

Special Operations Forces as an Instrument of Democratic State Defence in Hybrid Conflict

Vladimír ANDRASSY¹, Martin STANKO^{1*}

¹Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 03101 Liptovský Mikuláš, Slovak Republic

Correspondence: *martin.stanko@protonmail.com

Abstract

This paper examines the role of Special Operations Forces (SOF) in countering hybrid threats within democratic states, focusing on the Slovak Republic as a front-line NATO member. Using qualitative historical-comparative analysis and a review of security doctrines, the study demonstrates that SOF enable effective operations below the threshold of open armed conflict. The central hypothesis posits that SOF effectiveness is not independent of democratic governance but fundamentally dependent upon it: public trust, legal accountability, and robust parliamentary oversight are prerequisites for operational legitimacy. The paper identifies the "Democratic Dilemma" – the tension between operational secrecy and democratic transparency – and proposes a "Democratic Hybrid Defence" model in which oversight and effectiveness are mutually reinforcing. The study contributes to the field by explicitly linking SOF capabilities with civilian control mechanisms in a Central European geopolitical context.

KEY WORDS: *Special Operations Forces, Hybrid Conflict, Democratic State, Civil-Military Relations, National Resilience, Oversight, Gray Zone.*

Citation: Andrassy, V.; Stanko, M. Special Operations Forces as an Instrument of Democratic State Defence in Hybrid Conflict. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 2026. ISSN 2538-8959, <https://doi.org/10.47459/cndcgs.2026.83>

1. Introduction

The 21st century has brought fundamental changes to the security environment, characterised by increasing instability, unpredictability, and heightened tensions in strategically key regions [1]. The dynamic development of the security situation is conditioned by the synergy of ongoing kinetic conflicts and the emergence of sophisticated, non-kinetic threats that directly attack the stability and integrity of democratic actors. In response, democratic states primarily within NATO and the EU must continuously increase their preparedness and resilience to the entire spectrum of modern challenges [2]. The international security order has shifted from the predictable binary structure of the Cold War to a state of permanent "strategic competition" where the boundaries between war and peace are deliberately blurred [3]. In this "gray zone," adversaries synchronously combine multiple instruments of power to achieve strategic goals while purposefully operating below the threshold of open armed conflict [4].

One of the most pressing strategic challenges of our era is the concept of the "weaponisation of everything," where information, economics, energy, and law each serve as vectors of hybrid aggression [5]. According to Frank Hoffman's foundational definition, hybrid wars represent a multimodal strategy integrating conventional, unconventional, and terrorist capabilities simultaneously and in a synchronised manner [6]. This erosion of established borders between domains creates critical vulnerabilities for democratic institutions, which are traditionally structured on a strict separation of internal and external security. Actors such as Russia and China exploit the openness of democratic systems – abusing transparency, judicial processes, and information freedoms – to degrade national resilience from within. Against this backdrop, Special Operations Forces (SOF) emerge as one of the most agile and adaptively suited instruments for the defence of democratic countries in the contemporary security environment.

1.1 Research Problem and Hypothesis

The "Democratic Dilemma" at the core of this study involves a structural tension: the secrecy and speed required to defeat hybrid aggression stand in direct conflict with democratic requirements for transparency, accountability, and oversight. SOF embody this conflict most acutely, as their operational effectiveness relies on low visibility, while

democratic legitimacy demands rigorous legal accountability and public trust. Failure to adapt SOF risks being outpaced by autocratic adversaries who face no such governance constraints. Conversely, adopting autocratic methods of operation without oversight risks eroding the very democratic order that SOF are tasked to protect.

The central hypothesis of this study is therefore: SOF constitute an indispensable, yet contextually conditioned, instrument of democratic defence in hybrid conflict. Their effectiveness is not a function of elite status alone, but of their deliberate integration within a framework of robust democratic oversight, legal accountability, and societal resilience. Counter-terrorism (CT), long considered the primary SOF mission, is in this study reframed as just one element of a broader spectrum of gray-zone activities that modern SOF must master.

1.2 Research Questions and Objectives

To validate this hypothesis systematically, the study investigates the following four research questions (RQ), each of which receives an explicit answer in the conclusions:

RQ1: What specific tactical and strategic attributes make SOF uniquely suited for defence against hybrid threats in the gray zone?

RQ2: How have contemporary security doctrines – specifically NATO and the Slovak Republic – evolved to integrate SOF into a Comprehensive Defence framework?

RQ3: What are the primary risks associated with the employment of SOF in ambiguous environments regarding democratic legitimacy and civil-military relations?

RQ4: How can a model of "Democratic Hybrid Defence" be constructed to ensure that SOF effectiveness and democratic oversight are mutually reinforcing rather than contradictory?

The objective of this research is to provide a comprehensive analysis of the strategic utility of SOF for the Slovak Republic and its allies. By synthesising military theory, historical-comparative analysis, and contemporary policy review, the study offers a set of concrete recommendations for the professionalization and integration of SOF within a robust democratic framework.

