distinguish neutrality from isolation. While isolation implies distancing from international processes and weakening state capacities, neutrality is an active stance that requires deterrence, diplomatic flexibility, and participation in regional security initiatives, such as partnerships with NATO through the Partnership for Peace. As an example, Serbia participates in multinational exercises with NATO partners while maintaining military and economic relations with the Russian Federation and the People's Republic of China, showing that neutrality is not a passive policy.

One factor that may be of great importance is Serbia's geopolitical hub in the Balkan environment. It is expressed in the position of the Balkan "geopolitical cross" in the "sensitive intersecting zone", which was formed centuries ago, in the field of aggressive geopolitical action outside the Balkan political factors (states and alliances), as a zone of their violent infiltration (Despotović, 2010). As previously stated, Serbia is located in the geopolitical hub of the Balkans, a region that represents a contact zone for major actors. The presence of several global and regional powers - the EU, the USA, the Russian Federation, the People's Republic of China, and Turkey - creates a dynamic environment in which every decision has effects in multiple domains. For example, China's investments in infrastructure, US diplomatic pressure on the issue of Kosovo and Metohija, and EU integration processes require Serbia to maintain credibility and flexibility simultaneously in a multi-actor environment. Serbia's specific geopolitical position allows it to act as a mediator, but also requires constant risk management from pressures.

4.1. Threat perception

Modern threats include a range of hybrid and information-based components that operate below the threshold of armed conflict and may pose a threat to national security. As a small country, Serbia is not immune to these threats. Threat perception in Serbia can be grouped into three main categories.

The first group of threats is cyber and critical infrastructure. Threats include hacker attacks on state systems, energy, and telecommunications infrastructure. Such incidents can disrupt state functions and cause significant economic and security consequences. These threats include cyber-attacks on critical infrastructure and state systems, which can disrupt the functioning of basic social and economic resources. Another form of threat manifestation is most often disinformation campaigns and the manipulation of media narratives, which affect the public's beliefs and institutional capacity for decision-making. The last example is economic and political pressures from great powers. These often manifest as economic dependence, conditionality, and foreign policy pressures that undermine institutional stability.

An example is research on the economic aspects of cybersecurity. Vidović and Beriša show that cyberattacks have direct socio-financial consequences that materialize outside the digital space, including jeopardizing the functioning of critical infrastructure and financial flows within the national economy (Vidović & Beriša, 2025). This is precisely why the development and strengthening of information and cybersecurity capacities have become a priority in Serbia, which implies institutional coordination and the ability to respond not only to the technological but also to the structural implications of such attacks (Stošić & Janković, 2022).

The second group of threats comprises informational influences. Disinformation, propaganda, and manipulation of public opinion can affect political stability and the perception of legitimacy of state institutions. Controlled media narratives and diplomatic channels attempt to mitigate this effect. Disinformation and propaganda narratives, as part of broader informational threats, can undermine trust in institutions and the useful functioning of democratic processes. Studies in the regional and international contexts indicate that hybrid operations include media manipulation as a means of political influence, which requires a prolonged, multi-actor response (Kuçi, 2024). A similar principle can be applied to Serbia, which is a significant regional actor in the Balkans.

The third group of threats comprises economic and political influence. Threats come through economic sanctions, energy dependence, or pressure from international actors. Serbia perceives them as a challenge to maintaining strategic autonomy and pragmatic positioning. In addition, economic and political pressures from great powers, whether through economic dependence, investment ties, or political conditionality, represent a powerful instrument in hybrid strategies that operate below the threshold of military conflict and can have serious implications for institutional stability and national autonomy. This is in line with a broader security approach that recognizes that security is achieved not only through military resilience, but also through economic resilience and social stability. In addition, resilience is generally conceptualized as a multidimensional system that encompasses institutional, technological, and social capacities (Milenković & Cvetković, 2025).

Therefore, Serbia perceives these threats as a direct challenge to national security and institutional stability, requiring the development of a multi-actor deterrence system that combines state, private, and civilian capacities. In addition, modern approaches increasingly emphasize the need to integrate defense studies and disaster risk reduction into a single security framework (Roković & Dimitrijević, 2025). Such a system includes strengthening cyber resilience, legal and regulatory frameworks, public diplomacy, and strategic communications that aim to reduce vulnerability to information and economic pressures, while building society's capacities to respond to complex and asymmetric threats.

