AD SECURITATEM

THE BEST ESSAYS BY COURSE PARTICIPANTS AT THE BALTIC DEFENCE COLLEGE

ACADEMIC YEAR 2025/2026

BALTIC DEFENCE COLLEGE

Cover design: BALTDEFCOL and ChatGPT. Original picture edited to a winter scene by ChatGPT, then edited in Photoshop for correctness (original building name overlaid, deleted AI inaccuracies in signs) by Multimedia Administrator Mr Raido Saar.

Ad Securitatem is a collection of the best papers from our main courses.

Tartu 2026

TABLE OF CONTENTS

FOREWORD

The contemporary security environment continues to evolve at a pace that challenges established assumptions and frameworks. In this context, professional military education must go beyond the transmission of established knowledge; it must cultivate the capacity to navigate uncertainty, to evaluate rapidly evolving technologies, and to maintain sound judgement in environments where information is abundant but not always reliable.

While geopolitical tensions and conventional military risks remain central, the rapid expansion of technological capabilities, most notably in artificial intelligence, adds a further layer of complexity to an already demanding landscape. This is visible not only in practice, but often even more so in academic settings, where fast-evolving AI tools increasingly challenge traditional approaches to teaching, learning, and research.

This year's research project engaged with these developments from the outset. For this volume, we have selected the highest-evaluated papers from across all courses. The topics, ranging from air power and operational resilience to artificial intelligence, transatlantic relations, strategic communication, and emerging security dynamics, demonstrate the breadth of our students' interests and their ability to engage critically with contemporary challenges. *Ad Securitatem* continues to provide a valuable platform for the publication of these insightful contributions.

Dr. Asta Maskaliūnaitė,
Director, DPS

BEST ESSAYS OF THE JOINT COMMAND AND GENERAL STAFF COURSE (JCGSC) AND CIVIL SERVANTS' COURSE (CSC)

MAJ Reet STAMM: The Air Littoral: Rethinking Airspace Control in the Near-Surface Battlespace

JCGSC Writing Award

Supervisor: LTC Ivar SAMMAL

Statement on the Use of Artificial Intelligence (AI) Tools:

Microsoft Copilot has been used as an advisor in an educational context to collect data, investigate, and outline information for the preparation of a Research Paper. Microsoft Copilot and Grammarly have been used to refine grammar and sentence structure in English (UK).

I have reviewed and verified all AI-refined material and have made modifications when deemed necessary to ensure the integrity and correctness of the final text.

Introduction

Today, the common idiom ‘The future is now!’ serves as a constant reminder to all those who are involved in operational competitiveness and technological innovation within the alliance military community.

‘Competing with future peer adversaries will require advanced battlespace management concepts to facilitate rapid synchronisation of efforts to create dilemmas for adversaries’ (Rossetti, 2021, p. 28). It means that future conflicts will require militaries to evolve both technologically and conceptually, such as integrating unmanned systems across domains rather than relying on siloed operations. The Western military's mantra of ‘cheap, many, and fast’ is accelerating and shaping contemporary drone innovation processes (Kunertová, 2025, p. 21). Thus, it emphasises the necessity of quickly adapting not only to advanced unmanned technologies but also to envisioning new ways and means to use them to defeat the adversary in tomorrow´s multidimensional contested battlespace. Therefore, this research paper focuses on the evolution of the battlespace within the third dimension, airspace, and examines the near-surface layer of airspace, the so-called ‘air littoral’, where the widespread use of small- to medium-sized unmanned aircraft, commonly referred to as ‘drones’, is challenging the current doctrinal concept of military airspace, which in this research is treated as ‘conventional airspace’.

This research paper introduces the thesis that drones are transforming the air littoral into a dynamic, networked, and all-domain digital airspace, compelling militaries to reassess the conventional airspace control system and make necessary adaptations.

By elaborating the argument, the theory of Revolution in Military Affairs (RMA) suggests that fundamental changes in warfare occur when advances in technology, changes in military doctrine, and organisational adaptation reinforce one another, producing a new conceptual approach, along with new ways and means of conducting military operations (Knox and Murray, 2001, p. 12). In this regard, the RMA framework, which anticipates the synergistic interaction of technology, doctrine, and organisation,

is considered in this paper. As the modern concept of the air littoral is relatively new, originating from US Air Force researchers in the early 2020s, it has since evolved into a broader understanding of the military airspace concept across multiple domains. Therefore, the academic discussion of this paper draws on the work of international scholars, US and NATO military studies, and publications. To further support the arguments, the paper also looks forward to examining conditions and lessons derived from Ukrainian operational experience; however, such validation is limited to publicly available information and therefore remains only partial.

This research paper is divided into three chapters that, in parallel with the RMA framework, outline the past, present, and future concepts of military use and control of airspace, derived from the emerging involvement of drones within the conceptual air littoral.

Into the Blue Skies: The Vertical Expansion of Warfare

This first chapter examines the historical pattern of technological competition in military aviation, providing a broad overview of its development from early history to the present. It also outlines the doctrinal approach to conventional airspace control and how unmanned aircraft have gradually developed into a force capable of competing with manned aircraft in that airspace.

History shows a pattern – technological competition drives military adaptation.

The airspace has always evolved through technological competition in aviation, forcing the military to adjust its doctrinal and organisational structures. This pattern is observable throughout the history of aviation. Looking back, from the first use of balloons to the moment the Wright brothers first demonstrated controlled, powered flight, each major leap in aviation technology has influenced the character of military operations and the structure of the battlespace. By World War I, the states had come to recognise that the sky was a usable environment, and it became a combat domain with the introduction of observation aircraft, bombers, and fighters, along with the refinement of air missions. Still, this new domain remained completely unregulated, with no laws or recognised concept of national airspace sovereignty. The change

occurred in 1919, after World War I, when the Paris Convention Treaty (1919) established regulations for international air navigation and recognised state sovereignty over national airspace. In 1944, when the International Civil Aviation Organisation (ICAO) Chicago Convention, the foundation for modern civil aviation, was agreed upon by the member states, the first fundamental principle of that treaty was that airspace is an extension of national territory (UN, 1944).

In parallel to civil aviation developments, NATO also maintained its role in airspace utilisation. In cooperation with civil aviation authorities, it has sought satisfactory solutions to ensure that military aircraft can operate both on the ground and in the air with sufficient freedom of movement to achieve military objectives, whether for training and exercises or for operational tasks such as peacetime air policing. For example, as 'Aspects of NATO: Airspace Co-ordination' (1961) describes, until 1959, the airspace above 20,000 feet was used almost exclusively by military aircraft. Interaction and coordination with civil airspace users took place only in the lower airspace below that level. The situation changed as civil jet transport aircraft, cruising on higher altitudes, began to be employed in increasing numbers. This development led NATO, in the 1960s, to develop a broader understanding of airspace structure, along with new coordination and control methods, and the modernisation of supporting technology, such as radars, data transmission, and handling systems. These developments in the past align with the Revolution in Military Affairs (RMA) as a 'fundamental change when advances in technology, doctrine, and organisational adaptation reinforce one another' (Knox and Murray, 2001, p. 12). As a result, these technological advancements in civil aviation have prompted the military to concurrently review and establish principles for the airspace control system. Due to this competition, military aviation has expanded its operational range and capabilities beyond civil aircraft. Today, the application of higher levels enables the military to avoid interference with commercial air traffic. It provides tactical benefits, such as broader sensor coverage, greater protection against surface-to-air threats, and reduced radar visibility.

This short journey through aviation history demonstrates the pattern that, as military aviation has advanced through competitive innovation, the military has continually been compelled to reassess and adapt not only the technological capabilities that support air operations but also its doctrines and organisational structures.

The relevance of conventional airspace control.

In the context of conventional warfare, the structured airspace control system provides efficient methods for controlling the air and supporting forces. The general understanding is associated with violent, regular-deploying armies, force-on-force combat, centred on decisive points and the ability to achieve capabilities, leadership, or materiel 'knockout' (Hutto and Rogers, 2025, p. 7, 11). In this context, the airspace control system must rely on clarity. Therefore, the distinction between *control of the air*, *air control*, and *airspace control* is important, as each term refers to a different aspect of control. The three terms sound similar, but in military doctrine (AJP -3.3), they mean different things: *control of the air* is a desired operational condition, while *air control* is about a set of activities, and *airspace control* refers to the coordinated set of measures that organise, manage, and regulate the use of airspace. In detail, *control of the air* employs the airspace within operational areas across all domains by enabling friendly forces to operate at the optimal place and time without prohibitive air interference from the adversary (AJP 3.3, item 1.5.1.1 (1)). Once a sufficient degree of *control of the air*, whether air superiority or air supremacy, is achieved, air power can be projected where and when required; however, this condition is never permanent and must be continually maintained.

Based on these doctrinal foundations, NATO focuses on the practical mechanisms that enable air-land integration in the shared battlespace. To strengthen effective teamwork between air and land services and components, NATO has tested and refined its joint fires and air-ground integration methods for air execution, surface fires, airspace management, air and missile defence, and army aviation during exercises conducted since 2021 (Güleç and Kelley, 2025, p. 35). From an airspace control perspective, a defined volume of airspace, with dimensions that allow ground manoeuvre and interoperability, is delegated to land forces so they can manage assigned aircraft and deconflict all airspace users, including friendly manned and unmanned aircraft as well as artillery and missile ordnance. This arrangement enables land forces to execute organic fires and aviation operations rapidly, without requiring further coordination with the airspace controlling authority (Güleç and Kelley, 2025, p. 36), which, in most cases, is the air component command. Within the airspace delegated to land forces, drone

activity has been gradually increasing, creating additional challenges for deconfliction, situational awareness, and the integration of manned and unmanned operations.

Drones as an emerging phenomenon in warfare, or not?

Drones are nothing new in warfare, particularly. Although it may appear that drones have only become a significant part of the airspace-user community over the past decade, especially during the Russo-Ukrainian war, they have played an important role in warfare for much longer. Sauser (2026, p. 127–128) traces the employment of UAVs over several decades, from the Vietnam War to Israel's Beqaa Valley operation and includes the Gulf War. During the Vietnam War, the potential of drones was demonstrated in high-risk missions over heavily defended airspace, where they conducted reconnaissance sorties in place of manned aircraft. Their employment then evolved into more sophisticated roles, as seen in the Israel–Syria conflict, where UAVs provided real-time targeting data for strikes (Sauser, 2026, p. 127–128). However, these systems still lacked their own strike capability. This began to change after the Gulf War and from 2001 onwards in Afghanistan, and later in Pakistan and Yemen, American drones were conducting not only spying, surveillance, and battle damage assessment but also targeted attacks (Sauser, 2026, p. 128; Sotoudehfar and Sarkin, 2023, p. 131).

Unmanned aircraft in warfare continued to evolve into advanced, long-endurance, large airframes equipped with powerful sensors and missile capabilities, primarily used to target international terrorism (Kunertová, 2025, p. 6). In parallel, the civilian industry continued to develop small, inexpensive commercial and hobbyist drones, built from readily available components purchased in electronics shops and subject to little scrutiny, carrying sensors, detectors, and communications, and, in some cases, transporting loads (Lavers, 2025, p. 42). Since the Nagorno-Karabakh War, this cost-effective drone concept, gradually adopted by militaries, has begun to transform the character of warfare by creating a lethal 'mass effect' through saturation of the battlefield (Davis, 2025, p. 75-76). Cheap forms of precision mass, delivered by swarms of armed drones, compel forces operating at range to disperse to survive. As the Russo–Ukrainian War demonstrates, for the missions and masses, two broad categories dominate the conflict: military drones and civilian drones adapted for military

purposes (Sotoudehfar and Sarkin, 2023, p. 140). It has been recognised that ‘consumer drones have mutated from a security nuisance into combat assets’ (Kunertová, 2025, p. 6). It confirms Cohen's (1996, p. 42) view that civilian technologies also bring revolutionary changes in warfare, thereby constituting a contemporary RMA.

As this chapter has shown, the evolution of military aviation and the patterns of technological competition have shaped the doctrinal foundations of conventional airspace control. While originally designed for manned aviation, these doctrines have been developed as drone operations have emerged. Until recently, it has been assumed that drones operate alone and need to be kept separate from manned aircraft, with dedicated airspace control measures assigned to ensure safe deconfliction. However, this long-standing safety precaution is becoming increasingly difficult to sustain. It is becoming apparent that drones are rapidly evolving into systems that can compete with manned aircraft within conventional airspace, particularly in the near-surface battlespace, the so-called air littoral.

Air Littoral Today: An Emerging Operational Environment

These days, unmanned aircraft, increasingly enabled by AI, are signalling a new era in warfare. Just as the jet aircraft redefined air power in the mid-20th century, drones are now transforming the lower, near-surface layer of airspace. This emerging environment, which is growing increasingly dense with autonomous systems and digitalised sensing, creates new challenges for airspace control while altering the relationships between air and land forces. This chapter examines these developments in the air littoral, where the widespread use of small- and medium-sized drones is redefining conventional airspace control.

Drone trade in the liminal space between land and air domains.

As the air littoral becomes operationally significant, the traditional boundaries between land and air domains, along with their domain-centric structures, are becoming less relevant. For much of the past century, Douhet’s (2003) concept of air power shaped Western thinking about the air domain. Control of the air has been seen as something achieved mainly within conventional airspace by air forces using manned aircraft as

their primary assets. Operationally, this separation is reflected in engagements either between manned fighters operating in mid-air or between attacking aircraft and surface-to-air missile (SAM) systems in the near-surface layer of the airspace (Bremer and Crieco, 2024, p. 12). In contrast, land forces have traditionally focused on occupying and controlling territory through land-based actions. Although both forces sometimes project power into each other's domains, such as aircraft striking ground targets and land forces employing fires reaching into the air domain, the boundaries between these domains and their associated structures have remained firmly intact (Bremer and Grieco, 2024, p. 75). This indicates that, despite recent concepts promoting joint, multi-domain operations, a domain-centric mindset remains deeply institutionalised.