1.3 Methodology and Research Procedure

The methodology employed in this research is primarily qualitative, utilising a combination of historical-comparative analysis and a comprehensive review of strategic documents and academic literature. The selection of a qualitative approach is justified by the nature of the research problem: the "Democratic Dilemma" and the normative dimensions of SOF employment cannot be adequately captured by quantitative metrics. The goal is analytical interpretation rather than statistical generalisation.

The study draws on a deliberately diverse set of sources to ensure analytical triangulation. These include: (1) foundational theoretical works on the concept of hybridity [6][7][8][14]; (2) official government strategies and policy documents of the Slovak Republic and NATO [11][15]; and (3) contemporary applied research from specialised think tanks including STRATPOL, GLOBSEC, and the Joint Special Operations University (JSOU) [12][16][20]. Where possible, primary sources such as official strategic documents are preferred over secondary commentary.

The research proceeds through three analytically distinct stages. The first stage (Chapters 2–3) establishes the conceptual foundation through theoretical analysis of hybrid warfare and the strategic utility of SOF. The second stage (Chapter 4) applies this framework empirically to the Slovak Republic, examining the specific geopolitical context and the role of the 5th Special Forces Regiment (5. pŠU). The third stage (Chapter 5) addresses the normative dimension – the conditions under which SOF employment can be considered democratically legitimate and legally sound. The findings of all three stages are synthesised in Chapter 6, where the four research questions receive explicit answers. The following abbreviations are used throughout this paper: SOF – Special Operations Forces; CT – Counter-terrorism; SFA – Security Force Assistance; UW – Unconventional Warfare; MISO – Military Information Support Operations; ROE – Rules of Engagement; IHL – International Humanitarian Law; OPSEC – Operational Security.

2. Theoretical and Conceptual Framework – The Genesis and Evolution of Hybridity

2.1 Historical Perspectives: Hybridity as a Permanent Phenomenon

While the term "hybrid warfare" gained prominence in the early 21st century, the underlying strategic logic – the deliberate combination of conventional and irregular means to confuse, exhaust, and delegitimise an opponent – is historically persistent. As Murray and Mansoor [7] demonstrate in their comprehensive survey, "fighting complex opponents" has been a consistent challenge for conventional powers from the ancient world to the present. The Roman Empire, for instance, frequently encountered hybrid threats on its frontiers, where Germanic tribes utilised a mixture of guerrilla tactics, political subversion, and localised conventional strikes to negate the numerical and technological superiority of Roman legions.

During the Napoleonic Wars, the "Spanish Ulcer" provided one of history's most instructive examples of hybrid strategy: the devastating synergy between the regular Spanish army and irregular guerrilleros paralysed the French Grande Armée, which was designed for decisive conventional battles. This historical precedent carries direct analytical relevance:

hybridity is typically the strategy of the perceived weaker party, deliberately engineered to offset the material superiority of a conventional hegemon. Understanding this logic is essential for democratic states, which must design defensive postures that can address threats whose very purpose is to remain below the threshold of conventional response.

2.2 The Hoffman Legacy: Defining The 21st Century Challenge

The modern conceptualisation of hybrid warfare is inextricably linked to the work of Frank G. Hoffman [6], writing in the aftermath of the 2006 Lebanon War. Hoffman identified hybrid wars as those incorporating "a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder." His contribution was analytically transformative: rather than treating these modes as sequential phases of a campaign, Hoffman recognised them as simultaneously and synchronously employed, creating a "strategic overload" for traditional defensive structures.

For democratic states, the implications of Hoffman's framework are particularly acute. When an adversary deploys civilian proxies, cyber saboteurs, or disinformation operatives alongside its conventional forces, the traditional "military-first" response may be deemed legally excessive, politically escalatory, or simply inapplicable. The appropriate legal and political response becomes deeply contested – and this ambiguity is not an unintended side-effect but the central strategic weapon. This is precisely the challenge that RQ3 seeks to address: the risks to democratic legitimacy arise not merely from how SOF operate, but from the structural ambiguity that hybrid adversaries deliberately engineer to paralyse democratic decision-making.

2.3 The Gray Zone and the Threshold of Armed Conflict

The culmination of hybrid warfare theory is the concept of the "Gray Zone." As defined by the Joint Special Operations University (JSOU) [16], this is a contested space in the spectrum of conflict where state and non-state actors pursue political, economic, informational, and military activities that are aggressive and designed to change the existing order, but which do not rise to the level of open kinetic warfare that would trigger a collective defence response such as NATO's Article 5. The Gray Zone is not merely a physical space – it is a cognitive and legal space, deliberately constructed by the adversary.

The European Commission's Joint Framework on Countering Hybrid Threats [11] emphasises that the threshold of conflict is intentionally kept ambiguous by the aggressor. This ambiguity exploits the legalistic and risk-averse nature of democratic decision-making: democratic governments require legal authorisation, political consensus, and public legitimacy before committing military force. Each of these requirements takes time – and time is precisely what an adversary operating in the gray zone uses to establish irreversible facts on the ground. To counter this, a state must be able to "operate in the gray" with forces capable of precision action, low visibility, and strategic impact. This sets the stage for the analysis of SOF as the primary defensive instrument, directly addressing RQ1.