4.2. Actors

In the context of the Republic of Serbia, it is possible to distinguish several actors in the concept of multi-domain deterrence: state, non-state, and societal actors. The main carriers of multi-actor deterrence in the Republic of Serbia are state actors, primarily the Serbian Armed Forces, security institutions, and the diplomatic network. The Serbian Armed Forces are a key element of deterrence, underpinned by a defense concept aimed at protecting territorial integrity and responding to crises in the immediate environment. Its capabilities to operate across multiple domains, including cyber and information space, enable limited but credible responses to hybrid threats, thereby contributing to deterrence without relying on the classical superiority of force. In addition, security institutions integrate intelligence, police, and civilian capacities, thereby strengthening the preventive dimension of deterrence and enabling early recognition and neutralization of threats below the threshold of armed conflict. Serbia's diplomatic network also plays a significant role, enabling flexible management of multi-vector relations, especially regarding key issues such as Kosovo and Metohija, regional stability, and energy security.

In addition to state structures, non-state and societal actors also make a significant contribution to multi-actor deterrence in Serbia. The academic and expert community helps shape security policies through analyses, studies, and public expertise, thereby indirectly influencing the quality of strategic decision-making and increasing the rationality of responses to complex threats. The media and information space plays a special role in shaping deterrence signals, as it influences public perception and external actors alike, thereby bringing deterrence into the domain of strategic communications. At the same time, the information sector and national cyber capabilities represent a key line of defense against cyberattacks on critical infrastructure and institutional systems, acting both preventively and reactively. The diaspora, as a specific social actor, can act as an external multiplier of Serbia's influence, especially in diplomatic, economic, and informational processes, thereby expanding the reach of national deterrence beyond formal state channels.

The interaction of state and non-state actors represents the essence of the multidomain logic in Serbia's multi-actor deterrence system. It is precisely through this synergy that the political and operational costs of potential aggression increase, thereby reducing the cost-effectiveness of hybrid and indirect actions against the state. Instead of positioning itself as a frontline actor in the confrontation with great powers, Serbia, through coordinated actions by various actors, positions itself as a "node" in the regional and broader security environment. Such an approach allows the maintenance of deterrence credibility without the need for symmetrical military superiority, relying on a combination of institutional resilience, social cohesion, and active perception management. Multi-actor deterrence thus appears as an adaptive, contextually responsive model of security for a small state in conditions of limited resources and formal military neutrality.

In the Serbian context, multi-actor deterrence operates through fragmented but recognizable coordination paths. State actors, namely the Ministry of Defense, the Ministry of Foreign Affairs, and the National Security Council, integrate political and legal instruments. In contrast, non-state and corporate actors (energy and technology companies, media actors) contribute technical and cognitive signals. International actors and partners operate through formal and informal mechanisms of consultation and advice. The governance mechanism is partly centralized (through state coordinators), but in practice is fragmented, reflecting the limitations of small, neutral states in a multi-actor environment and confirming the need for strategic pragmatism.

In addition, in the case of Serbia, multi-actor deterrence manifests itself through multiple domains and actors. First, legal and normative signaling is realized through the adoption of defense strategies and participation in international agreements, which indicates to potential aggressors an institutionally regulated and predictable environment. Second, diplomatic channels and media narratives are used to convey clear messages about interests and readiness to coordinate with alliances and partners; an example is diplomatic contacts with NATO members and simultaneous public communication about the policy of military neutrality. Third, cyber capabilities and corporate partnerships serve as an indirect deterrent, as modern IT systems, together with technology companies and institutional platforms, increase the costs of potential hybrid attacks and prevent information

manipulation. These examples show how different actors and domains, through concrete and verifiable activities, produce a cumulative deterrent effect in a complex security environment.

4.3. Limitations and risks of multi-actor deterrence in the case of Serbia

It is particularly important to consider the limitations and risks of applying this concept to small states, including Serbia. The multi-actor approach to deterrence faces several challenges in small states. Coordination challenges and capacity asymmetry can be particularly highlighted here. Namely, multi-actor deterrence involves interactions among multiple state and non-state actors, often leading to coordination problems in implementing the strategy. Institutional fragmentation and the diversity of competencies slow the decision-making process and can cause delays in responding to crises, especially in the case of cyberattacks or information overload. In addition, the asymmetry in actors' capacities, where some have significant resources and expertise. In contrast, others have limited ability to act, can result in uneven implementation of the strategy, reducing its credibility and influence with potential adversaries. These coordination challenges underscore the need for clear governance mechanisms, standardized procedures, and ongoing dialogue among all relevant actors for multi-actor deterrence to be effective.

Contemporary threats to Serbia's national security, including cyberattacks, information influence strategies, and economic and political pressures, are increasingly viewed as part of a hybrid threat that requires an integrated, multi-actor response from state and non-state actors. Academic analysis indicates that modern threats encompass "non-military threats and hybrid components" that are inextricably linked to the functioning of the national security system and require broad coordination of capacities in order to effectively counter them (Lović & Stojanović, 2024).