This heritage-based separation is increasingly untenable as drones reshape the power projection in the near-surface layer of airspace. This paradigm is now being challenged by drones, which are taking a core role in counter-battery fire, deep reconnaissance, and battlefield interdiction, roles traditionally reserved for army aviation (Tourret, 2025, p. 5). This appears most evident in Ukraine, where a refined power concept integrates joint combat power into the air littoral to establish local air superiority through combined arms, making notable use of electronic warfare and air defence in close coordination with 'micro-airpower' (Jackson and Arrol, 2024, p. 62). As Lavers (2025, p. 45) notes, unmanned aircraft have not changed the nature of air power but have altered its characteristics through cumulative technological evolution. This aligns with Kunertová (2025, p. 5), who argues that drones are transforming air forces and reinventing the practice of air power, and Weller et al. (2025, p. 55), who describe the air littoral as a liminal space continually reshaped, traded, conquered, and surrendered by old and new aerial actors. Together, these perspectives highlight trends that erode domain boundaries and foster synergistic changes in technology, operations, doctrine, and organisational structures.

How to differentiate the drones in contemporary warfare.

In current conflicts, boundary erosion is no longer theoretical. As discussed earlier, drones represent a new variable that is altering legacy-based airspace control practices, making clear differentiation increasingly important. NATO's Class I–III

system (Table 1. NATO drone classification) establishes a baseline, yet it does not fully align with the realities of drone use in modern conflict. While classes II-III drones generally operate under conditions like those of manned aircraft, this alignment no longer holds for class I drones.

Table 1. NATO drone classification (Hutto and Rogers, 2025, p. 10)

Class	Category	Normal employment	Normal operating altitude	Normal mission radius	Primary supported commander	Example platform
Class III (< 600 kg)	Strike/Combat	Strategic/national	Up to 65,000 ft MSL	Unlimited (BLOS)	Theatre	Reaper
	HALE	Strategic/national	Up to 65,000 ft MSL	Unlimited (BLOS)	Theatre	Global Hawk
	MALE	Operational/theatre	Up to 45,000 ft MSL	Unlimited (BLOS)	JTF	Heron
Class II (150–600 kg)	Tactical	Tactical formation	Up to 18,000 ft AGL	200 km (LOS)	Division, brigade	Watchkeeper
Class I (< 150 kg)	Small (>15 kg)	Tactical unit	Up to 5,000 ft AGL	50 km (LOS)	Battalion, regiment	Scan Eagle
	Mini (<15 kg)	Tactical sub-unit (manual or hand launch)	Up to 3,000 ft AGL	Up to 25 km (LOS)	Company, platoon, squad	Skylark
	Micro (<66 J)	Tactical sub-unit (manual or hand launch)	Up to 200 ft AGL	Up to 5 km (LOS)	Platoon, Squad	Black Widow

Most class I drones incorporate a wide range of commercial technologies, including first-person view (FPV) drones originally designed for racing but now adapted for military use (Hutto and Rogers, 2025, p. 9; Kunertová, 2025, p. 7). Employed by land forces at the battalion level and below, they typically operate below 5,000 feet above ground level and interact directly with army organic aviation and ground-based air defence systems. Their variability in capabilities, employment methods, and mission sets makes them difficult to categorise comprehensively (Hutto and Rogers, 2025, p. 9) and existing classifications do not adequately differentiate drones in air littoral in ways that create meaningful operational insight into their employment or limitations (Weller et al., 2025, p. 57). Recent technological advances further complicate the picture. Several class I drones, such as UJ-22 Airborne, Skydio X2, and Autel Evo II, can now reach altitudes above 5,000 feet, overlapping with the class II-III drones like the Bayraktar TB2 and even manned aircraft. This vertical convergence reinforces the understanding that wartime practice is shaped less by doctrinal classification than by the capabilities of aircraft or drones to perform a given mission (Hutto and Rogers, 2025, p. 9).

Open-source data on the maximum take-off weights (MTOW) of drones used by Ukraine against Russia shows that, aside from the Bayraktar TB2 (700 kg) and the Tu-143 (1,230 kg), most of them fall within NATO class I (under 150 kg). These drones

therefore dominate activity in the air littoral below 10,000 feet above ground level (Figure 1. Drones used by Ukraine).

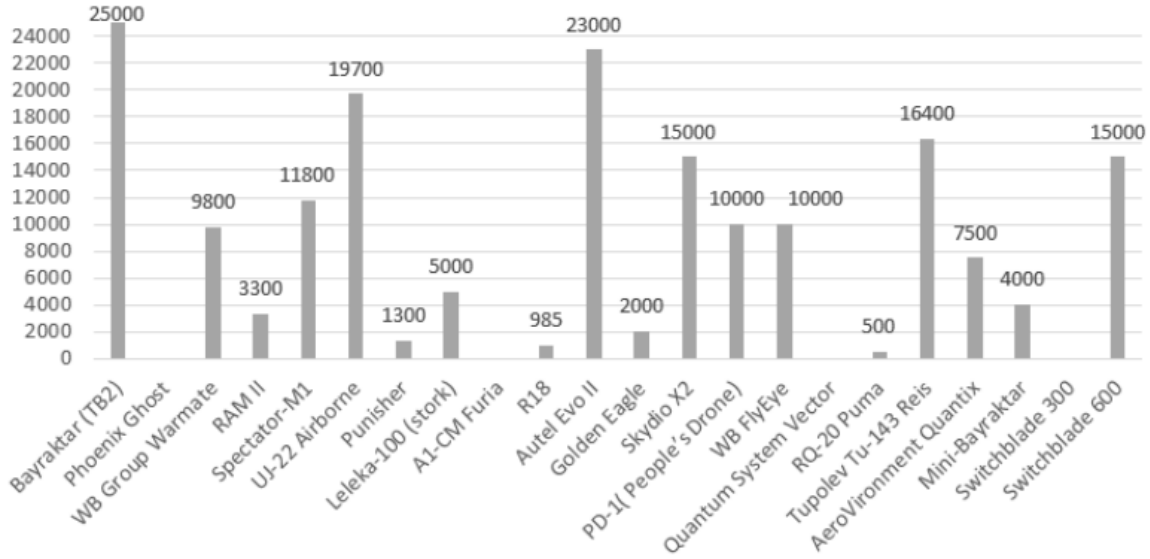

Figure 1. Drones used by Ukraine (altitude in feet). (Sotoudehfar and Sarkin, 2023, p. 152)

The combination of legacy and modern technologies, rapid innovation cycles, and the proliferation of small, inexpensive, smart, and highly lethal weapons and drones, operating alongside army aviation and air defence, places significant pressure on the land forces' surface battlespace. As Bremer and Grieco (2021, p. 71) and Kunertová (2025, p. 7) note, drones can effectively ‘mine’ the lower airspace, creating persistent threats for both ground forces and high-value air assets.

Although airspace control procedures apply in principle to both manned and unmanned aircraft, drones present distinct challenges. Their smaller size, lower radar signature, and varied operating profiles make them more difficult to detect and identify, requiring dedicated control measures rather than integration into shared airspace with manned aircraft (AJP-3.3.5, para 4.11). These differences in classification, detectability, and control highlight a persistent gap in how manned and unmanned aircraft are treated within the battlespace. As Bremer and Grieco (2021, p. 68) argue, bringing the air war closer to the surface fight makes it more likely that the army or navy will need to strive for control of the air littoral through local, persistent occupation. However, airspace control limitations and disparities between surface and air operations may not ensure

the level of control required to achieve air superiority. Adversary interference through air and missile threats against surface forces is likely to remain persistent, even when air forces maintain control of the skies.

Reconfiguring the battlespace: drones across time, space and force.

Understanding how future drone operations align with the dynamics of the combat battlespace requires examining how drone technologies interact with the core elements of time, space, and force, which together shape the character of future combat operations.

The *time* determines the tempo and sequencing of actions, and the ability to act, react, or exploit opportunities against the adversary, primarily by land forces. In this context, drones expedite the combat sensing, decision-making and strike cycles. One of the critical characteristics of drones' operational performance is endurance, which varies across drone designs from minutes to 24 hours and will increase in the future with modifications to long-endurance power systems and payloads (e.g., sensors) (Lavers, 2025, p. 47). It means that the duration of drone airspace usage and the provided deconfliction should be considered over extended time periods.

The *space*, including terrain, distance, positioning, and battlefield geometry, is another element that influences combat efficiency and airspace usage. In this sense, the drones are expected to expand the battlespace and saturate it with presence. The near-ideal conditions for drone operations, allowing clear lines of sight for sensors and control links, may not be the case when the drone's sensors, communication, and battery endurance are affected by mountainous terrain, heavily forested areas, or severe weather conditions (Sauser, 2026, p. 129). This limitation can be addressed in battlefield geometry when drones operate in stacks, establishing different layers for different missions and infantry units (Sauser, 2026, p. 136). This layered drone operations approach is shaping the future use of air littoral, as it requires a flexible, real-time, and dynamic approach to airspace control by different drone operators in land forces.

The *force* aspect refers to the application of combat power across the battlespace. Drones' primary contribution lies in creating a persistent concentration of assets over wider areas through the increased mass of attritable systems. The innovations in civil drone technologies and military drone usage in ongoing conflicts are signalling the drone activities in groups or swarms. The distinction between a group or a formation and a swarm, based on numbers or operating conditions, is not yet clearly defined within NATO but requires utmost attention, as parallel civilian technologies are advancing rapidly and will influence the use of military drones in the near future. The ’mass effect’ or ’ precision mass’ by cheaply produced drones is already changing warfare in Ukraine, as 50-drone swarms are tested (Sauser, 2026, p. 142), and it is demanding new tactics, equipment and leadership for armies to fight (Davis, 2025, p. 76).

Taken together, across the dimensions of time, space, and force, drones are reshaping the battlespace by accelerating operational tempo, expanding the area of action, and enabling new forms of massed combat power. These shifts show that drones are not just adding capabilities but redefining how land forces will fight in future conflicts and interact with air.

Air Littoral Tomorrow: From Procedural Control to Digital Dominance

The previous chapter examined the essence of the air littoral and traced the evolution of drone employment to the present. Building on that foundation, this chapter analyses how drones interact with the battlespace through the RMA framework, highlighting the synergistic interaction between technology, doctrine, and organisations that would drive effective digital airspace control in the contested air littoral.

Will the drones control or occupy the skies?

From a conceptual perspective, drones are more likely to enable forces to occupy the airspace in the future than to control the skies. Their ability to overwhelm adversary defences through offensive saturation in lower airspace, using waves of small sensors, decoys, and munitions, making it increasingly difficult to achieve and maintain operational advantage (Kunertová, 2025, p. 9, 21). This growing complexity in the air

littoral means that conventional procedural methods of airspace control will no longer suffice. Looking forward, these methods will be refined from reliable but inefficient procedural methodologies to more advanced machine-learning and AI-enabled models that blend positive control with predictive techniques (Jackson and Arrol, 2024, p. 67). Considering this, the conventional airspace control system is expected to transform from a centralised, slow, radar-based, and human-driven system into a real-time, distributed, sensor-fused, and AI-supported airspace control model. This new software-driven approach will form a modern, digitalised system capable of managing the air littoral, where drones, loitering munitions, artillery trajectories, electronic warfare effects, and counter-unmanned aircraft systems operate simultaneously. Through the occupation of airspace, autonomy, mass, and networking, drones are becoming instruments that will redefine the tempo and geometry of the battlespace, supported by modernised technology, updated doctrine, and adaptive organisational structures across both air and land operations.

Technological ecosystem.

The future technological landscape of digital airspace is shaped by the comprehensive integration of digital infrastructure, the increasing autonomy of drones, and the need for interoperable, resilient systems. Supporting a distributed, real-time, AI-enabled airspace control architecture depends on well-established structures that integrate continuous multi-sensor fusion coverage of the air littoral, advanced command and control systems, multi-domain sensors, and robust networks capable of operating in contested, cluttered environments. In Sauser's vision (2026, p. 141), multilayered defensive systems using networked radars, acoustic sensors, and electro-optical systems would establish overlapping coverage from the ground up to the stratosphere. Although he describes this primarily as 'a capability to distinguish hostile drones from friendly systems', such a network would also directly support the broader aims of the digital airspace control concept.

As Ukraine's experience shows, drone capabilities rely heavily on an expanded ecosystem of private technology companies that provide critical digital infrastructure, including cloud computing, communications, data-sharing platforms, cybersecurity, satellite imagery, and internet connectivity. This civil–military sensor network provides

most data used in decision-making and targeting processes. It also centralises drone operations within a digitalised command-and-control system, taking over data collection, connectivity, fusion, analysis, and targeting functions (Kunertová, 2025, p. 15). Consequently, it is essential to anticipate interoperability challenges in airspace control and battlespace management as diverse drone systems and sensor networks are integrated into the air littoral, particularly in terms of how they interact with other unmanned aircraft when operational conditions require it.

A drone's level of autonomy is another significant factor that shapes how force, time, and space interact. Autonomy distinguishes drones from traditional weaponry or manned aircraft and determines how they can be employed (Sotoudehfar and Sarkin, 2023, p. 161). It also influences the development of the digital airspace control system and the way drones interact within the littoral. Both the platform's autonomy and the degree of automation in airspace management are critical. Whether a drone is autonomous, semi-autonomous, or human-controlled, each category entails distinct operating conditions that must be considered in future airspace control frameworks. The same applies to more advanced and collaborative AI-driven drones that are to operate primarily in two areas: autonomous targeting and swarm command, as AI can allow them to continue the mission even under jamming, without a navigation or communication link for an adversary to disrupt (Kunertová, 2025, p. 19-20). However, such capabilities depend on reliable data and stable patterns, so discrepancies can lead to safety failures and compromise real-time, dynamic airspace control.

Nevertheless, from the interoperability and resilience aspect, drones remain vulnerable to electronic warfare, directed energy weapons, cyber threats, or GPS-based (Global Positioning System) navigation attacks, such as jamming and spoofing. These vulnerabilities require additional configurations to exploit brief spectrum gaps (Davis, 2025, p. 85; Lavers, 2025, p. 44) and to ensure compatibility with future digitalised airspace control methods. Technological resilience depends on mesh networking, frequency agility, encrypted links, and fallback modes for degraded communication.

Organisational landscape.