3. Special Operations Forces – Strategic Utility in The Gray Zone

3.1 The "Third Option": Sof in the Spectrum of Conflict

For decades, Special Operations Forces (SOF) were perceived primarily through the lens of counter-terrorism (CT) and high-value targeting. However, in the contemporary era of "strategic competition," their utility has returned to foundational roots: operating effectively in the space between war and peace. As Finlan [10] identifies, SOF represent "warfare by other means," providing political leaders with a critical "third option" when conventional military force is too escalatory and diplomatic or economic measures are too slow or insufficiently targeted to address a specific threat.

The strategic value of SOF is not derived solely from specialised equipment or advanced individual tactics, but from the "SOF mind-set" – a unique cognitive approach to problem-solving in conditions of extreme ambiguity and complexity. This mind-set allows SOF to navigate the Gray Zone, where adversaries utilise asymmetric and ambiguous techniques to achieve national goals without triggering regular military responses [23]. In this space, SOF act as a clandestine and responsive option, lowering the threshold for effective state action while maintaining a comparatively minimal physical footprint that reduces the risk of unintended escalation. This combination of cultural expertise, cognitive adaptability, low visibility, and multi-domain reach constitutes the direct answer to RQ1.

3.2 Indirect Action: Building Resilience Through SFA and UW

In hybrid conflict, the most strategically consequential SOF capabilities are often found not in direct action but in "indirect action." Security Force Assistance (SFA) and Unconventional Warfare (UW) are two core SOF activities that directly counter the methods of hybrid aggressors. SFA focuses on building and professionalising partner forces and domestic security institutions, creating a "deterrence by denial" effect [19]. By strengthening the internal security architecture of a democratic state, SFA reduces the systemic vulnerabilities – weak border control, corrupt local institutions, under-equipped police – that adversaries like Russia seek to exploit through proxy forces or "little green men."

Unconventional Warfare (UW), traditionally viewed as an offensive tool for enabling resistance movements behind enemy lines, has been reimagined within "Total Defence" models as a critical defensive pillar. By preparing a stay-behind resistance capability that can be activated in the event of territorial incursion, a state sends an unambiguous signal to any potential occupier: the cost of seizure will be protracted, costly, and ultimately unsustainable [17]. The USASOC UW Pocket Guide defines these activities as enabling a resistance movement to "disrupt or overthrow" an occupying power. In the Slovak context, this means integrating 5. pŠU expertise into a broader national resilience strategy that involves not just the military, but the entire societal fabric – from local self-governance structures to civil defence organisations.

3.3 Mastering the Human and Cognitive Domains

The "Human Domain" is arguably the most decisive battlefield of hybrid warfare. Hybrid threats do not primarily seek to destroy military hardware; they seek to erode the perceptions, loyalty, and will of the target population, gradually hollowing out the social cohesion upon which democratic states depend. SOF are uniquely positioned to operate in this domain because of their foundational emphasis on language proficiency, regional expertise, and deep cultural understanding. Unlike conventional forces, which are platform-centric, SOF are operator-centric: the individual operator's ability to influence local actors, build networks of trust, and navigate complex social environments is the primary capability.

Military Information Support Operations (MISO), once considered a secondary activity, have become central to SOF operations in the gray zone, where the narrative often determines outcomes before a single conventional shot is fired. Modern SOF must achieve "cognitive superiority" – the capacity to process information faster than the adversary, identify disinformation narratives in real time, and counter them through precise influence operations. The integration of MISO into the SOF operational toolkit directly reinforces the answer to RQ1: the breadth of the SOF attribute set – spanning kinetic, cognitive, legal, and informational domains – is precisely what makes them the most versatile instrument available to a democratic state in hybrid conflict. By contrast, the deployment of conventional forces in a cognitive domain operation would be at best ineffective and at worst counterproductive.

3.4 Integration in Comprehensive Defence Models

NATO's "One Defence" concept positions SOF not as an isolated elite capability but as the critical connector between conventional forces, intelligence agencies, and civilian law enforcement and governance structures. In a hybrid scenario, a threat may begin as a cyber attack or criminal act within the civilian domain and gradually escalate into a military crisis. SOF's ability to operate seamlessly across the civil-military boundary – analogous in some respects to gendarmerie-type forces but with far greater offensive and intelligence capacity – is essential for ensuring a unified and coherent state response [23]. This cross-domain integration capacity is what makes SOF operationally indispensable in Comprehensive Defence models and provides the key substantive answer to RQ2: NATO and allied doctrines have evolved to place SOF at the centre of the connective tissue between domains, not merely at the sharp end of direct action.

4. The Slovak Republic – Geopolitical Vulnerabilities and Domestic Sof

4.1 Geopolitical Context: The Eastern Flank and the Carpathian Frontier

The Slovak Republic occupies a pivotal and strategically sensitive position on NATO's Eastern Flank, serving simultaneously as a transit corridor for Alliance logistics and as a strategic buffer within the Central European region. Historically situated at the crossroads of major European power dynamics, modern Slovakia finds itself on the front line of the renewed "strategic competition" between democratic alliances and revisionist powers. The proximity to the ongoing conflict in Ukraine has fundamentally altered Slovak security perception, transforming hybrid threats from abstract theoretical possibilities into daily operational and political realities.