Another significant segment comprises the risks of instrumentalization and external pressures. In addition to internal coordination challenges, multi-actor deterrence in Serbia carries the risk of instrumentalization by non-state actors. When the academic community, media, information sector or diaspora act independently or are influenced by external actors, there may be a loss of control over initiatives and questions of legitimacy of these activities. At the same time, Serbia faces external pressures from great powers that seek to reduce the state's room for maneuver and to binarize its choices of political or economic orientation. These factors reduce the flexibility of the multi-actor approach and require careful coordination of state and non-state actors to maintain deterrence as credible, adapted to the context, and resistant to instrumentalization or political pressures.

Finally, we can divide constraints into internal and external. Internal constraints arise from fragmented coordination and differing capacities among state and non-state actors, thereby reducing the effectiveness and consistency of deterrence measures. Also, legitimacy issues and incoherent messaging can undermine the perception of deterrence signals, which require clear lines of accountability, regular synchronization mechanisms, and coordinated strategic communication.

External constraints include pressures to take sides, the influence of intermediaries, and economic dependence, which can narrow the room for maneuver. Mitigating them involves a multi-vector diplomatic approach, clear frameworks for cooperation, and diversification of sources to maintain flexibility and deterrence effectiveness.

5. Conclusion

The contemporary international security environment requires small states such as Serbia to adapt classical deterrence models to multi-actor and multi-domain forms. Serbia does not rely on the symmetry of force or formal allied guarantees for its security, but rather develops a network of state and non-state actors that influence the risk calculation of potential adversaries. This strategy of multi-actor deterrence allows for increasing the costs of undesirable behavior, managing uncertainty, and maintaining strategic maneuver space in conditions of military neutrality. The paper confirmed the hypothesis that Serbia, as a small and militarily neutral state, achieves a deterrent effect

through a combination of state and non-state actors, the networking of different domains of action, and the strategic shaping of the perception of risk among potential aggressors.

The analysis shows that small states can achieve deterrence through multi-actor and multi-domain strategies that do not rely solely on military superiority. Key elements include:

- Increasing the complexity of the security environment;
- Coordination of state and non-state actors;
- Strategic pragmatism and networking in international institutions.

The multi-actor approach shows that deterrence is no longer a linear process between two powers, but a dynamic and contextually conditioned phenomenon in which institutional complexity, perception and coordination of different domains play an important role. At the same time, this logic fosters structural fragmentation, the potential instrumentalization of non-state actors, and external pressures that require constant attention and flexibility in strategic planning.

The application of multi-actor deterrence in the case of Serbia points to a new model of adaptive, complex, and networked deterrence that could serve as an analytical framework for other small states in multipolar and hybrid security environments. The key conclusion is that the effectiveness of small states' deterrence does not stem solely from the amount of force, but from the ability to manage the complexity of the environment, institutional capacities, and risk perception.

6. References

1. Baev, P., Marsh, N., & Martins, B. (2025). Distributed deterrence: Europe's new security logic and action plan. PRIO Policy Brief, 4. Преузето са https://cdn.cloud.prio.org/files/592ba438-863d-4237-8831-e7a9aa4245f2/PRIO%20Policy%20Brief%204%202025.pdf?inline=true
2. Beriša, H., Cvetković, V., & Pavić, A. (2024). Implications of Artificial Intelligence and Cyberspace on Risk Management Capabilities. International Journal of Disaster Risk Management, 6(2), 279-295. doi:http://dx.doi.org/10.18485/ijdrm.2024.6.2.18
3. Black, M., & Obradovic, L. (2022). Multi-actor deterrence: defining the concept. Aether (Maxwell Air Force Base Ala), 1(2), 69-80. Downloaded https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-1_Issue-2/Black.pdf
4. Ćurčić, M., & Dinić, J. (2024). Vojna neutralnost i saradnja kao instrumenti za ostvarivanje nacionalnog interesa Republike Srbije. Politika nacionalne bezbednosti, 27(2), 159-181. doi:https://doi.org/10.5937/pnb27-50341
5. Cvetković, V. M., & Šišović, V. (2024). Understanding the Sustainable Development of Community (Social) Disaster Resilience in Serbia: Demographic and Socio-Economic Impacts. Sustainability, 16(7), 2620.
6. Cvetković, V. M., Gole, S., Renner, R., Jakovljević, V., & Lukić, T. (2024). Qualitative insights into cultural heritage protection in Serbia: Addressing legal and institutional gaps for disaster risk resilience. Open Geosciences, 16(1), 20220755
7. Cvetković, V. M., Lipovac, M., Renner, R., Stanarević, S., & Raonić, Z. (2025). A Predictive Framework for Understanding Multidimensional Security Perceptions Among Students in Serbia: The Role of Institutional, Socio-Economic, and Demographic Determinants of Sustainability. Sustainability, 17(11), 5030.
8. Cvetković, V. M., Renner, R., & Jakovljević, V. (2024). Industrial Disasters and Hazards: From Causes to Consequences—A Holistic Approach to Resilience. International Journal of Disaster Risk Management, 6(2), 149–168.
9. Cvetković, V., Čvorović, M., & Beriša, H. (2023a). The Gender Dimension of Vulnerability in Disaster Caused by the Coronavirus (COVID-19). NBP, 28(2), 32-54.
10. Cvetković, V., Radovanović, M., Milašinović, S. (2021). Disaster Risk Communication: Attitudes of Serbian Citizens. Sociological Review, 55 (4), 1610-1647.