The future organisational landscape of digital airspace will recognise that control of the air littoral is ‘a joint problem, not solely the responsibility of the air force, army, navy, or marines’ (Jackson and Arrol, 2024, p. 57). As a result, structures will need to be adjusted with combined arms capabilities to ensure that drone-enabled effects are fully synchronised across the force. Thus, an integrated air-land operations and defence design, aligned with broader airspace utilisation and extending down to the micro level (Tourret, 2025, p. 12), nesting both ground-based air defence assets and aerial - and missile defence capabilities, requires land force leaders to develop a deeper understanding of (micro or air littoral) offensive and defensive counter-air operations (Jackson and Arrol, 2024, p. 63). Regardless, the optimal future solutions for establishing jointness and integration will depend on the specific state context, the size of the forces and the extent of the air littoral. In this environment, the air component must leverage its flexibility, versatility, and persistence to deliver effects in areas where ground forces are thin (Jackson and Arrol, 2024, p. 66). Here, Ukraine has led the way by creating a dedicated branch, the ‘Unmanned Systems Force’, for the operational employment and doctrinal development of unmanned systems across land, air, and maritime domains (Sauser, 2026, p. 132; Kunertová, 2025, p. 9, 12; Tourret, 2025, p. 14).

When civil and military drone models are adopted too quickly and without standardised hands-on training, the resulting safety and interoperability challenges, created by interface constraints across the diverse drone arsenals of allied countries, must be carefully considered (Kurnetová, 2025, p. 14). Moreover, because effective digital airspace control depends on shared understanding and trust among the involved services and components, increased dialogue and joint airspace training must become a collective effort (Jackson and Arrol, 2024, p. 61). That will shape the organisational framework within which the qualification standards must be achieved through comprehensive training and exercise. Ukrainian Unmanned Systems Force’s approach to standardising training programs demonstrates that capabilities development must be consistent across tactical- to strategic-level operators and planners, maintenance providers, technology developers, procurement agencies, suppliers, and civil contractors (Sauser, 2026, p. 133).

Doctrinal framework.

The future doctrinal framework of digital airspace will shift from platform-based thinking to systems-of-systems thinking, enabling diverse platforms to connect, make decisions, and act collectively (Rossetti, 2021, p. 28). This shift implies that militaries should optimise their resources to align the most effective shooters, sensors, and C2 nodes, thereby clarifying doctrinal roles and responsibilities for the coordinated employment of forces within the air littoral (Jackson and Arrol, 2024, p. 66). In this way, the conduct of operations comes to resemble an organic reconfiguration of strike assets, with innovation, rather than manoeuvre (Tourret, 2025, p. 13). As Davis notes, ’new platforms and tactics eventually stabilise into doctrines’ (2025, p. 77), underscoring the need for deliberate conceptual development rather than ad hoc adaptation. In this regard, Sauser (2026, p. 140) emphasises that updates to manuals should not be merely editorial but should reflect genuine doctrinal evolution. He argues that these fundamental reconsiderations should be incorporated into doctrine and guidance, including how drones operate in mass or swarm, how they are concentrated and contested within the battlespace, and how their employment increases tempo across the distinct phases of the battle rhythm. This, in turn, creates the prerequisite for shaping a cognitive, entrepreneurial, and legal environment that enables individuals within the forces to exercise technical initiatives in operating drones (Tourret, 2025, p. 16). The same dynamics should also drive adaptations to existing conventional airspace control doctrine, requiring operators and commanders to develop a mutual understanding grounded in new skills and a new mindset. As Jackson and Arrol (2024, p. 60) note, this mutual understanding is sometimes absent in the relationship between the army and the air force, partly because the army does not always view the Earth's surface as a domain boundary.

Looking ahead, the future of military airspace control in the air littoral will be highly dependent on resilient digital infrastructure, interoperable systems, and increasing levels of autonomy. As drones become capable of operating in extremely dense, contested environments, the real-time, AI-enabled architectures will replace traditional, human-centred models. Still, these advances will also raise new vulnerabilities that demand robust resilience and careful integration across a diverse range of drones. All

in all, these trends show that effective command and control of the air littoral from the airspace control system perspective will rely on technologically enabled, interoperable, and adaptive systems capable of managing a drone-saturated battlespace.

Conclusion

In sum, the idea that *' The future is now'* has taken on a new meaning in today's conflict-ridden world. Every day, new researches expand the possibilities for drone employment in the future. At the same time, ongoing technological advancements and their testing in Ukraine and the Middle East continue to accelerate their integration into modern warfare. The 'drone dilemma' in the air littoral is inherently a joint problem, driving changes across technology, doctrine, and organisation consistent with the theory of the Revolution in Military Affairs (RMA). These are forcing militaries to adapt new conceptual approaches and operational methods, as the air littoral becomes an increasingly contested airspace layer shaped by drones, loitering munitions, and cheap precision weapons.

The thesis of this research paper argued that drones are transforming the air littoral into a dynamic, networked, and all-domain digital airspace, compelling militaries to reassess the conventional airspace control system and make necessary adaptations. Across the study, a broad overview of the evolution of military aviation and airspace use is provided, tracing the emergence of the concept of the air littoral and the gradual rise of unmanned aircraft as credible competitors to manned aircraft in this layer of airspace. Contemporary conflicts demonstrate that the air littoral has become the primary near-surface battlespace for air-land integration. However, critical reflection is required before adopting emerging practices, given the ongoing nature of drone innovation and the influence of national and environmental factors arising from the Russo-Ukrainian conflict.

As the air littoral becomes more technologically dense, airspace control will increasingly rely on digital and autonomous systems. The traditional airspace control model, centralised, slow, radar-based, and heavily dependent on human operators, is expected to give way to a real-time, distributed, sensor-fused, and AI-supported system capable of managing the demands of future operations. This evolution

underscores two requirements: restructuring the airspace control system to accommodate large numbers of autonomous and semi-autonomous drones, and adopting a genuinely joint doctrinal approach, as no single service can manage this environment alone.

While this research paper does not address all the factors and conditions involved in transforming the conventional near-surface layer of airspace control systems into a digitally enabled air littoral, it offers a broad overview of how military airspace is evolving in response to technological change and the intensified contest over drones. It highlights the doctrinal and organisational adjustments required to adapt to this emerging environment. Future studies should further explore these issues, including the development of interoperable command-and-control structures, the impact of massed autonomous systems on airspace control systems, and the institutional reforms needed to sustain innovation at scale.

Bibliography

Bremer, K. Maximilian, and Grieco, A. Kelly. 2024. Contesting the Air Littoral. *Æther: A Journal of Strategic Airpower & Spacepower*. Vol 3, No 3, 2024, p. 10-24.

Bremer, K. Maximilian, and Grieco, A. Kelly. 2021. The Air Littoral: Another Look. *The US Army War College Quarterly: Parameters*. 2021. Vol 51, No 4, p. 67–80. DOI:10.55540/0031-1723.3092.

Cohen, A. Eliot. 1996. A Revolution in Warfare. *Foreign Affairs,* Vol 75(2), p. 37–54.

Davis, Eric A. 2025. Drones and the Changing Character of War. *Parameters*. Winter 2025-26, Vol 55, No 4, p. 74-97. DOI: 10.55540/ 0031-1723.3369

Douhet, Giulio. 2003. *The Command of the Air.* Upendra Arora for Natraj Publishers, Dehradun. New Delhi: Gay Printers.

Güleç, Erhan, and Kelley, Shawn. 2025. Integrating the Blue and Green Domains. Evolving NATO Air-Land Integration for Multi-Domain Operations. *The Journal of the JAPCC*. 2025, Ed. 40, p. 32–40.

Hutto, James Wesley, and Rogers, James Patton. 2025. The Drone Revolution: Towards a Synthesis in the Drone Debate. *European Journal of International Security*. 2025, p. 1-21.

Jackson, Kevin L., and Arrol, Matthew R., 2024. Defending and Dominating the Air Littoral. *Æther: A Journal of Strategic Airpower & Spacepower*, Vol. 3, No. 4, Winter 2024, p. 56-69.

Knox, MacGregor, and Murray, Williamson. 2001. *The Dynamics of Military Revolution, 1300–2050.* Cambridge: Cambridge University Press.

Kunertová, Dominika. 2025. Embracing Drone Diversity: Five Challenges to Western Military Adaptation in Drone Warfare. *King's College London, Freeman Air & Space Institute.* [Online] April 2025. [Cited 21 February 2026.] https://www.kcl.ac.uk/warstudies/assets/paper-29-dr-dominika-kunertova.pdf.

Lavers, Christopher. 2025. The Threat Posed by Commercial First-Person-View (FPV) Unmanned Aerial Vehicles (UAVs) Modified by Asymmetrical Warfare Actors. [ed] Tracey German, Fotios Moustakis and Andrew N. Liaropoulos. *The Co-Evolution of Technology and Warfare*. London: Routledge, 2025.

NATO. 1961. *Aspects of NATO: Airspace Co-ordination*. Paris: NATO Information Service. [Online] 2014. [Cited: 28 November 2025.] https://archives.nato.int/uploads/r/null/1/3/137418/0115_Aspects_of_NATO-Airspace_Co-ordination_1961_ENG.pdf.

NATO AJP-3.3. Allied Joint Doctrine for Air and Space Operations. Edition B, Version 1, Effective from 8 April 2016.

NATO AJP-3.3.5, Allied Joint Doctrine for Airspace Control. Edition C, Version 1, Effective from 5 March 2024.

Paris Convention, 1919. *Regulation of Aerial Navigation*. Treaty Series no 14, 1923. London: H.M. Stationery Office. [Online] [Cited: 01 January 2026.] https://treaties.fcdo.gov.uk/data/Library2/pdf/TS0014.1923.pdf.

Rossetti, Livio. 2021. Future Battlespace Management. Fighting and Winning in the Increasingly Complex Air Operations Environment of the Future. *The Journal of the JAPCC*. Winter/Spring 2021, Ed. 31, p. 26–31.

Sauser, Mark. 2026. Constrained Innovation: Drones and the Russo-Ukrainian War. *Survival*. February-March 2026, Vol. 68, 1, p. 127–148.

Sotoudehfar, Saba, and Sarkin, Jeremy Julian. 2023. Drones on the Frontline: Charting the Use of Drones in the Russo-Ukrainian Conflict and How Their Use May Be Violating International Humanitarian Law. *International and Comparative Law Review.* 2023, Vol 23, Issue 2, p. 129–169. DOI: 10.2478/iclr-2023-0018.

Tourret, Vincent. 2025. Design, Destry, Dominate: The Mass Drone Warfare as a Potential Military Revolution. *Ifri Papers*. Paris: Institut français des relations internationales (Ifri). [Online] 2025. [Cited: 08 March 2026.] https://www.ifri.org/en/papers/design-destroy-dominate-mass-drone-warfare-potential-military-revolution.

United Nations. 1944. *Convention on International Civil Aviation*. United Nations Treaty Series, Vol. 15, No 102. Chicago: UN, 1944.

Weller, Kevin; Janke, Christian; Holaschke, Michael, and Walthier, Bastian. **2025**. Liminal UAV Warfare: Categorising Littoral UAVs and Their Impact on the Colonisation of the Air Littoral. *The RUSI Journal*. 2025, Vol 170, Issue 6-7, p. 54-64. DOI: 10.1080/03071847.2025.2589829.

MAJ Scott GUTHRIE: AI, AGI and Asymmetric Defence: Estonia's Digital Advantage

Supervisor: CAPT (N) (ret) William 'Bill' COMBES

Statement on the Use of AI Tools:

Claude was used to brainstorm theses, and to refine these further. These were then copied into Word and modified to increase the writer's interest and ownership of the topic. Deep research literature searches were conducted with both Claude and ChatGPT to gather an initial literature base. ChatGPT was used to summarise each part of the of source material—after each source was read—and these summaries were used in a limited manner for recall while writing the paper. The summaries were not copied for writing. AI was not used to generate text or arguments. When the author could not find relevant source material as writing was ongoing, additional literature, news, and think tank searches were conducted with AI in order to expand usable source material. Once the major arguments were written, Claude was used to organise material into an outline. This was used for structure, as the content was already generated by the writer. ChatGPT was also used to brainstorm the limitations section, as the writer found it helpful to pick apart some of the paper's arguments. No text was copied, though 2 of the AI-generated ideas for limitations were used (written and expanded upon by the writer). Once the essay was complete, Grammarly was used to check grammar and spelling, though significant syntactical suggestions were ignored. My supervisor also used Claude (Anthropic) and Copilot to assist with supervision.

Introduction

In just four years, expert forecasts for artificial general intelligence (AGI) development have collapsed from 50 years away to a mere five years, with a 25% predicted probability of AGI emerging by 2027 and 50% by 2031 (Todd, 2025). Estonia has specifically recognised the growing importance of frontier AI models in the defence sphere and so has committed to allocating 30-50% of the annual defence R&D budget for developing defence AI, while committing to considerable increases in defence spending across the board (Kaitseministeerium, 2025).

This paper will use OpenAI's Charter definition of AGI as 'highly autonomous systems that outperform humans at most economically valuable work' (*OpenAI Charter*, 2018) with the important caveat that AGI is a continuum which encompasses everything from emerging AGI—which arguably already exists in frontier models—to superhuman, which is plausible but still theoretical (Morris et al., 2025).

The sense of urgency in preparing for conflict is understandable in the light of Russia's invasion of Ukraine. With a small territory offering limited strategic depth and a population of around 1.3 million, Estonia faces major challenges defending its 294-kilometre border with Russia and its population of 144 million. NATO's new force model enables greater deterrence through the forward positioning of more members' forces, including in Estonia. However, if an attack did come, the 0-10 day, 30-day, and 180-day mobilisation timelines (Deni, 2024) may be too late for Estonian and greater Baltic defence, with potential aggression scenarios measured in hours rather than weeks (Robert Lansing Institute, 2025). Estonia's 2025 defence AI strategy describes the situation well: 'Considering Estonia's small territory and limited resources available for defence, applying technological solutions, similarly to Ukraine, is vital for Estonia' (Kaitseministeerium, 2025).