As noted by Ondrejcsák [12], Slovakia's vulnerability is not merely a product of geography but also of deep historical and societal legacies. The "Carpathian Frontier" is not just a physical boundary but a cognitive one: competing narratives of East and West collide here, with segments of the population retaining significant historical scepticism toward Western institutions and NATO specifically. This cognitive vulnerability is not incidental but structurally exploited by adversaries. In this context, the Slovak state must defend its sovereignty against adversaries that seek to neutralise its alliance commitments without necessarily crossing physical borders. This environment makes the development of a deeply integrated SOF capability – embedded within a broader Comprehensive Defence posture – not merely desirable but strategically essential.

4.2 Analysis of Hybrid Threats in the Slovak Security Environment

Hybrid aggression against the Slovak Republic is characterised by its multimodal and precisely calibrated nature, targeting simultaneously the state's political will, social cohesion, and critical infrastructure. Research from GLOBSEC [20] and STRATPOL [12] identifies three core vectors of attack, each of which interacts synergistically with the others

to produce the "reflexive control" effect – a state of decision-making paralysis in which Slovak institutions inadvertently act in ways that serve the adversary's strategic goals.

The first and most pervasive vector is Cognitive Subversion. Slovakia remains among the most susceptible states in the EU to pro-Russian disinformation, a condition facilitated by a deeply polarised media landscape, the presence of legacy information channels with pro-Eastern orientations, and a segment of the population that harbours structural distrust of NATO and EU institutions. The disinformation ecosystem does not merely seek to spread false information; it seeks to erode epistemic trust itself – to make citizens doubt the reliability of any institutional source, creating a vacuum that adversaries fill with their own narratives.

The second vector is Energy Coercion. Slovakia's historical total dependence on Russian energy imports has long been systematically deployed as a tool of political leverage. While diversification efforts are underway, the transition period represents a sustained "gray zone" vulnerability: significant portions of Slovak industry and civil society remain sensitive to energy price shocks that can be deliberately engineered to create social unrest and undermine public confidence in the government's strategic direction.

The third vector involves Cyber and Physical Sabotage. Targeted cyber attacks against government institutions – particularly those involved in defence procurement, intelligence coordination, and critical infrastructure management – pose a constant and evolving threat. Of particular strategic significance is the vulnerability of transport and logistics infrastructure essential for NATO reinforcement operations on the Eastern Flank. The Černoch and Ditrych study [13] accurately identified that the "new phenomenon" of hybrid warfare would require a structural evolution of Slovak security forces to address these non-kinetic attack vectors, a prediction that the 2021 Security Strategy has begun to operationalise.

4.3 The 2021 Security Strategy: A Paradigm Shift in Resilience

The adoption of the Security Strategy of the Slovak Republic (2021) [15] represented a decisive and historically significant shift in national security policy. For the first time, a core strategic document explicitly named hybrid threats as a primary challenge to the democratic order of the state, moving beyond the previous framework that treated security primarily through a conventional military lens. The strategy's conceptual centrepiece is "Comprehensive Defence" – a model in which the armed forces constitute only one component of a broader national effort that necessarily involves all government ministries, the private sector, local authorities, and ultimately the citizenry as active participants in their own defence.

A key operational pillar of this strategy is the enhancement of national resilience across all domains. This involves: strengthening the legal framework to counter disinformation and foreign interference in democratic processes; professionalising the security services to detect and respond to "below-threshold" scenarios before they escalate; and modernising the Special Operations Forces as the most capable element for managing the ambiguity and complexity of the gray zone. The 2021 Strategy thus provides the direct policy answer to RQ2: Slovak doctrine has undergone a paradigm shift from a conventional territorial defence orientation toward a Comprehensive Defence model in which SOF serve as the primary instrument for gray-zone management.

4.4 The 5th Special Forces Regiment (5. pŠU): Evolution and Roles

The 5th Special Forces Regiment "Jozef Gabčík" (5. pŠU), based in Žilina, is the elite core of Slovak Special Operations Forces and the primary instrument through which the 2021 strategy's SOF modernisation mandate is being executed. Historically, the regiment was predominantly focused on expeditionary CT operations, deploying within NATO frameworks to Afghanistan and Iraq. This experience built an exceptional institutional knowledge base in direct action, sensitive site exploitation, and partner force training. However, the post-2022 security environment has demanded a profound doctrinal reorientation.

In the current geopolitical context, the 5. pŠU's primary missions have shifted toward territorial defence, national resilience building, and collective security within the NATO framework. In the specific context of hybrid defence, the regiment provides three critical capability pillars. First, SFA toward domestic security agencies: building the institutional capacity of police, border guards, and municipal authorities to detect, report, and initially respond to "little green men" scenarios before they escalate beyond the law enforcement threshold. Second, UW framework maintenance: sustaining and training the conceptual and practical architecture for a national resistance capability that can be activated in the event of a territorial incursion, ensuring that any occupation would face a protracted and costly resistance from a prepared population. Third, Special Reconnaissance: providing national leadership with reliable, classified "ground truth" assessments in ambiguous situations, particularly along sensitive border areas and infrastructure nodes. The integration of the 5. pŠU into the NATO Special Operations Headquarters (NSHQ) ensures full Alliance interoperability and access to shared intelligence, enabling a rapid and synchronised response to regional crises [9].