11. Cvetković, V.M., Tanasić, J., Ocal, A., Živković-Šulović, M., Ćurić, N., Milojević, S., Knežević, S. (2023). The Assessment of Public Health Capacities at Local Self-Governments in Serbia. Lex Localis, 21(4), 1201-1234.
12. Despotović, L. (2010). Obeležja geopolitičkog položaja Srbije i srpskih zemalja u kontekstu aktuelnih procesa balkanizacije. Sociološki pregled, 44(4), 541-566.
13. Dingil, H. (2025). Reshaping National Security and the Future of Warfare in the Age of Competitive Artificial Intelligence. Insight Turkey, 27(2), 413–420. doi:https://doi.org/10.25253/99.2025272.21
14. Freedman, L. (2004). Deterrence. Wiley.
15. Freedman, L. (2013). Strategy: A History. London: Oxford University Press.
16. Fukuda, J. (2024). War 3.0: the Rapid Change of Warfare - Deepening Deterrence in the New (Space and Cyber) Domains. Tokyo: The Sasakawa Peace Foundation. Преузето са https://www.spf.org/en/global-data/user224/war30therapidchangeofwarfare.pdf
17. Gajić, A. (2023). Geopolitički položaj Srbije nakon otpočinjanja rata u Ukrajini - neutralnost i strateško odvraćanje u kriznom kontekstu. Srpska politička misao, 80(2), 53-74. doi:https://doi.org/10.5937/spm80-44267
18. Glišin, V. (2025). Geopolitička obeležja položaja Srbije i srpskog naroda u savremenim međunarodnim odnosima. Napredak - časopis za političku teoriju i praksu, 6(2), 103-124. doi:https://doi.org/10.5937/napredak6-59395
19. Hew, S. (2013). The Direction of War: Contemporary Strategy in Historical Perspective. Cambridge: Cambridge University Press.
20. Järvenpää, P., Major, C., & Sakkov, S. (2019). Comprehensive Security in Finland. Helsinki: National Defence University.
21. Keinonen, M. (2024). Deterrence strategies for a small state: Analysis and survey. Journal of Military Studies, 13(1), 67-77. doi:https://doi.org/10.2478/jms-2024-0006
22. Keohane, R. (1969). Lilliputians' Dilemmas: Small States in International Politics. International Organization, 23(2), 291–310.
23. Kuçi, G. (2024). Russia's hybrid warfare in the western Balkans: geopolitical strategies and proxy actors. Octopus Journal: Hybrid Warfare & Strategic Conflicts, 3(27). doi:https://doi.org/10.69921/29031991
24. Lekić, S. (2017). Neutrality of Serbia and new geopolitical reality. Vojno delo, 69(3), 63 – 73. doi:https://doi.org/10.5937/vojdelo17030631
25. Lović, V., & Stojanović, M. (2024). The relation of the national security system of the Republic of Serbia to modern hybrid threats. Megatrend revija, 21(2), 135-152. doi:https://doi.org/10.5937/MegRev2402135L
26. Matthews, R., & Timur, F. B. (2023). Singapore's 'Total Defence' Strategy. Defence and Peace Economics, 35(1), 1-21. doi:https://doi.org/10.1080/10242694.2023.2187924
27. Mazarr, M. (2015). Mastering the Gray Zone: Understanding a Changing Era of Conflict. US Army War College Press.
28. Mazarr, M. (2018). Understanding Deterrence. Santa Monica, CA: RAND Corporation.
29. Meng, W. (2025). Expert Insight-Based Modeling Of Non-Kinetic Strategic Deterrence Of Rare Earth Supply Disruption: A Simulation-Driven Systematic Framework. International Journal of Environmental Sciences, 11(7), 1137-1152. doi:https://doi.org/10.64252/9tsfta55
30. Milenković, D. (2025). Theoretical, institutional and organizational aspects of the integrated disaster risk reduction system: Towards a deeper understanding of disaster resilience in Serbia. International Journal of Contemporary Security Studies, 1(1), 175–189. doi:https://doi.org/10.18485/fb_ijcss.2025.1.1.13
31. Milenković, D., & Cvetković, V. (2025). Rethinking Disaster Resilience: Conceptual Framework, Core Dimensions, and Key Actors. International Journal of Disaster Risk Management, 7(2), 455–468. doi:https://doi.org/10.18485/ijdrm.2025.7.2.25