Artificial intelligence technologies, specifically frontier AI systems, represent just such an asymmetric technological solution. Rapid advancements in frontier AI technologies and the removal of limitations for integration with defence development show that there

is great potential in this area (Evans, 2025). Additionally, the last few months have shown that well-equipped single actors can have an impact size that was previously reserved for large teams or networks, levelling the cyber playing field significantly for small states. Defensive uses of frontier AI models are also now useful for cyber defence ‘in practice, not just in theory’ (Anthropic, 2025), meaning that a state with highly digitalised infrastructure and an entrepreneurial base in technology fields can punch above its weight class in both the physical and the digital world. These effects are only likely to become more pronounced as frontier AI models continue to grow on the AGI capabilities continuum.

With this in mind, the thesis of this paper is that frontier AI model growth and potential AGI emergence by 2035 will asymmetrically benefit Estonia's defence and deterrence capabilities relative to Russian offensive capabilities, because current AI and potential future AGI amplify existing digital infrastructure advantages and reward rapid adoption and adaptation over military mass.

This paper will be relevant to NATO generally and to Estonian security specifically. It will contribute to deterrence theory by examining existing theory, its adaptation, and its application to small states in the context of ongoing and accelerating advances in the field of AI.

The roadmap for the paper is as follows: firstly, there is an examination of deterrence theory through the lens of frontier AI system capabilities and their likely abilities in the near future, given current AI use in the Ukraine conflict. This is followed by a discussion of Estonia’s digital infrastructure advantages. Next, the asymmetric defensive benefits of AGI for a capable small state are presented, after which potential deterrence mechanisms are showcased. Lastly, there is a discussion of limitations, followed by the conclusion.

Deterrence theory and current AI use in war

The academic literature on deterrence is wide and varied, spanning decades and multiple shifts and divergences in opinion. Taking this into account, this paper will primarily use Mazarr’s succinct analysis and summary written for RAND to gain a basic

understanding of the current status of deterrence as an idea. Deterrence theory emerged as a set of strategic concepts after World War II as nuclear powers wrestled with how to integrate apocalyptic weapons into national defence policy while working to ensure the same weapons would never be used against them.

Though nuclear deterrence is still a mainstay of great power security strategy, deterrence as a concept has widened to include conventional and hybrid warfare and can be defined in modern terms as the ‘nuanced shaping of perceptions so that an adversary sees the alternatives to aggression as more attractive than war’ (Mazarr, 2018, p. 2). Successful deterrence depends on three variables: the level of aggressor motivation, the clarity of deterrent communication, and the aggressor’s belief in the deterring state's capability and will (Mazarr, 2018, p. 8-10). For Estonia, the principal identified threat actor is the Russian Federation (Kaitseministeerium, 2023). The level of motivation for an imminent invasion of the Baltics is unclear, but Putin does have clear long-term ambitions to ‘restore’ what he sees as ‘historically Russian lands’ (Dickinson, 2025). With aggressor motivation difficult to control, clarity of communication and demonstration of capability and will are the remaining levers for deterrence. The rapid development of frontier AI systems and AGI presents a uniquely-timed opportunity to manipulate these levers.

In the traditional calculus, the deterrence variables mentioned above favoured mass. State capability has been determined by the number of fieldable divisions or by GDP. Small states such as Estonia have therefore been unable to deter large powers alone. However, if this calculus shifts from mass to the speed of adaptation, it changes fundamentally, because potential aggressors are no longer able to rely on differences in mass alone to determine capability mismatches. This is exactly the sort of change that AI, and eventually AGI, are poised to deliver.

Research and development in the field of artificial intelligence has been ongoing since the 1950s. Though they existed since around 2018, large language model (LLM) advances in 2023 introduced the public at large to breakthroughs in AI brought about in large part through unsupervised learning and self-optimisation with training on massive datasets (Marr, 2023). These breakthroughs have drastically shortened estimates of timeframes for the emergence of AGI; ‘in four years, the mean estimate

on Metaculus for when AGI will be developed has plummeted from 50 years to five years' (Todd, 2025). Shrinking timelines have led thinktanks such as RAND to tackle the issue as AGI or even superhuman level intelligence are deemed to be 'plausible' in the near term and present security problems with no current clear solutions (Mitre, Predd, 2025).

Contemporary Examples of AI in the Ukraine Conflict

The initial invasion of Ukraine was dubbed a 'special military operation' and experts in the West, as well as in Russia, expected Kyiv to fall in a matter of days, with the government and military lasting a few weeks at most (Naveed, Brennan, O'Connor, 2022). This, in retrospect, hugely underestimated the Ukrainians' will and capacity to resist and the political will in the West to materially support this resistance. What made Ukraine capable with such asymmetry of conventional forces? It was initially thought to be their innovative use of drones for ISR and direct strikes. However, the ability to rapidly adapt has proved to be the most powerful weapon in the conflict. With 'AI support[ing] decision-making, intelligence processing, and targeting, [...] what makes Ukraine's achievements particularly impressive is the speed of change in the doctrine of warfare' (Kaitseministeerium, 2025).

Stated simply, AI has been integral to this war of adaptation. As an example, in Ukraine, the targeting, command and control and situational awareness comprising the 'nervous system' of the battlefield, are enabled by AI-powered DELTA and Avengers digital combat platforms. This is accelerating the speed of battle to a jarring pace, with kill chain decisions being made in seconds, even when vehicles are camouflaged or in non-ideal weather conditions (Digital State UA, 2025).

Though Ukraine's use of AI to enable rapid adaptation is more than impressive, a paradox immediately arises. If Ukraine has so successfully integrated AI and Russia has continued incurring massive losses (Lendon, 2026), why is the conflict still ongoing? The most intuitive explanation is that the deterrent and combat advantages of AI systems are overblown and are inadequate for a determined adversary. However, it is likely the truth is more complex.

As described above, the first highly capable LLMs did not emerge until 2023, with the Ukraine conflict already ongoing, and therefore could not have factored into Russia's original risk calculus. Additionally, as Russia underestimated Ukraine's ability and will to defend itself, Putin has faced subsequent pressure for success. As a result, he has doubled down on the conflict because a perception of failure within Russia could amount to an existential threat to his power. Therefore, it may be that the deterrence variable of aggressor motivation is extreme in this case and cannot be overcome by conventional deterrence, even with amplified losses from AI-enabled systems. A last potential consideration is Ukraine's lack of NATO Article 5 protection, which lowers the perceived cost of aggression. Estonia is not similarly isolated, and the increased uncertainty brought about by AI could tip the deterrence scale.

The story from Ukraine confirms that, even when deterrence seems to have failed, rapid, AI-enabled adaptation can enable a numerically inferior force to endure well past what traditional capability comparisons would suggest would be possible. The implications for Estonia are clear. The question becomes whether Estonia also possesses the requisite institutional mechanisms to ensure this rapid adaptation. An abstract list of potential tech assets is inadequate. There must be a true culture of rapid adoption and adaptation to provide a mechanism through which it can communicate capability and thereby influence Russia's threat calculus.

Estonia's Digital Infrastructure as an Enabler of AI, Adaptation, and Deterrence

Estonia is a highly digitally capable state. It is 'widely considered one of the most technologically advanced nations in Europe, and much of its private sector expertise is signed up for a "cyber militia"' (Freedberg, 2025). Its government functions are 100% digitalised as of 2024. They are secured through the open-source X-Road software ecosystem. This system has been resilient against cyber attack with 'no known major security breach involving X-Road' (Marak, 2025; e-Estonia, 2024a; Vassil, 2016).

Nationwide, mandatory two-factor authentication ensures citizens can securely interact with online services, and the Estonian-designed KSI blockchain enables distributed consensus with near-complete transparency and security. This means that no one, from hackers to the government, can manipulate data without the alterations being

visible to all (e-Estonia, 2024b). KSI blockchain implementation by Estonia at an architectural level after Russian cyberattacks in 2007, demonstrates a digital security focus at a national level (Semenzin, Rozas, Hassan, 2022).

The sophisticated triad of Smart-IDs, X-Road and KSI blockchain in its ‘Secure by Design’ digital infrastructure makes it highly resilient and usable for secure work. It is also capable of rapid adaptation with new AI-based businesses and defence applications easily integrated into the ecosystem. A highly secure and resilient national digital infrastructure is an example of deterrence by denial, with demonstrated capabilities making it unlikely for adversaries to achieve their goals in the cyber domain. In addition to its broad-based foundation of digitisation and digital security plus resilience, Estonia is also a leader in the field of cyber defence.

As part of its response to massive Russian cyberattacks in 2007, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) was established in Tallinn in 2008, and Estonia remains the permanent host country as well as a regional hub office of DIANA, a NATO defence innovation accelerator (Clement, 2024). CCDCOE organises annually the largest and most complex live-fire cyber resilience exercise in the world—Locked Shields—with over 2000 participants from 32 nations. Five other major NATO exercises are hosted or supported by the CCDCOE annually. This robust collaboration with allies in offensive and defensive cyber operations is well-publicised. In deterrence terms, it represents efforts to reinforce any aggressor’s belief in Estonia's capability and will to fight in the cyber domain, along with opportunities for clear deterrent communication.

The focus on defence sector cybersecurity and operations also attracts entrepreneurs with Estonia’s ‘agile start-ups and small or medium enterprises [...] emerging as a significant driver of defence AI development’ and more than a dozen companies implementing AI in their processes or products. Additionally, international projects involving Estonian companies secured over half a billion euros of funding in 2023 alone (Jermalavičius, 2024; Kaitseministeerium, 2025).

Estonian national policies also make it relatively easy for this defence innovation to occur, as they systematically encourage an environment that benefits startups,

especially in the digital sector. Tax competitiveness encourages rapid small-business growth. The e-residency program opens up a large European customer base to foreign entrepreneurs while adding their talents to the start-up scene. Programs like Accelerate Estonia ensure that adaptation and flexibility are baked into government structure and policy. This allows for both public and private sector organisations to remain agile in the face of emerging opportunities and threats.

Estonia's cyber infrastructure, its cooperation with allies in the cyber domain, and its agile startup ecosystem create a system that is more than just the sum of national strengths. It promises to decouple mass from military capability in the age of AI. Conventional capabilities scale with population and industrial production, but AI-enabled capabilities scale with adoption and adaptation speed. Estonia's digital system is purpose-built for modular adoption of new capabilities as technology advances. While Russia can always field more conscripts or produce more artillery ammunition, it cannot easily change its entire digital infrastructure or business environment. As AI continues to advance, this adaptation speed gap will become crucial for defensive and deterrent advantages.

Defensive Advantages of AI Integration

Since Estonia is a digitally optimised state whose defence sector and agile start-up ecosystem are readily integrated with frontier AI models and, eventually, AGI, it is worth considering the defensive advantages that could be gained by adopting this revolutionary technology to the greatest extent possible. This section will discuss a small number of advantages—non-exhaustive examples—to be gained at the technology's current level, as well as speculatively with the emergence of AGI.

As an initial example, in the realm of defensive cyber operations, defenders have historically had the advantage of choosing the 'terrain' as they have control of how systems are set up and administrated. Attackers, in turn, can choose any point on the attack surface to conduct their operations. When dealing with an adversary with greater mass, two historical issues for defenders have been scale and speed: the sheer amount of attack surface that exists for any given program, and the ability for attacks to propagate at machine speed while human defenders lag behind looking for solutions

(Withers, 2025). More attack surface typically means more vulnerabilities and bugs. Servers being spread across time zones means fewer humans are available to defend them at any given hour. Rapidly spreading attacks have enabled attackers to accomplish their missions before solutions are found.

AI provides a unique solution to these problems of mass. If thousands of defensive AI 'agents' are continually inspecting and probing the attack surface for potential issues, they are 'likely to further harden the broader digital ecosystem [...] [by] review[ing] code or organisational practices for security vulnerabilities and adapt[ing] them to adhere to best practices' (Lohn, 2025, p. 71). This army of agents could also recognise a new vulnerability, phishing target, or malware application being actively exploited and patch it before any real damage could be done.

In the past, this was not realisable due to the resource burden and diminishing returns involved in securing, probing and hardening systems at scale, let alone in real time. Modern AI capabilities make it possible (Withers, 2025). AGI emergence would make it both easier and cheaper. Estonia's current digital infrastructure is a perfect setting for this kind of systematic hardening. If Estonia's critical infrastructure, communication networks, early-warning radar, command-and-control systems, etc., are significantly more resilient, this does a great deal to enable cost-effective defensive warfighting as a small state.

In kinetic terms, an example of how AI integration can bolster defence is through autonomous or semi-autonomous defensive weapons. An example of this is Israel's Iron Dome, which uses AI-powered algorithms to recognise, categorise, and counter incoming airborne threats (Laje, 2024). Ukraine has also integrated AI into its air defence systems. It has been able to repel combinations of cruise and ballistic missile attacks which would have proven difficult or impossible for traditional human-based teams (Kaitseministeerium, 2025).

Further development in this direction, especially with frontier AI models and AGI, could even allow for defence against massive swarms of cheap drones, cruise missiles, and ballistic missiles of the style that overwhelm even the best modern defences. An advanced AI could quickly recognise the slower speed or signature of drones and

automatically deploy counter-drones and other inexpensive loitering munitions to counter these threats, while saving the more expensive interceptor missiles for faster-moving targets. This would protect targets and ameliorate the current economic attrition imbalance brought about by munitions price disparities, which a small state like Estonia could not sustain in the long term. AGI could also be integrated with future advances in air defence, such as directed-energy weapons, to further shift the battlefield balance back to the defender, even when this defender is a small state and less numerous or possesses fewer resources.

A third defensive advantage is decision-making and decision speed superiority. This is already being witnessed on both sides of the Ukraine conflict, but with Ukrainian forces embedding AI into their C2 and battlefield awareness systems. These systems can recognise and respond to threats in real time, far outstripping human processes and reaction times. This ‘Super-OODA loop’ shrinking from hours to seconds effectively removes the attacker’s traditional advantage of surprise and redefines the offence-defence balance on the battlefield (Raksa, 2025). A true AGI could fully automate this process, making any non-machine coordinated attack much less likely to succeed. Despite real risks of machine miscalculation and escalation, compounding advantages result. As retired Royal Navy Adm. Radakin stated in a recent interview, ‘Whoever reaches artificial general intelligence, and then artificial super intelligence, will be the ones with an enormous military advantage [...] And if ASI means I fall one second behind my opponent, I may never catch up’ (Radakin, 2025).