The SWOT analysis presented in Table 1 provides a structured overview of the Slovak hybrid defence posture. The two principal strengths – an elite, NATO-interoperable SOF capability in the 5. pŠU and a forward-looking 2021 Security Strategy – represent genuine institutional assets positioning Slovakia favourably relative to its regional peers. However, these are meaningfully offset by two structural weaknesses.

Table 1: SWOT Analysis of Slovak Hybrid Defence and SOF Integration

STRENGTHS	WEAKNESSES
Elite, NATO-interoperable SOF (5. pŠU); Modern 2021 Security Strategy; Strong NSHQ integration.	Societal susceptibility to disinformation; Resource constraints for sustained gray-zone operations; legislative oversight gaps.
OPPORTUNITIES	THREATS
Regional cooperation (V4/B9); EU-NATO Joint Framework synergy; growing public awareness of hybrid threats.	Erosion of public trust in state institutions; potential energy-related social unrest; evolving legal gray zones.

The first is the persistent societal susceptibility to disinformation: Slovakia's polarised information environment means that adversarial cognitive operations find fertile ground, and even well-designed hybrid defence measures can be delegitimised before they take effect if the information space remains contested. The second involves resource constraints: sustained gray-zone operations require persistent human intelligence presence, long-term partner capacity building, and continuous information environment monitoring – all resource-intensive and competing with conventional force modernisation within a constrained defence budget.

The opportunities column highlights significant multilateral frameworks within which Slovak SOF can operate. The Visegrád Group (V4) and Bucharest Nine (B9) provide both political and practical platforms for regional SOF cooperation, intelligence sharing, and joint capacity building. The EU-NATO Joint Framework on Countering Hybrid Threats [11] provides a legal and institutional basis for coordinated below-threshold responses transcending the capabilities of any single member state. Conversely, the threat column identifies the most structurally dangerous risks: the ongoing erosion of public trust in state institutions – a process adversaries actively accelerate through disinformation – and the potential for energy-related social unrest to create the conditions of internal instability that hybrid aggressors seek to exploit as a precursor to more direct forms of pressure. Together, these findings reinforce the core argument: military SOF capability and societal resilience are not independent variables but mutually constitutive elements of effective hybrid defence.

5. The Democratic Imperative – Oversight, Legality, and Accountability in the Shadows

5.1 The Democratic Dilemma: Secrecy Vs. Transparency

The fundamental tension within a liberal democracy facing hybrid aggression lies in the structural contradiction between the operational requirements of secrecy and the normative requirements of public transparency – a challenge that constitutes the analytical core of RQ3. SOF, by their very nature, thrive in the "Gray Zone": an environment where visibility is a tactical liability and ambiguity is a strategic asset. Yet in a democratic system, the legitimacy of the use of force is derived from the consent of the governed, the clarity of legal mandates, and the accountability of those who exercise coercive state power.

This "Democratic Dilemma" is exacerbated in hybrid conflicts, where the lines between internal security, intelligence operations, and military activities are deliberately blurred by the adversary. Transparency is not merely a bureaucratic requirement – it is an operational source of national resilience. As the Open Government Partnership [21] emphasises, democratic societies' ultimate strength lies in the depth of public trust in their institutions. When citizens trust the state, they are structurally less susceptible to foreign disinformation and cognitive subversion. If, on the other hand, SOF are perceived as operating outside democratic norms – as a secret force accountable to no one – they become a liability that adversaries can exploit through information warfare, portraying the military as an instrument of internal repression. Therefore, SOF oversight must achieve a "golden mean" where operational security (OPSEC) is rigorously maintained at the tactical level, while the existence of robust oversight mechanisms is publicly affirmed at the strategic level. This distinction – between tactical secrecy and strategic accountability – is the analytical key to resolving the Democratic Dilemma identified in RQ3.

5.2 Legal Frameworks and the Phenomenon of Lawfare

The Gray Zone is simultaneously a legal battlefield. Adversaries increasingly employ "Lawfare" – the deliberate use of legal processes, norms, and international institutions as instruments of strategic competition – to delegitimise democratic responses before they can be mounted [24]. Lawfare involves the manipulation of international norms, the exploitation of definitional ambiguities in IHL, the strategic abuse of litigation, and the use of international forums to establish narratives of equivalence between aggressor and defender. For SOF operating in this space, every action must be grounded in a robust, pre-existing, and publicly known legal framework capable of withstanding both domestic and international scrutiny.

In the NATO context, the legal preparation of the operational environment is increasingly recognised as a core component of special operations planning, not a post-hoc consideration [25]. This involves proactively reinterpreting existing norms, advocating for new international legal frameworks to address gray-zone activities, and establishing clear domestic legal authorities for SOF action in "non-war" scenarios. For the Slovak Republic, this necessitates a targeted modernisation of the domestic legal code to clearly define the mandates, authorities, and limitations governing SOF employment in contexts such as countering organised sabotage, assisting police during a declared state of emergency, or

conducting intelligence preparation of the environment. Without such legal clarity, SOF operators face "operational paralysis" – the risk that decisive action in defence of the state exposes them to criminal liability in the absence of explicit authorisation. This legal gap is not merely an administrative inconvenience; it is a strategic vulnerability that adversaries can calculate into their planning.