32. Milenković, D., & Cvetković, V. M. (2025). Rethinking Disaster Resilience: Conceptual Framework, Core Dimensions, and Key Actors. International Journal of Disaster Risk Management, 7(2), 455–468.
33. Nikolić, N., Cvetković, V. M., Renner, R., Cvijović, N., & Gačić, J. (2025). Disaster Risk Perception and Local Resilience near the 'Duboko' Landfill: Challenges of Governance, Management, Trust, and Environmental Communication in Serbia. Open Geosciences, 17(1): 20250850.
34. Ocal, F., & Torun, S. (2025). Leveraging Artificial Intelligence for Enhanced Disaster Response Coordination. International Journal of Disaster Risk Management, 7(1), 235–246. doi:https://doi.org/10.18485/ijdrm.2025.7.1.13
35. Ochmanek, D., Wilson, P., Allen, B., Meyers, J., & Price, C. (2017). U.S. Military Capabilities and Forces for a Dangerous World. Santa Monica, CA: RAND Corporation. Преузето са https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1782-1/RAND_RR1782-1.pdf
36. Pavić, A., & Beriša, H. (2025). Strategic pragmaticity as a factor in achieving serbia's national interests. Serbian Political Thought, 92(4), 25-49. doi:https://doi.org/10.5937/spm92-59186
37. Popović-Mančević, M. (2025). Non-Traditional Roles of Military Actors: NATO's Engagement in Natural Disaster Response. International Journal of Contemporary Security Studies, 1(1), 75–84. doi:https://doi.org/10.18485/fb_ijcss.2025.1.1.6
38. Roković, V., & Dimitrijević, I. (2025). Bridging Defense Studies and Disaster Risk Reduction: Comparative Perspectives from the Former Yugoslavia. International Journal of Disaster Risk Management, 7(2), 65–86. doi:https://doi.org/10.18485/ijdrm.2025.7.2.5
39. Schelling, T. C. (1960). The Strategy of Conflict. Cambridge: Harvard UP.
40. Snyder, G. (1961). Deterrence and Defense: Toward a Theory of National Security. Princeton, NJ: Princeton University Press.
41. SSU, S. S. (2025, February 23). Defence Strategies of Small States and Smaller Forces. Преузето January 19, 2026 са Arab Center for Research and Policy Studies: https://www.dohainstitute.org/en/News/Pages/the-defence-strategies-of-small-states-and-smaller-forces-ar.aspx
42. Stošić, L., & Janković, A. (2022). Cybercrime in the Republic of Serbia: prevalence, situation and perspectives. Kultura polisa, 19(4), 82–99. doi:https://doi.org/10.51738/Kpolisa2022.19.4r.82sj
43. Thorhallsson, B. (2012). Small States in the UN Security Council: Means of Influence? The Hague Journal of Diplomacy, 7(2), 135–160.
44. Vidović, N., & Beriša, H. (2025). Economic Aspects of Cyber Security: Socio-Financial Consequences of Cyber Attacks. International Journal of Contemporary Security Studies, 1(1), 149–162. doi:https://doi.org/10.18485/fb_ijcss.2025.1.1.11
45. Vidović, N., Cvetković, V., Beriša, H., & Milašinović, S. (2025). Understanding Ransomware Through the Lens of Disaster Risk: Implications for Cybersecurity and Economic Stability. International Journal of Disaster Risk Management, 7(1), 247–264. doi:https://doi.org/10.18485/ijdrm.2025.7.1.141
46. Vračević, N. (2025). Strategic Roles of Private Military Companies: The Evolution and Privatization of Warfare in the Context of Contemporary Global Conflicts. International Journal of Contemporary Security Studies, 1(1), 163–174. doi:https://doi.org/10.18485/fb_ijcss.2025.1.1.12