In addition to cyber, kinetic, and C2 defensive advantages, frontier AI models and AGI also offer a chance to offset economic and manpower disadvantages inherent to a small state. For instance, digital information warfare is cheap and effective, making it a ‘perfect’ asymmetric weapon. Russia spent only four million USD on their most high-profile information operation in the US (Polyakova, 2018). AI and AGI integration into targeted information campaigns would further reduce costs and personnel requirements and increase effectiveness. AI-driven automated and unmanned systems also decrease the manpower losses that a relatively small organisation like the Estonian Defence Force cannot afford in the face of a more populous adversary (Jermalavičius, 2024).

This section has outlined examples of defensive advantages to be gained through AI adoption and integration. The key similarity of the above defensive advantages is that none of them depend on the mass of the force employing them. They instead scale based on the quality and speed of integration into existing systems, something Estonia's infrastructure is primed to deliver. But defence and deterrence are not the same thing. The question remains of how potential defensive advantages can effectively provide deterrent signalling.

Deterrence Advantages with AI integration

For a country in a defensive alliance like NATO, deterrence is at least as important as defence. This section will discuss a limited number of deterrence opportunities enhanced or enabled by AI in a small, digitally capable state like Estonia. Offensive cyber capabilities could theoretically be applied to persuade adversaries of a state's capability and will. The current problem with using them for deterrence is that the offensive cyber operations of a state are inherently classified (Kosseff, 2019). This is to prevent the adversary from gaining knowledge of capabilities, prevent escalation in competition or conflict, and preserve expensive and hard-won cyber advantages.

This could all change with AGI. 'AGI could cause a systemic shift that alters the balance of global power [...] [and] upend military balances by uplifting a variety of capabilities that affect key building blocks of military competition' (Mitre, Predd, 2025, p. 4). If the cost of acquiring and fielding offensive cyber abilities—both in time and money—is dramatically reduced, then the idea of 'defending forward' through intermittent disruption of adversary military capabilities through cyber attack could be a viable, though risky, approach to deterrence.

Also, in the cyber domain, leveraging the capabilities of AGI to return to the original nuclear deterrence theory is useful. The idea exists of creating an AGI-powered 'splendid first cyber strike that completely disables a retaliatory cyberstrike' (Mitre, Predd, 2025). It would be difficult to demonstrate this capability, but its crippling potential could be a potent deterrent against a large state if realised.

For physical operations, integrating AI into automated border defence could upend the current risk calculus for adversary incursions. The Baltic Defence Line is an ongoing project to harden the border with Russia by using a combination of explosive and non-explosive barriers, combined with strongpoints (Riigi Kaitseinvesteeringute Keskus, 2025). These relatively passive defences could be enhanced by 24/7 monitoring, threat analysis, and automated response. Existing Estonian defence companies can already provide integrated drone stations, smart cameras, and AI-driven C2 software to monitor and defend the border (Vihma, 2024). During peacetime, this sort of system could be hardwired and scaled for remarkable resilience and resistance to electronic warfare, allowing a small number of Estonian personnel to effectively monitor and rapidly respond along the border against a numerically superior foe.

The amount of ‘Human in the Loop’ for kill chain decisions could be adjusted from semi to fully automated and back again based on the evolving threat picture, political appetite, and type of threat identified. The right system, with the right frontier AI or even AGI, could dramatically reduce the costs for defenders to cover the entire border in real time and increase the risks for attackers, even for ‘routine’ probing incursions or special reconnaissance missions. Publicity about an AI-guarded border and ultra-rapid response would offer clear deterrent communication. A few botched missions into Estonian territory with high-profile Russian losses would increase deterrent credibility through action.

As with the defensive advantages, the deterrence opportunities discussed above exploit speed and uncertainty instead of mass. For Estonia, the implication is that deterrence can be reframed at a base level. The credibility message is not that cost can be imposed on the aggressor through resistance and attrition over time, but rather that disproportionately high and uncertain costs can be inflicted before the mass can be brought to bear. This shifts the advantage from mass to agility.

The Game is Changing: Why Agility Beats Mass in the World of AI and AGI

Though the above-noted defensive and deterrent advantages of AI and AGI represent shifts in the offence-defence balance of war, it could be argued that offensive advantages could offset these gains. However, in Estonia's case, there is reason to

believe this will not be the case. As discussed in an earlier chapter, Estonia is primed to rapidly adopt and integrate AI and AGI breakthroughs due to its robust and secure digital infrastructure, as well as its agile startup ecosystem, both encouraged by state policy. As RAND's analysis argues, 'Cultural and procedural factors drive an institution's technological adoption capacity and are more consequential than being the first to achieve a scientific or technological breakthrough' (Mitre, Predd, 2025, p. 4). Estonia's Ministry of Defence has also embraced this idea and acknowledges that AI and autonomous systems represent a chance to create asymmetric advantages against an adversary of larger mass (Kaitseministeerium, 2025, p. 4).

In contrast, despite its proven ability to adapt on the battlefield in Ukraine, Russia does not share the same institutional culture regarding AI technology. Russian political and military leaders seem stuck in a narrow view of AI's rapidly developing capabilities, insisting on its usefulness for specific tasks, but not for system-transforming input and oversight (Fink, 2021, p. 2-3). Though Russia has genuine technical talent, the systemic differences between Estonian and Russian approaches to defence AI could lead to compounding advantages for the smaller state as advances beget further advances.

AI is an amplifier of existing systems and will multiply what exists in each state, respectively (Peter et al., 2026, p. 17). In this setting, Russia's asset of numerous citizens would be eclipsed by Estonia's smart and adaptive strategies and systems (Dear, 2024, p. 5), which could 'neuter and potentially undermine' Russia's traditional advantage of being a military power with more mass effect, something similar to what is already being seen in today's conventional conflicts (Radakin, 2025).

The resource factor is also likely to swing heavily in the small state's favour as AI technology advances. The current barriers to domination in the world of AI, such as raw compute power, which are keeping wealthier nations at the cutting edge, could change in an instant as unexpected breakthroughs lower resource requirements in the nascent field (Pavel et al., 2025, p. 5). DeepSeek is a recent example of a model which achieves results just inferior to industry leaders, but at a fraction of the development cost due to differences in its training methods and reasoning algorithms (Martens, 2025). This example shows a trend away from scale and toward fine-tuning of models,

which may allow countries with much smaller national budgets to develop economically viable defence AI solutions.

The last and potentially most crucial unknown that AI brings to the traditional offence-defence-deterrence balance is precisely that: the unknown. The future has always been unknowable, but if a true AGI or rather an artificial super intelligence emerges—an AGI which far surpasses human capabilities—then the nature of war will likely become qualitatively different than it is now, and ‘the past will not be a guide to forecast or understand the future’ (Compagnoni, 2023, p. 1).

The cumulative implication of the factors described above is that military mass, which has traditionally been insurmountable in the warfighting calculus, finds its decisive status reduced. When resource barriers to cutting-edge technology are plummeting, and when each new breakthrough can render previous technology and force structures obsolete overnight, the deterrence advantage shifts from the heaviest hitter to the most nimble. For Estonia, this means that the deterrent and defensive advantages discussed in this paper are synergistic, not just additive. The goal shifts from matching Russia’s mass to outpacing its ability to adapt.

Limitations

This paper argues that advances in frontier AI systems and the potential step forward to AGI will asymmetrically benefit Estonia’s defence and deterrence relative to Russian offensive capabilities. The paper's logic is grounded in deterrence theory and further supported by examples from the Ukraine conflict and Estonia’s digital and entrepreneurial ecosystem. However, there are important limitations to this which must be considered.

First and foremost, the argument leans heavily on non-objective forecasting regarding timelines and potential capabilities of AGI. Though the paper defines AGI according to the OpenAI charter and explicitly describes it as a continuum of ability, the absence of a universally accepted definition for AGI makes it difficult to cleanly argue against the thesis. In the same vein, the forecasts quoted in the paper, as well as those present in other source materials, are vulnerable to shifting definitions, technological bottlenecks

and rapid advances. This uncertainty affects the deterrence and defensive advantages emphasised in the paper. As a caveat, it should be noted that these advantages do not depend on AGI emergence. After all, frontier AI systems are effectively utilised in current conflicts. The emergence of AGI would only further enhance them.

Secondly, many examples of potential deterrent and defensive applications of AI and AGI in the paper make reference to the Ukraine conflict. While this conflict provides unique insight into modern applications of technology, it must be noted that Estonia and Ukraine are quantitatively and qualitatively different, from population to area to features of terrain and fiscal resources. Additionally, elements of the Ukraine conflict which are unique, such as massive Western military and financial support, the density of the battlefield spaces, and rapid innovation in the current battle space, may not translate to conflict in the Baltics. This limitation is at least partially mitigated by Estonia's membership in NATO, which provides the alliance depth and access to resources which Ukraine lacked.

Third, the paper's cyberspace-related claims in the realm of deterrence are severely limited by the already-discussed secrecy surrounding cyber operations. Even if AGI significantly reduces the costs of cyber capability development and execution, states will still have strong incentives to keep their most powerful capabilities classified, thereby impairing the clear communication required for deterrent signalling. Ambiguity, by its very nature, however, could provide some benefits to deterrent signalling as Russia must assume the capabilities exist, especially given regular cyber exercises conducted with partners.

Fourth, the paper's core claims regarding asymmetric development of AI and AGI-related capabilities assume that Estonia's policy and start-up environment, as well as its digital infrastructure ecosystem, will continue on course, encouraging a culture of rapid adaptation. Alongside this, it assumes that, in the years ahead, Russia's past organisational and political constraints will remain as they were. However, adversaries can adapt new doctrine, and Russia can make up time and capabilities through espionage and commercial acquisition, especially as AI technology improves and becomes cheaper. Parallel to this, systems which work well today in Estonia can slide into complacency if they are not properly maintained and refreshed. However, it takes

time for change to happen at the national level, and it seems likely that the current rapid adapter will keep adapting rapidly, and vice versa.

Last of all, there are legal and ethical questions which challenge the feasibility of several proposed AI applications in this paper—think automated border defence, flexibility of human input for kill-chain decisions, and pre-emptive cyber attacks. In the face of existential threats, Ukraine has been largely free to defend itself while, in the near term, ignoring or setting aside some of these questions. This will likely not be the case for a NATO member. Rules of engagement, alliance cohesion, escalation management, and other legal and ethical questions will have to be addressed, which could hamper adoption speed to the point of severely limiting any advantages. Importantly though, Estonia's existing role as host of the CCDCOE and DIANA regional hub positions it to shape these frameworks. With this in mind, Estonia has the opportunity to ensure that alliance governance enables rather than constrains the rapid adoption of AI-related technology applications.

Conclusion

In conclusion, this paper has argued that frontier AI model growth and potential AGI emergence by 2035 will asymmetrically benefit Estonia's defence and deterrence capabilities relative to Russian offensive capabilities because current AI and potential future AGI amplify existing digital infrastructure advantages and reward rapid adoption and adaptation over military mass.

The examination of deterrence theory through the lens of AI technology and contemporary examples from the Ukraine conflict gave context. It demonstrated that modern warfighting calculus is shifting from mass to agility, benefitting a small state like Estonia. The examination of Estonia’s digital infrastructure and its policies encouraging a vibrant start-up community highlighted the advantages of its digital infrastructure and its ability to adapt rapidly. Both advantages will be amplified by AI technology and will contribute to the agility advantage, further boosting Estonia’s capabilities vis-à-vis Russia in the age of AI and AGI. Finally, the examination of current and future deterrence and defensive advantages enabled and compounded by this agility gave practical examples of how Estonia can punch above its weight class in the

age of AI and AGI. This will subsequently offer asymmetric benefits in competition with Russia, whose greater mass and slower adaptation are relative disadvantages in this context.

Framed simply through Mazarr's three deterrence variables, this paper showed that AI enables greater uncertainty for attacker costs, which blunts the aggressor's motivation variable, even though it is difficult to control. Estonia's digital infrastructure, both public and within NATO's structure (CCDCOE/DIANA) cover the remaining two deterrence variables through clarity of communication and demonstrations of capability and will.

This argument has implications for NATO. Small states, which historically have lacked the mass needed for large-scale conflict, can serve as the alliance's innovation nexus. While larger states can provide deterrence through mass effect, smaller alliance members can work to ensure that the NATO apparatus remains nimble and relevant in a rapidly changing environment. With this comes a few recommendations. Firstly, Estonia could consider formalising AI milestones within its 2025-2030 window, aligned with the 30-50% defence AI commitment already made. Secondly, Estonia could use its position as host of CCDCOE and DIANA to spearhead NATO development of frameworks for AI autonomy in defence, turning a potential limitation into an advantage. Lastly, NATO could create small-state capability incentives which value agility and technology adoption speed as much as it currently values traditional capabilities.

In conclusion, the very speed of development and opacity which make AI technology so revolutionary also counsel caution and humility when prognosticating about outcomes. The most decisive future advantages brought about by AI may not currently be foreseeable, but could emerge from the interplay between second- and third-order effects in advancing algorithms, automation, politics, and escalation dynamics in a changing world. If AI development crosses the border from current highly advanced frontier systems to a genuine superintelligence, then deterrence may be shaped by the 'unknown unknowns' of the future. The current realities make investments in reasonable, governable AI integration essential. The near-future possibilities make the building of resilient and adaptable institutions an imperative, as the rules of the security environment may change faster than any state is able to adapt.

Bibliography

ANTHROPIC. 2025. Building AI for cyber defenders. *Anthropic*. [Online]. 10 March 2025. [Cited : 12 October 2025]. https://www.anthropic.com/research/building-ai-cyber-defenders.

CLEMENT, Sven. 2024. Nato and artificial intelligence: navigating the challenges and opportunities. *Special Report, NATO Parliamentary Assembly*. [Online]. 24 November 2024. https://www.nato-pa.int/download-file?filename=/sites/default/files/2024-12/058%20STC%2024%20E%20rev.2%20fin%20-%20NATO%20AI%20-%20CLEMENT%20REPORT_0.pdf.