5.3 Parliamentary Oversight and Accountability Models

Effective parliamentary oversight is a defining and non-negotiable characteristic of democratic control of armed forces (DCAF). The role of the legislature is to scrutinise military priorities, resource allocation, and – crucially in the SOF context – the scope and legal basis of deployments and operations [22]. However, traditional oversight mechanisms are structurally ill-suited to handle the operational tempo and classificatory requirements of SOF activities in hybrid environments. Parliaments in many EU and NATO member states face a significant "oversight deficit" in the domain of special operations, where the executive branch traditionally exercises maximal discretion and legislative scrutiny is minimal [23].

To address this structural weakness, democratic states must implement specialised oversight models specifically calibrated to the SOF context. This means establishing permanent, non-partisan parliamentary committees with appropriate security clearances and the institutional capacity to hire independent technical experts with operational backgrounds. Critically, these committees should operate on a principle of "outcome-based" oversight: evaluating whether SOF activities produce strategic outcomes aligned with nationally defined objectives and democratic values, rather than attempting to micromanage tactical decisions for which they lack the necessary expertise. The goal is not parliamentary direction of operations – which would be both operationally dangerous and constitutionally inappropriate – but rather systematic verification that the executive's use of SOF remains within mandated legal and strategic boundaries. Trust between political and military leadership, as BMLV [22] emphasises, is "the heart of effective democratic control" and must be cultivated deliberately and continuously through regular, structured, and genuinely confidential dialogue.

5.4 Public Trust as a Strategic Asset

In the Human Domain of hybrid conflict, the ultimate centre of gravity is the will of the population and the depth of their trust in state institutions. If SOF employment is perceived as opaque, unaccountable, or operating outside democratic values, it becomes a strategic liability: the adversary will amplify this perception through information operations, portraying elite forces as agents of a secretive authoritarian turn within what was ostensibly a democracy. Conversely, a transparently governed, professionally visible, and democratically accountable SOF community serves as a powerful force multiplier for national resilience.

The Open Government Guide [21] identifies civic participation and media literacy as essential pillars of democratic resilience in hybrid conflict. While the operational details of specific SOF missions must remain classified, the existence of oversight mechanisms, the general principles governing SOF employment, and the strategic rationale for maintaining an elite special operations capability should be communicated clearly and consistently to the public. By building genuine societal understanding of the role of SOF in Comprehensive Defence, the state constructs a "social contract" that immunises the population against adversarial narratives designed to portray elite military forces as threats to civilian society rather than its guardians.

The practical instruments for achieving this public trust dimension include: regular public communication from the Ministry of Defence on the broad strategic rationale and principles of SOF employment (without compromising OPSEC); curriculum integration of national security and resilience literacy into secondary and tertiary education; structured engagement between SOF and local communities, civil society organisations, and municipal authorities as part of the SFA and resilience-building mission; and the establishment of an independent annual review of the overall hybrid defence architecture – published in a non-classified form – that affirms to the public that oversight mechanisms are functioning and that SOF employment remains within democratic norms. These measures collectively constitute a strategic communication architecture that transforms public transparency from a bureaucratic obligation into an operational instrument of national resilience.

Table 2: Comparison of Oversight Models for Special Operations Forces

Oversight Level	Primary Actor	Key Mechanism	Challenge in Hybrid Conflict
Executive Control	Ministry of Defence / President	ROE, Strategic Mandates	Risk of politicisation of elite units
Legislative Oversight	Parliamentary Defence Committee	Budgetary approval, Inquiries	Slow response; lack of technical expertise
Judicial Review	Military / Civil Courts	Adherence to IHL	Gray zone actions lack clear legal precedent
Civilian Oversight	Ombudsmen / Civil Society	Public reports, human rights monitoring	Restricted access due to classified operations

It is worth noting that this model of "strategic accountability with tactical confidentiality" is not without precedent. Finland, widely regarded as the most resilient democracy in the face of Russian hybrid pressure, has long practised a model in which Total Defence is deeply embedded in public culture, the principles and oversight of its special

operations forces are publicly understood, and individual operational details remain classified. The Finnish model demonstrates empirically that it is possible to maintain both high SOF operational effectiveness and high democratic accountability – and that the two are mutually reinforcing rather than competing. For the Slovak Republic, which faces analogous geopolitical pressures but starts from a position of greater societal division and weaker institutional resilience, the Finnish experience offers both inspiration and a concrete policy benchmark. The path to "Democratic Hybrid Defence" is demanding, but it has been walked before.

6. Conclusions and Recommendations – The Democratic Hybrid Defence Model

6.1 Synthesis: Answering the Research Questions

This study has systematically examined the role of Special Operations Forces as a primary defensive instrument for democratic states in the context of 21st-century hybrid conflict. The analysis traversed conceptual, empirical, and normative dimensions, allowing for a comprehensive and triangulated evaluation of the central hypothesis. The findings can be systematically organised around the four research questions posed at the outset.