COMPAGNONI, Ares Simone Monzio. 2023. Will Artificial General Intelligence Change the Nature of War? *Military Strategy Magazine*. 11 May 2023. Vol. 8, no. 4. DOI 10.64148/msm.v8i4.5.

DEAR, Keith. 2024. Exploring the Future Operating Environment: 2035-50. *Special Competitive Studies Project (SCSP).* [Online]. December 2024. https://www.scsp.ai/wp-content/uploads/2024/12/DPS-Exploring-the-Future-Operating-Environment-2035-50.pdf.

DENI, John R. 2024. The new NATO Force Model: ready for launch? *Outlook*. 27 May 2024. No. 4.

DICKINSON, Peter. 2025. Reclaiming Russia's 'historical lands': How far do Putin's imperial ambitions extend? *Atlantic Council*. [Online]. 23 December 2025. [Cited : 4 January 2026]. https://www.atlanticcouncil.org/blogs/ukrainealert/reclaiming-russias-historical-lands-how-far-do-putins-imperial-ambitions-extend/.

DIGITAL STATE UA. 2025. Ukraine's Defence Tech Ecosystem: Real-Time Coordination and AI Targeting in Action. *Digital State UA.* [Online]. 3 September 2025. [Cited : 12 January 2026]. https://digitalstate.gov.ua/news/tech/2-sekundy-i-tsil-vyiavleno-iak-pratsiuye-tsyfrova-ekosystema-zsu.

E-ESTONIA. 2024a. X-road – Interoperability services. *e-Estonia*. [Online]. [Cited : 13 January 2026]. https://e-estonia.com/solutions/interoperability-services/x-road/.

E-ESTONIA. 2024b. KSI blockchain. *e-Estonia*. [Online]. [Cited : 13 January 2026]. https://e-estonia.com/solutions/cyber-security/ksi-blockchain/.

EVANS, Scarlett. 2025. OpenAI Awarded $200M Contract to Develop AI for Defense. *AI Business*. [Online]. 19 June 2025. [Cited : 12 October 2025]. https://aibusiness.com/nlp/openai-awarded-200m-contract-to-develop-ai-for-defense.

FINK, Anna. 2021. Russian Thinking on the Role of AI in Future Warfare*. Russian Studies Series* 5/21. [Online] https://www.ndc.nato.int/fr/russian-thinking-on-the-role-of-ai-in-future-warfare/#:~:text=Burenok%20observes%20that%20%E2%80%93%20at,a%20significant%20priority%20for%20the.

FREEDBERG, Sydney J. Jr. 2025. Estonia pledges major investments in military AI. *Breaking Defense*. [Online]. 24 March 2025. [Cited : 28 September 2025]. https://breakingdefense.com/2025/03/estonia-pledges-major-investments-in-military-ai/.

JERMALAVIČIUS, Tomas. 2024. Caught Between Today and Tomorrow: Defence AI in Estonia. In: BORCHERT, Heiko, SCHÜTZ, Torben and VERBOVSZKY, Joseph (eds.), *The Very Long Game: 25 Case Studies on the Global State of Defense AI*. Cham: Springer Nature Switzerland.

KAITSEMINISTEERIUM. 2023. Estonian National Security Concept. *Kaitseministeerium.* [Online]. 22 February 2023. https://kaitseministeerium.ee/sites/default/files/eesti_julgeolekupoliitika_alused_eng_22.02.2023.pdf.

KAITSEMINISTEERIUM. 2025. Defence artificial intelligence strategy for Estonia. *Kaitseministeerium.* [Online]. 2026. Republic of Estonia Ministry of Defence. https://kaitseministeerium.ee/sites/default/files/defence_artificial_intelligence_strategy_for_estonia.pdf.

KOSSEFF, Jeff. 2019. The Contours of ‘Defend Forward’ Under International Law. In: *2019 11th International Conference on Cyber Conflict (CyCon)*. Tallinn, Estonia: IEEE. May 2019. pp. 1–13.

LAJE, Diego. 2024. Iron Dome and the Next Anti-Missile Weapon. *AFCEA International*. [Online]. 1 April 2024. [Cited : 15 January 2026]. https://www.afcea.org/signal-media/international/iron-dome-and-next-anti-missile-weapon.

LENDON, Brad. 2026. Russia’s 1.2 million casualties in Ukraine dwarf all its conflicts since World War II, report says. *CNN*. [Online]. 28 January 2026. [Cited : 3 March

2026]. https://www.cnn.com/2026/01/28/europe/russia-ukraine-casualties-csis-report-intl-hnk-ml.

LOHN, Andrew J. 2025. The Impact of AI on the Cyber Offense-Defense Balance and the Character of Cyber Conflict. [Preprint] [Online]. 17 April 2025. [Cited : 26 September 2025]. arXiv:2504.13371.

MARAK, Sunanda. 2025. X-Road Technology: A digital backbone of Estonia's Cyber security and DPI. *Future Shift Labs.* [Online]. 2025. [Cited : 13 January 2026]. https://futureshiftlabs.com/x-road-technology-a-digital-backbone-of-estonias-cyber-security-and-dpi/.

MARR, Bernard. 2023. A Short History of ChatGPT: How We Got to Where We Are Today. *Forbes*. [Online]. 19 May 2023. [Cited : 4 January 2026]. https://www.forbes.com/sites/bernardmarr/2023/05/19/a-short-history-of-chatgpt-how-we-got-to-where-we-are-today/.

MARTENS, Bertin. 2025. How DeepSeek has changed artificial intelligence and what it means for Europe. *Bruegel*. [Online]. 8 December 2025. [Cited : 16 January 2026]. https://www.bruegel.org/policy-brief/how-deepseek-has-changed-artificial-intelligence-and-what-it-means-europe.

MAZARR, Michael J. 2018. Understanding Deterrence. *RAND.* [Online]. [Cited : 31 December 2025]. https://www.rand.org/pubs/perspectives/PE295.html.

MITRE, Jim and PREDD, Joel B. 2025. Artificial General Intelligence's Five Hard National Security Problems. *RAND.* [Online]. 10 February 2025. https://www.rand.org/pubs/perspectives/PEA3691-4.html#:~:text=This%20paper%20puts%20forth%20five%20hard%20problems%20that,%284%29%20artificial%20entities%20with%20agency%2C%20and%20%285%29%20instability.

MORRIS, Meredith Ringel, SOHL-DICKSTEIN, Jascha, FIEDEL, Noah, WARKENTIN, Tris, DAFOE, Allan, et al. 2025. Levels of AGI for Operationalizing Progress on the Path to AGI. *Proceedings of the 41st International Conference on Machine Learning* [Online]. 24 September 2025. [Cited : 12 October 2025]. arXiv:2311.02462.

NAVEED, Jamali, BRENNAN, David and O'CONNOR, Tom. 2022. Exclusive: U.S. Expects Kyiv's Fall in Days, Ukraine Source Warns of Siege. *Newsweek*. [Online]. 24 February 2022. [Cited : 11 January 2026]. https://www.newsweek.com/us-expects-kyiv-fall-days-ukraine-source-warns-encirclement-1682326.

OPENAI CHARTER. 2018. Charter. *Open AI*. [Online]. [Cited : 12 October 2025]. https://openai.com/charter/.

PAVEL, Barry, KE, Ivana, SMITH, Gregory, BROWN-HEIDENREICH, Sophia, SABBAG, Lea, et al. 2025. How Artificial General Intelligence Could Affect the Rise and Fall of Nations: Visions for Potential AGI Futures. *RAND.* [Online]. 2 July 2025. https://www.rand.org/pubs/research_reports/RRA3034-2.html.

PETER, Sibylle, KROPP, Martin, DINGSØYR, Torgeir, DILLON, Clare, DIEBOLD, Philipp, et al. (eds.). 2026. *Agile Processes in Software Engineering and Extreme Programming – Workshops: XP 2025 Workshops, Brugg-Windisch, Switzerland, June 2–5, 2025, Revised Selected Papers*. Cham: Springer Nature Switzerland.

POLYAKOVA, Alina. 2018. Weapons of the weak: Russia and AI-driven asymmetric warfare. *Brookings*. [Online]. 15 November 2018. [Cited : 28 September 2025]. https://www.brookings.edu/articles/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/.

RADAKIN, Tony. 2025. Reflections on the UK's Role in Defense. *CSIS*. [Online]. 13 August 2025. https://www.csis.org/analysis/reflections-uks-chief-defence-staff#:~:text=It%E2%80%99s%20a%20race%20we%20must,and%2C%20in%20the%20future%2C%20ASI.

RAKSA, Michael. 2025. Reshaping Air Power Doctrines: Creating AI-Enabled 'Super-OODA Loops.' Shift Paradigm. [Online]. 3 February 2025. [Cited : 15 January 2026]. https://theairpowerjournal.com/reshaping-air-power-doctrines-creating-ai-enabled-super-ooda-loops/.

RIIGI KAITSEINVESTEERINGUTE KESKUS. 2025. Baltic Defence Line. Riigi Kaitseinvesteeringute Keskus. [Online]. 2025. [Cited : 9 November 2025]. https://www.kaitseinvesteeringud.ee/en/baltic-defence-line/.

ROBERT LANSING INSTITUTE. 2025. The Suwałki Corridor Crisis: An Analysis of a Possible Russian Offensive and NATO Response Scenarios. *Robert Lansing Institute*. [Online]. 27 May 2025. [Cited : 10 October 2025]. https://lansinginstitute.org/2025/05/27/the-suwalki-corridor-crisis-an-analysis-of-a-possible-russian-offensive-and-nato-response-scenarios/.

SEMENZIN, Silvia, ROZAS, David and HASSAN, Samer. 2022. Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia. *Policy and Society*. 26 July 2022. Vol. 41, no. 3, pp. 386–401. DOI 10.1093/polsoc/puac014.

TODD, Benjamin. 2025. Shrinking AGI timelines: a review of expert forecasts. *80,000 Hours*. [Online]. 21 March 2025. [Cited : 28 September 2025]. https://80000hours.org/2025/03/when-do-experts-expect-agi-to-arrive/.

VASSIL, Kristjan. 2016. Estonian e-Government Ecosystem. 2016.

VIHMA, Peeter. 2024. The future of warfare is here - DefSecIntel Solutions. *e-Estonia*. [Online]. 18 September 2024. [Cited : 15 January 2026]. https://e-estonia.com/the-future-of-warfare-is-here-defsecintel-solutions/.

WITHERS, Caleb. 2025. Tipping the Scales: Emerging AI Capabilities and the Cyber Offense-Defense Balance. *Center for a New American Security*.

MAJ Maarek KALLAS: Enhancing NATO's Air Power Resilience through Agile Combat Employment (ACE) in the Baltic Sea Region: Operational Strategies and Challenges

Supervisor: LTC Ivar SAMMAL

Statement on the Use of AI Tools:

I confirm that I used AI tools, specifically Grammarly and Microsoft Copilot, solely for textual improvements, grammar corrections and translation purposes. No AI-generated content was used to create original ideas or to alter the substantive meaning of the text.

LIST OF ABBREVIATIONS

ACE – Agile Combat Employment

A2/AD – Anti-Access/Area Denial

AAR – Air-to-Air Refuelling

C2 – Command and Control

NATO – North Atlantic Treaty Organisation

DDA – Deterrence and Defence Concept of the Euro-Atlantic Area

ISR – Intelligence, Surveillance and Reconnaissance

EW – Electronic Warfare

SEAD – Suppression of Enemy Air Defences

DEAD – Destruction of Enemy Air Defences

IAMD – Integrated Air and Missile Defence

HNS – Host Nation Support

USAF – United States Air Force

ADR – Airfield Damage Repair

TTP – Tactics, Techniques, and Procedures

RAF – Royal Air Force

RSOMI – Reception, Staging, Onward Movement and Integration

JAPCC – Joint Air Power Competence Centre

1. INTRODUCTION

1.1 Background and Relevance

The Baltic Sea region has become one of NATO's most strategically sensitive theatres (Surwillo et al, 2025, p.8). The Russian invasion of Ukraine has led to regional changes. The most significant is that Finland and Sweden, which had previously remained neutral, have joined the North Atlantic Treaty Organisation (NATO). This decision has significantly expanded NATO's operational responsibilities and extended the Alliance's border with Russia. At the same time, Russia has also continued to strengthen its military presence in the Baltic Sea region. Deploying weapon systems and electronic warfare capabilities in the Kaliningrad Oblast that create extensive anti-access/area denial (A2/AD) capabilities in Baltic Sea Region (Dalsjö et al., 2021, p.171). Continued airspace violations and incursions by unmanned aerial vehicles into allied territory, as well as hybrid activities by Russia, underscore the vulnerability of the Baltic Sea region. In such a security environment, NATO's deterrence and defence posture should become more dynamic. This requires a change in mindset and the adoption of new concepts.

Euro-Atlantic Deterrence and Defence Concept (DDA) from 2022, clearly emphasizes the need for greater operational flexibility, distributed power projection, and rapid response capabilities across the Alliance (Covington, 2023). The example of the war in Ukraine shows that speed, agility, and dispersed location can be decisive factors in preventing an aggressor from achieving air superiority (Goodwin, 2024, pp 51-57). In summary, NATO's operational thinking is increasingly moving towards more dynamic, dispersed capabilities.

This paradigm shift is most clearly reflected in the Agile Combat Employment (ACE) concept. ACE represents a strategic shift for NATO air forces from traditionally centralized operations to a more flexible, dispersed, and resilient operational concept (Oppelaar, 2023, pp. 52-57). Furthermore, ACE is not only a technical change, but it should also be a broader transformation that increases the Alliance's ability to operate in an unpredictable, rapidly changing, and increasingly hostile threat environment

(Oppelaar, 2023, p. 59). Considering also the limited air force capabilities of the three Baltic states, Finland and Sweden's NATO membership and Russia's A2/AD coverage, the implementation of ACE in the Baltic Sea region is relevant and warrants an analytical approach. Addressing this topic will help highlight regional characteristics and opportunities within the NATO framework.

1.2 Objectives and Structure of the Study

Consequently, this study examines the possibilities and limitations of implementing the ACE concept in the Baltic Sea region and identifies strategic, operational, and institutional challenges to better understand how to organise the ACE concept more effectively. This study emphasises that the effective implementation of ACE in the Baltic Sea region is feasible. However, this requires a shift from fragmented bilateral exercises to a coordinated regional approach that systematically integrates a dispersed operational culture with the host nation’s support capabilities.

The analysis draws on doctrines, regional security studies, and recent exercises, examines the historical development of ACE, the specific characteristics of air forces in the Baltic Sea region, and the threat development, with the aim of assessing how a unified regional framework could transform existing capability gaps into operational strengths.

This study is structured into five parts. The first two parts provide a comprehensive understanding of the nature of the ACE concept and its historical development into a separate US Air Force doctrine. In addition, NATO's adaptation and interpretation of ACE principles are analysed, and the most essential principles of the concept in the context of operational and strategic planning are highlighted and illustrated with examples from previous exercises. The third part focuses on the specific characteristics of the Baltic Sea region, considering the security threats in the area and NATO's existing and potential capabilities. The fourth and fifth parts are analytical. Building on the preceding chapters, they assess the feasibility of ACE implementation in the region and develop concrete recommendations for a unified regional framework.

2. THE EVOLUTION AND ESSENCE OF AGILE COMBAT EMPLOYMENT

2.1 Historical Background

What exactly is ACE in the context of air power? To answer this question, we need to consider it from two perspectives. The first perspective is the US's revival of this concept from a historical perspective. The ACE concept cannot be considered a new idea. This is more of an evolutionary development that has been shaped by the practices of US expeditionary forces in various military conflicts (Davis, 2021, pp. 1-10). Those conflicts have highlighted the importance of dispersed bases and mobile logistics systems in maintaining survivability (Davis, 2021, pp. 1-2). In addition, political and geographical constraints have created a constant need for the US to have a flexible network of bases (Nicastro, 2024, pp. 1-2).

In the post-Cold War period, the US significantly reduced the number of its global air bases, which reduced its worldwide dominance and operational capabilities (US AF Doctrine Note 1-21, 2022). Due to the changed geostrategic situation, the growing dominance of Russia and China in certain regions, the development of weapon systems, and budgetary and political constraints, the ACE concept is seen as one possible measure for adapting to the changing situation described in the previous part (Nicastro, 2024, p. 1). In other words, ACE is part of a broader US Air Force strategy aimed at maintaining competitive advantage over major powers, particularly China and Russia.

2.2 Core Principles and Definition

According to US Air Force doctrine, ACE is defined as a ‘proactive and reactive operational scheme of manoeuvre executed within threat timelines to increase survivability while generating combat power’ (US AF Doctrine Note 1-21, 2022). Doctrinally, the central idea of the concept is the distribution of units and capabilities between separate locations according to the situation, with minimal time expenditure and logistical footprint. This makes it more difficult for the enemy to plan actions against it, allowing for greater survivability, operational flexibility, and operational sustainability (US AF Doctrine Note 1-21, 2022). ACE is divided into five types of activities based on its characteristics. The first of these is Setting the Theatre. This includes the pre-

placement of equipment and troops, access, and negotiations with allies. Another essential feature is the dispersal of forces before the enemy acts, known as the Proactive ACE Manoeuvre. This, in turn, necessitates a robust Command and Control structure. Thirdly, the response to the opponent's actions is discussed, focusing on dispersion and flexibility to operate from separate locations and to move to different places during the operation. Fourth, a coordinated attack by dispersed forces, which can rely on robust C2 and force protection before operational activity. The last important element is support and sustain between dispersed locations, as well as fast recovery capability. (US AF Doctrine Note 1-21, 2022).

In summary, the ACE concept in the US is treated doctrinally within a strategic framework, emphasising its global applicability and role in the context of competition between major powers (Nicastro, 2024, p. 1).

NATO's approach is operational, focusing on practical principles that enable the concept to be translated into concrete actions through coordinated operations among allied countries. This difference in approach to ACE reflects the US's strategic ambition and NATO's need to adapt the concept to the operational realities of a multinational environment. This involves increasing operational flexibility and resilience, reducing dependence on large air bases, which are highly vulnerable to attack, and thus directly related to maintaining combat readiness. In the context of combat readiness, the rapid redeployment of units and the conduct of dispersed operations are no less critical. (Oppelaar, 2023, pp. 54-59).

It creates the conditions for operating in multiple locations simultaneously and, in the context of deterrence, demonstrates the interoperability of the allies. The successful implementation of the ACE concept is based on changes in logistics, command and control, and training to support the independent and flexible operation of smaller units. At its core, ACE is built upon three fundamental principles. Establishing a distributed network of bases, employing modular force structures, and executing autonomous operations (Oppelaar, 2023, pp. 56-59; US AF Doctrine Note 1-21, 2022). Collectively, these principles enable allied forces to operate in a dispersed manner, mitigate logistical vulnerabilities, and preserve air superiority under crisis conditions.

Implementing ACE, however, requires comprehensive doctrinal, logistical, and cultural adaptation across the alliance (Oppelaar, 2023, pp. 56-59).

The success of ACE depends on several other factors as well, like infrastructure readiness, logistical flexibility, resilient communication capabilities, interoperability among allies, and multi-capable airman capabilities. Interoperability is particularly vital in a multinational environment, where harmonisation of standards and cross-servicing are essential to ensure operational flexibility. By integrating these principles into regional defence planning, NATO strengthens its ability to deter aggression and maintain strategic stability in an increasingly contested security environment (Chadwick, 2024). However, without adequate resource allocation and sustained investment, ACE risks remaining a declarative concept rather than evolving into a tangible operational capability (Taylor et al., 2024).

2.3 US and NATO ACE Approaches Comparison

The US and NATO approaches to the ACE concept differ in some respects but share several similarities. The US places greater emphasis on flexibility and rapid response (US AF Doctrine Note 1-21, 2022). For NATO, cooperation, standard procedures, and the fact that all member states operate within a common framework are more important. To better understand, a comparison of the differences is presented in Table -1. It focuses on five key attributes including origin and doctrinal status, scope and framing, command and control (C2), logistics and sustainment, protection and integration with joint functions. These attributes were selected because they capture the essential dimensions of ACE implementation and enable a systematic analysis of how the US and NATO address similar operational challenges within different organisational frameworks and priorities.

Table 1: Comparison of the operational impact of the US and NATO ACE concepts

Attribute	US ACE doctrine	NATO approach	Operational impact
Origin and doctrinal status	Service-level, formalized in USAF doctrine (AFDN 1-21) as an operational concept for the US Air Force	Alliance-level adaptation. ACE principles adopted across NATO and implemented through national contributions and NATO guidance rather than a single service doctrine	US doctrine gives clear authorities and processes. NATO relies on harmonising many national doctrines
Scope and framing	Emphasises five core elements (posture; C2; movement; protection; sustainment) linked to Joint All-Domain Operations	Emphasises interoperability, Host Nation Support (HNS), multinational exercises and regional practices tailored to member capabilities	US framing drives service investments and specific TTPs. NATO framing prioritises interoperability, sovereign constraints and collective burden-sharing
Command and control (C2)	Focus on decentralised, resilient C2 within USAF constructs and delegated authorities to enable rapid manoeuvre under threat timelines	Focus on multinational C2 harmonisation, NATO command relationships and political control. Requires coordination across national chains	US can authorise rapid delegated action within service. NATO must reconcile national authorities, which can slow decision cycles in some scenarios
Logistics and sustainment	Emphasises expeditionary logistics, pre-positioning, service-led sustainment solutions	Emphasises HNS, multinational coordination, reliance on national stocks and host-nation arrangements	US invests in organic expeditionary sustainment. NATO approach depends on member willingness to pre-position and on harmonised RSOMI/HNS procedures
Protection and integration with joint functions	ACE explicitly integrates protection counter-UAS, and considerations as core elements	NATO integrates ACE principles into collective defence planning but must balance member air/missile defence architectures and regional A2/AD threats	US doctrine drives specific protection investments. NATO must coordinate diverse national IAMD/SEAD capabilities and doctrine to protect dispersed sites

Source: Compiled by the author based on the sources used

To bring out the most important, the US ACE doctrine has been formally articulated at the Air Force level, enabling rapid decision-making and clear processes. In NATO, ACE principles are adopted at the alliance level and implemented through member-state contributions and NATO directives, which means that standardisation takes longer but increases political legitimacy. The US doctrine emphasises the creation of a distributed base network and invests in organic logistics solutions, while NATO relies more on host-nation support and cooperation among member states. In terms of command, the US doctrine allows for rapid delegation and flexible command. At the same time, NATO must consider the decision-making processes of different countries, which can slow down response times but strengthen collective cohesion. In summary the strengths of the US approach are flexibility and innovation, while those of NATO are broad-based cooperation and standardisation.

2.4 ACE in Practice

Allied air force exercises in the Baltic Sea region over recent years have clearly demonstrated that the implementation of the ACE concept has become a practical reality. Table -2 highlights practical examples of implementing the ACE concept in the Baltic Sea region. It clearly confirms the key arguments presented in previous subchapter.

The success of the ACE concept depends primarily on next factors. First, the creation of a dispersed base network that allows air forces to operate flexibly and reduces dependence on fixed infrastructure (Chadwick, 2024). Second, the use of modular force structures that support rapid redeployment and interoperability between allies (Taylor et al., 2024; Oppelaar, 2023). And thirdly, the capability for autonomous operations, which allows units to operate independently in different conditions and, if necessary, restore operational capability even in situations with limited resources (Oppelaar, 2023).

Table 2: Implementation of the ACE concept in Baltic Sea region over recent years

Year	Location	Description	Sources (Appendix – 1)
2025	Finland / Sweden	Finland–Sweden: aircraft cross-servicing exercise and interoperability testing	NATO Allied Air Command; Finnish Air Force
2025	Estonia	Estonia–Netherlands, F-35 detachment and cross-servicing and combat readiness	Estonian Ministry of Defence; NATO Allied Air Command
2024	Lithuania	Lithuania–Sweden–France: Distributed deployments and HNS testing	NATO Allied Air Command
2025	Finland	Baana ex series highway landings	Finnish Air Force
2024	Finland	Dispersed-base operations exercise (resilient C2 and dispersion drills)	Finnish Army; Yle
2024	Estonia	Estonia–USA runway repair / expeditionary airfield damage repair exercise	Aviano Air Base (USAF); NATO Allied Air Command
2025	Estonia	Estonia–UK hot-pit refuelling training and exercise	Forces News (RAF hot-pit coverage)
2025	Estonia	Estonia–Canada highway landing exercise	ERR News; Forces.net
2025	Finland	ACS technician training (aircraft cross-servicing course)	Finnish Air Force

Source: Created by the author based on a variety of public sources

The exercises and cooperation projects listed in the table also illustrate how these principles have been applied in different countries and situations and adapted to local conditions. The creation of a dispersed base network has become a reality thanks to regular exercises in which aircraft land and operate on temporary landing strips or roads. This reduces dependence on large, stationary bases and increases unit survivability. Such dispersion is at the core of the ACE concept and enables rapid response and flexibility.

The cross-servicing of aircraft, hot-pit refuelling, and airfield restoration (ADR) highlighted in the table demonstrate how a modular force structure and cooperation between allies enable rapid redeployment and the continuation of operations even under conditions of limited resources. ADR exercises, such as the runway repair or expeditionary airfield damage repair exercise conducted in Estonia, are crucial because they enable the restoration of operational capability even after an enemy

attack or infrastructure damage. This reinforces the chapter's argument that successful implementation of ACE depends on interoperability among allies, standardised procedures, and continuous training.

Autonomous operational capabilities are supported by exercises in which units operate independently across different countries and under varied conditions, using local resources and relying on allies. We can also conclude that the successful implementation of ACE requires not only technological and logistical changes but also a change in mindset, with flexibility and adaptability key to this concept.

3. SECURITY ENVIRONMENT AND AIR POWER IN THE BALTIC SEA REGION

3.1 Capability Gaps in NATO’s European Air Forces

NATO air forces can be characterised by their unique technological capabilities worldwide (Burcznska, 2018, p. 85). Extensive multinational exercises and operations demonstrate impressive interoperability, but also reveal persistent shortcomings that, if underestimated, could result in failing to realise the full potential of the air domain in a military context. Focusing on Europe's current air capabilities, it is essential to note that the ability to conduct air operations requires not only the existence of various aircraft platforms but also other complementary capabilities (Wall et al., 2023, pp. 1-2). This means that, in order to project air power at a specific time to a specific place, enablers are needed in addition to weapon platforms. For example, in order to carry out widespread and high-intensity air operations, AAR, ISR, EW capabilities, and a functioning C2 system are essential (Binnendijak et al., 2020, pp. 17,87). If these capabilities are lacking or fragmented in a regional context, this has a direct impact on operational planning and the simultaneous execution of operations (Wall et al., 2023, p. 1; Binnendijak et al., 2020, p. 17).

Currently, Europe is undergoing modernisation of its air domain capabilities, characterised by the gradual introduction of fifth-generation platforms. However, modernising platforms alone will not solve today's operational bottlenecks (Binnendijak et al., 2020, pp. 5-7). Without the development of airborne ISR, EW, and C2 capabilities, the potential of these platforms in Europe may remain unrealised. Furthermore, in an operational context, the tactical advantage of fifth-generation

aircraft may not translate into a broader impact end goal (Bronk, 2022, p. 2; Binnendijak et al., 2020, p. 7). This clearly highlights one of the bottlenecks in European air capabilities. Focusing on enablers, we see that Europe lags behind the US in this area, with European countries collectively possessing approximately only one-third of the NATO Airborne C2 or AAR capabilities (Wall et al., 2023, pp. 1-3).

Another critical factor in the case of European air forces is the low concentration of operational bases in the region, and their reinforcement has been neglected (Bronk, 2023, pp. 5-9). The vulnerability of bases, the number of aircraft parking spaces, and logistical concentration are critical factors that limit operational resilience. Densely concentrated infrastructure makes air forces vulnerable and reduces their ability to maintain operational tempo and minimise counter-effects (Taylor et al., 2024).