In answer to RQ1 – what attributes make SOF uniquely suited to gray-zone defence – the analysis demonstrates that SOF's distinctive utility derives not from any single capability but from the integrated combination of five mutually reinforcing attributes: (1) the cognitive adaptability of the individual operator, enabling effective action in conditions of extreme ambiguity; (2) multi-domain reach, spanning kinetic direct action, SFA, UW, MISO, and Special Reconnaissance within a single organisational framework; (3) persistent low-visibility presence that enables intelligence preparation of the environment and influence operations without triggering the escalatory dynamics associated with conventional force deployment; (4) cultural and linguistic expertise that allows SOF to operate within the Human Domain, building the networks of trust that are the primary defensive asset in a hybrid conflict targeting population loyalty; and (5) the capacity for economy of force, producing outsized strategic effects with a minimal physical footprint.

In answer to RQ2 – how NATO and Slovak doctrines have evolved – the analysis confirms a significant paradigm shift. Both NATO's "One Defence" concept and the Slovak Republic's 2021 Security Strategy have moved decisively from a conventional territorial defence orientation toward a Comprehensive Defence model. In this model, SOF serve as the critical connective tissue between conventional military, intelligence, and civilian domains. The 5. pŠU's transformation from an expeditionary CT force to an integrated Comprehensive Defence asset exemplifies this doctrinal evolution at the national level, while its integration into the NSHQ ensures alignment with Alliance-wide strategy.

In answer to RQ3 – the primary risks to democratic legitimacy – the analysis identifies the "Democratic Dilemma" as the central governance challenge: the structural tension between the operational necessity of secrecy and the democratic requirement for accountability. The primary risks are threefold. First, legal ambiguity: where domestic law fails to define SOF mandates in gray-zone scenarios, operators face operational paralysis or, conversely, act without legal sanction, undermining rule of law. Second, parliamentary oversight deficit: where legislatures lack the expertise and access to conduct meaningful scrutiny, the executive's use of SOF becomes effectively unaccountable, creating conditions for abuse and eroding public trust. Third, narrative vulnerability: where SOF operations are not anchored in publicly understood strategic rationale and visible oversight frameworks, adversaries can weaponise perceived opacity to delegitimise the entire Comprehensive Defence effort in the information space.

In answer to RQ4 – how a "Democratic Hybrid Defence" model ensures mutual reinforcement of effectiveness and oversight – the study concludes that the resolution of the Democratic Dilemma lies in maintaining a principled distinction between tactical-level operational security and strategic-level institutional transparency. SOF missions are, appropriately, classified. However, the oversight structures that govern these missions, the legal framework that authorises them, and the strategic objectives they serve must be publicly known and politically affirmed. This framework of "strategic accountability with tactical confidentiality" transforms oversight from a constraint on operational effectiveness into an active strategic asset: it builds the public trust that constitutes the ultimate centre of gravity in hybrid conflict, and it denies adversaries the narrative ammunition they seek to delegitimise democratic defence.

6.2 Recommendations

On the basis of these findings, the study advances four concrete recommendations for the Slovak Republic and analogous NATO member states. First, a dedicated legal modernisation effort should clearly define SOF mandates in below-threshold scenarios, establish robust ROE for gray-zone operations, and ensure that legal preparation of the operational environment is treated as an integral component of SOF planning – not a post-hoc consideration. Second, a permanent specialised parliamentary oversight committee with appropriate security clearances and independent technical advisory capacity should be established to conduct outcome-based scrutiny of SOF activities, building institutional knowledge of special operations that currently does not exist at the legislative level. Third, continued investment in the 5. pŠU's transformation toward a Comprehensive Defence orientation – including SFA capacity, UW framework development, and MISO integration – should be treated as a strategic priority, proportionate to the severity of identified hybrid threats. Fourth, a sustained public communication strategy should be developed to build societal literacy around the role of SOF in national defence, the existence of robust oversight mechanisms, and the strategic rationale for

Comprehensive Defence – transforming the population from a passive object of hybrid attack into an active participant in national resilience.

6.3 Limitations and Directions for Further Research

This study is subject to several limitations that define the scope of its conclusions and open directions for further research. The qualitative methodology, while appropriate for the normative and conceptual dimensions of the research problem, does not permit statistical generalisation across multiple national contexts. The findings are anchored in the Slovak case study and, by doctrinal extension, the broader NATO framework; their applicability to non-NATO democracies or states with fundamentally different civil-military traditions would require separate empirical analysis.

Furthermore, the rapidly evolving character of both hybrid warfare doctrine and SOF organisational development means that specific institutional details – particularly regarding the 5. pŠU's current capabilities and the state of Slovak legal modernisation – may change significantly in the near term. The conceptual framework, particularly the "Democratic Hybrid Defence" model and the principle of "strategic accountability with tactical confidentiality," is intended to be durable across these changes; however, its operationalisation will require ongoing adaptation.

Three directions for further research emerge from the findings. First, a comparative study of parliamentary SOF oversight models across NATO member states would provide an empirically grounded basis for identifying best practices applicable to the Slovak context. Second, an analysis of the interaction between national resilience metrics and hybrid attack intensity – drawing on the growing body of quantitative data from Finland, the Baltic states, and Ukraine – would allow for a more rigorous empirical assessment of the causal relationship between societal resilience and hybrid deterrence effectiveness. Third, the legal dimension of gray-zone operations remains one of the least theorised areas in both academic and policy literature; a dedicated legal-doctrinal analysis of Slovak and international legal frameworks as they apply to SOF in below-threshold scenarios would constitute a significant contribution to both scholarship and policy practice.

7. Conclusions

Legitimacy is not a constraint on effectiveness – it is a prerequisite for it. In a hybrid conflict where the decisive battle is for the narrative and the will of the population, any strategic gain achieved through illegitimate or unaccountable means represents a net strategic loss. The central hypothesis of this study is confirmed: SOF are an indispensable instrument of democratic defence in hybrid conflict, but their indispensability is conditional. It is conditional on their integration within a framework of Comprehensive Defence, their grounding in robust legal authority, their subjection to meaningful democratic oversight, and their visible embeddedness within the societal fabric they are tasked to protect. The "Vanguard" of democratic defence is not merely an elite military unit. It is the manifestation of a democratic state's institutional will to survive and to do so on its own terms, without sacrificing the values that make its defence worth mounting.

Acknowledgements. The authors are grateful to the reviewers and to the editorial board of CNDCGS 2026 for their constructive comments. Any views expressed are those of the authors and do not represent the official position of the Armed Forces Academy.

References

1. Ivančík, R. – Nečas, P. Rising significance of the air force in current unpredictable security environment. INCAS Bulletin, 2020, 12(2), 237–246. <https://doi.org/10.13111/2066-8201.2020.12.2.20>
2. Ivančík, R. – Nečas, P. Air transport terrorism: One of the most feared types of asymmetric security threat. INCAS Bulletin, 2020, 12(4), 227–239. <https://doi.org/10.13111/2066-8201.2020.12.4.21>
3. Ivančík, R. – Nečas, P. Hybridné hrozby: Bezpečnostná výzva pre demokratické spoločnosti. Praha: Leges, 2025. ISBN 978-80-7502-823-5.
4. Andrassy, V. – Ondruš, M. The Gray Zone and Its Place in Security Environment. Proceedings of CNDCGS, 2024, 90–98. <https://doi.org/10.3849/cndcgs.2024.90>
5. Galeotti, M. The Weaponisation of Everything. New Haven: Yale University Press, 2022. ISBN 978-0-30025-344-5.
6. Hoffman, F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute, 2007.
7. Murray, W. – Mansoor, P. R. (eds.) Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. Cambridge: Cambridge University Press, 2012.
8. Renz, B. – Smith, H. (eds.) Russia and Hybrid Warfare – Going Beyond the Label. Helsinki: Aleksanteri Institute, 2016.
9. Robinson, L. One Hundred Victories: Special Ops and the Future of American Warfare. New York: PublicAffairs, 2013.
10. Finlan, A. Special Forces, Strategy and the War on Terror: Warfare by Other Means. London: Routledge, 2008.
11. European Commission. Joint Framework on Countering Hybrid Threats. Brussels, 2016. [<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018>]

12. Ondrejcsák, R. (ed.) Hybridné hrozby a Slovenská republika. Bratislava: STRATPOL, 2017.
13. Černoch, P. – Ditrych, O. (eds.) Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy. Praha: ÚMV, 2017.
14. Zemánek, L. Hybridní válka Ruské federace: Teorie a praxe. Praha: Academia, 2018.
15. Ministerstvo obrany SR. Bezpečnostná stratégia Slovenskej republiky (2021). Bratislava, 2021.)
[<https://www.mosr.sk/bezpecnostna-strategia-sr-2021/>]
16. Joint Special Operations University (JSOU). 2024 Special Operations Research Topics. MacDill AFB: JSOU Press, 2024.
17. USASOC. Unconventional Warfare Pocket Guide (GTA 90-01-003). Fort Bragg: USASOC, 2012.
18. U.S. Department of State. Report on Gray Zone Conflict. Washington D.C., 2017.
19. Atlantic Council. The Next Decade of Strategic Competition: How the Pentagon Can Use SOF to Better Compete. Washington D.C.: Scowcroft Center, 2025.
20. GLOBSEC. Slovak Republic Hybrid Threats Vulnerability Study. Bratislava: GLOBSEC Policy Institute, 2026.
21. Open Government Partnership (OGP). Defence and Security: Hybrid Threats Guide. Washington D.C., 2025.
22. BMLV. Parliamentary and Executive Oversight of the Defence Sphere. Vienna: Federal Ministry of Defence, 2018.
23. GSDRC. The Use of Force Under International Auspices: Strengthening Parliamentary Accountability. Birmingham: GSDRC, 2024.
24. Zima, A. Towards a War of Norms? From Lawfare to Legal Operations. Paris: Ifri, 2022.
25. U.S. Naval War College. A Special Operations Approach to Lawfare. Newport: Stockton Center, 2024.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of CNDCGS 2026 and/or the editor(s). CNDCGS 2026 and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.