The operational sustainability of European air forces is also limited by insufficient SEAD capabilities, ammunition shortages, and the fragmentation of integrated air and missile defence (IAMD) systems (Bronk, 2023, pp. 29-35). The production capacity and stockpile size of European countries have so far been insufficient to support long-term, intensive air operations, which has increased dependence on imports and created a risk of rapid stock depletion in a conflict situation (Bergmann et al., 2025 pp. 27-28). In addition, based on the NATO IAMD development perspective (NATO, 2025), we can conclude that coverage in Europe is uneven and fragmented across countries, which reduces collective defence capabilities and creates gaps in coordinated air defence and missile defence operations (Muravska, 2023, p. 11). It is also important to focus on aspects related to political, institutional, and geographical characteristics. This means that the interests and objectives of union members may differ (Sperling et al., 2018 pp. 888-914). Small countries often lack complex capabilities and frequently depend on integration and contributions from other countries (Burcznska, 2018, pp. 85-104; Gioe et al., 2024, pp. 145-153). Furthermore, the geographical aspect cannot be considered less important.

3.2 Characteristics and Limitations of Baltic States' Air Forces

The Baltic Sea region is NATO's eastern axis and one of the main focuses of its critical deterrence strategy since Russia's full-scale aggression against Ukraine (Covington,

2023). Russia's A2/AD capabilities in Kaliningrad create a situation where the Baltic Sea region is geographically vulnerable (Dalsjö et al., 2021, pp. 169-174). It has become increasingly difficult for NATO in terms of both operational continuity and adaptation, given the specific characteristics of the air forces of the countries in the region.

The Baltic states' limited defence capabilities and small armed forces make them dependent on NATO's collective defence. From a capability perspective, one of the most significant gaps is the lack of air defence, which makes the Baltic states entirely dependent on NATO in today's security environment (Hurt et al., 2023, pp. 1-16). In addition, the Baltic states lack weapon platforms, which are crucial for air defence and achieving air effects (Harper et al., 2018, pp. 1-28). Furthermore, due to the size of these countries, their military infrastructure is limited (Saab, 2024). At the same time, based on open sources, it is clear that the Baltic states have focused on the rapid reception and hosting of allies, training their personnel in cross-servicing aircraft and refuelling, and are practising operating with allies from austere landing strips and an operational network integrated with NATO.

3.3 The Impact of Finland and Sweden’s NATO Accession

The accession of Finland and Sweden to NATO has significantly reduced the region's vulnerability, bringing substantial military resources and strategic advantages (Lawrence et al., 2025, p. 5). When discussing Finland's current air force and prospects from an ACE perspective, we can argue that the principles discussed in the previous chapter have been a fundamental pillar of the air force.

Various sources provide a reasonably comprehensive overview of these principles. Finland can be considered a pioneer in the use of dispersed bases and temporary landing strips, and in the implementation of this concept (Keränen, 2024, pp. 6-12). Thus, for them, ACE is not an abstract doctrine but an everyday practice, as demonstrated by the different series of exercises and drills as well as the heightened interest of allies in participating in them. In operational terms, this could have a significant impact on their integrated air defence system through the combination of SEAD/DEAD and ACE principles. (Keränen, 2024; Bronk, 2023, pp. 12-13)

Theoretically, it can be concluded that Finland is setting a precedent with its approach. Combining the operational activities of the fifth-generation platform with the ACE principles may offer a solution to several operational challenges that NATO is currently facing. Examples include dependence on technology provider nations, survivability, operational sustainability, and vulnerability of critical capabilities (JAPCC, 2022).

In addition, the limited air refuelling capability, currently one of the most significant operational capability gaps for European air forces, can be eliminated through support for their operational design (Wall et al., 2023). In summary, this is what makes the Finnish Air Force unique in the region. Their dispersed infrastructure, systematic training, and operational design, which focus on short-range, rapid aircraft servicing at various temporary locations during operations, make them less dependent and ensure operational flexibility (Keränen, 2024, pp. 8-11).

Sweden’s approach may seem similar to Finland's. Specifically, Sweden has been developing and implementing the principles derived from the ACE concept since the Cold War era (Friis et al., 2024, pp. 813-824). However, what makes Sweden unique compared to Finland is the existence of a national aircraft platform developed with a focus on dispersion, operational flexibility, and rapid readiness (Wikman, 2024, pp. 9-11; White Book, 2021, pp. 5-6). In other words, their aircraft, weapons, and crews can move between bases in Sweden under operational pressure, disperse, and continue to operate according to standardised procedures, which ensures their legal certainty and operational sustainability (Wikman, 2024). Additionally, the operation of these platforms is not directly impacted by air refuelling capabilities or donor country support. Thus, operationally, their approach is quite similar to that of Finland, or vice versa.

4. ASSESSING ACE IMPLEMENTATION IN THE BALTIC SEA REGION

4.1 The impact of Russia's A2/AD capabilities on the Baltic Sea region

Based on the discussions in the previous chapter, we can conclude that NATO air forces in Europe possess cutting-edge technological capabilities. In addition, various operations and international exercises have demonstrated their strong interoperability. However, we can conclude that there are also persistent shortcomings that, in one way

or another, undermine credible deterrence and the air forces' readiness to address specific factors that hinder operational activities.

One such vulnerability is Russian A2/AD capabilities in the Baltic Sea region, whose impact on the tempo of operations should not be underestimated, and whose suppression at critical moments may prove challenging in an operational context, limiting freedom of manoeuvre. At the same time, various starting points emphasise exploiting rapid operational windows to minimise the effects of hostile A2/AD. This, in turn, can only be based on rapid operational readiness and sustainability.

Considering everything described above, a dilemma is emerging. On the one hand, NATO's European air forces are focused on technological superiority and fifth-generation capabilities. On the other hand, there is a lack of enablers, and small countries are unable to develop a full range of capabilities in the air domain.

Focusing specifically on the unique characteristics of NATO air forces at the Baltic Sea region it is possible to fill the gap between the two extremes. The question is how to transform weaknesses into strengths and thereby create operational effects. In other words, is it possible to turn the limited number of bases in the region, the lack of tanker aircraft, and the overall lack of mass into strengths?

The operational activities of bases in Estonia, Latvia, and Lithuania have demonstrated that short rotation cycles, modular logistics, and rapid reception and service capabilities enable allies to quickly deploy various power packages, regardless of nationality, if necessary. The concept of dispersed bases in Finland and Sweden, austere landing-stripe operations, and modernised platforms ensures reliability, rapid deployment, and sustainable operations.

However, limited air refuelling capabilities, fragmented air defence, and the ability to suppress enemy air defence are existential problems. At the same time, by implementing a distributed, modular approach and keeping sorties short, it is possible to achieve the same operational effect at theoretically lower resource costs. This means fewer tanker hours, less risky flight profiles, and greater flexibility. They should not always rely on more equipment, but on different operational thinking and more

effective management, which reduces vulnerability and maintains operational tempo even under conditions of limited resources.

4.2 Regional Strengths and Weaknesses in ACE Implementation

The air forces in the Baltic Sea region can be considered a testing ground for the ACE concept, where its specific activities and capabilities are being tested. In the Baltic states, ACE-type practices are often associated with NATO rotations and the enhancement of local air force units' capabilities. Estonia, Latvia, and Lithuania are characterised by growing readiness to implement host-nation support (HNS) mechanisms. At the same time, the practice is often rotation-based and depends on specific exercises or the country of the allies.

In recent years, Finland and Sweden have demonstrated capabilities that align with ACE principles. Hot-pit refuelling reduces dependence from AAR capabilities. Aircraft cross-servicing enables different nations to provide a range of services to allied platforms, reducing logistical dependence on home bases and from national support elements. Using austere landing strips in the Baltic and Nordic countries has demonstrated dispersal capability, complicating the enemy's planning cycle and making targeting more difficult. Regular dispersed deployments will test pre-positioning of equipment and HNS procedures.

4.3 Challenges of Regional Cooperation

Despite the above examples, this also comes with one of the main regional bottlenecks. When we analyse the various exercises conducted in the region in recent years, we see an interesting pattern. Namely, cooperation between the countries discussed above is minimal. For example, Estonia has conducted its latest exercises in cooperation with Canada, Belgium, and the UK. Lithuania has cooperated with France and Sweden, while the Nordic countries have focused on each other and other European countries. As a tentative conclusion, this points to a lack of a harmonised regional approach.

The states of the Baltic Sea region clearly demonstrate that, by implementing the principles of the ACE concept, previously significant weaknesses in an operational context may no longer be as important. Furthermore, the implementation of ACE-related activities and thinking by Finland and Sweden has proven that it increases operational flexibility and survivability. Regular capability deployments, such as those in Estonia and Lithuania, strengthen trust between allies. Interoperability with many different countries serves as a psychological deterrent, especially in today's security environment. At the same time, regional fragmentation should not be viewed as a technical problem or a growing difficulty. It should be viewed as a significant bottleneck, given the regional specificities of NATO's capability shortfalls. If the implementation of ACE remains fragmented in the regional context, it may lose some of its deterrent value.

5. TOWARDS A UNIFIED REGIONAL ACE FRAMEWORK

The analysis presented in this study shows that ACE-related activities in the Baltic Sea region are growing but remain structurally fragmented. The preceding chapters identified three interrelated problems: limited regional capabilities in key supporting areas, the lack of a common framework among the five countries bordering the Baltic Sea, and exercises conducted bilaterally rather than based on a unified regional logic. The following recommendations address all three problems in order and build on existing strengths in the region.

The first and most critical recommendation is dedicated to the creation of a Baltic Sea ACE sub-working group under the command of NATO Allied Air Command. An analysis of the region’s current exercise patterns reveals an interesting pattern. Specifically, Estonia, Latvia, Lithuania, Finland, and Sweden all conduct ACE-related activities, but do so on separate tracks and with rotating partners. A permanent working group would change this. It would bring together the air component planners and HNS coordinators of all five countries on a common platform, harmonize ACE-related tactics, techniques, and procedures across the entire region, and coordinate an annual exercise cycle that systematically rotates through the countries. In other words, it would transform the progress of individual countries into a shared regional warning posture.

Without such a mechanism, what has been achieved so far will not translate into a reliable collective capability.

The second recommendation concerns Finland and Sweden specifically. As discussed in Chapter 3.3, both countries have developed a dispersion-based operational culture prior to the formal articulation of ACE in U.S. Air Force doctrine. This experience is not yet being fully utilized at the alliance level. Therefore, it is recommended to institutionalize Finnish and Swedish dispersion expertise as a knowledge package to be transferred through the NATO, making it available to all allied partners. Specifically, this means expanding existing Finnish-Swedish cross-service exercises to include full participation by the Baltic states and conducting dedicated joint exercises involving all five countries to test the regional concept from the chain of command down to logistics and dispersion. For them, dispersed operations are not an abstract doctrine, but daily practice. This makes them natural sources of expertise for the region as a whole.

Third, the region needs targeted capability investments that do not depend on large-scale procurement. Three areas stand out as priorities. The harmonization of cross-service standards should be accelerated so that every allied aircraft can be serviced at any regional temporary landing site, regardless of national affiliation. Robust, multinational C2 systems must be developed to enable the command and control of dispersed units under warfare pressure. And the Baltic states' current focus on austere runway operations and airfield restoration capabilities should be set as one of the priority capability development. These investments build on what already exists. They combine national strengths rather than starting from scratch.

It can be concluded that implementing the ACE concept in the Baltic Sea region is feasible. However, this requires a substantive shift from fragmented bilateral cooperation toward a coordinated regional approach. The region has the foundations in place. What is missing is a framework to bring them together.

CONCLUSION

Russia's A2/AD capabilities in Kaliningrad, combined with the limited air power resources of the Baltic Sea region, make the implementation of the ACE concept both

urgent and strategically relevant. The ACE concept focuses on dispersing air forces and capabilities to different locations to reduce dependence on enablers such as AAR and fixed infrastructure, and to make it more difficult for the enemy to plan its actions. This enhances survivability, operational flexibility, and sustainability, without requiring the mass that small nations cannot generate.

The Baltic Sea region has made real progress, focused on the rapid reception of allies, host-nation support, and operating from austere strips. However, they lack independent air defence platforms and remain entirely dependent on collective NATO deterrence. Finland and Sweden's accession has changed the region's strategic calculus, both bring decades of dispersal-based operational experience, and in Sweden's case, a nationally developed platform designed from the outset for rapid redeployment under operational pressure.

The main finding of this work is that regional cooperation remains fragmented. The Baltic Sea region countries conduct exercises with different allies, but there is no unified regional approach. This reduces the deterrent value and operational effectiveness of the ACE concept. Platform modernisation is underway but upgrades alone will not solve this. What the region needs is a framework that connects existing national strengths into a coherent collective capability and the foundation for that framework already exists.

ACE is not a silver bullet. It does not eliminate capability gaps, nor does it replace the mass and enablers the region lacks. However, in today's security environment it is the most accessible and practically achievable option available. No new platforms, no large budgets, no fundamental restructuring of forces required. When air power is dispersed, continuously moving, and operating from unpredictable locations, an adversary faces a targeting problem that is difficult to solve. That enables ensuring survivability, rapid combat readiness, operational sustainability, and reduced dependence on enablers in a resource-constrained environment.

Bibliography

Bergmann, Max and Svendsen, Otto. 2025. How Europe Can Defend Itself with Less America. *A Report of the CSIS Europe, Russia, and Eurasia Program.* October 2025, pp. 1-36.

Binnendijak, Anika, et al. 2020. At the Vanguard: European Contributions to NATO's Future Combat Airpower. 22 October 2020.

Bronk, Justin. 2023. Regenerating Warfighting Credibility for European NATO Air Forces. *Whitehall Reports.* Defence and Security Studies, 22 February 2023, pp. 1-39.

Burcznska, Maria E. 2018. Multinational cooperation: building capabilities in small air forces. *European Security.* 2018, Vol. 28, 1, pp. 85-104.

Chadwick, Luca. 2024. The 'ACE' up their sleeves: Understanding NATO Agile Combat Employment. 26 January 2024.

Covington, Stephen R. 2023. NATO's Concept for Deterrence and Defence of the Euro-Atlantic Area (DDA). 2023.

Dalsjö, Robert and Jonsson, Michael. 2021. More than Decorative, Less than Decisive: Russian A2/AD Capabilities and NATO. *Global Politics and Strategy.* 28 September 2021, Vol. 63, 5, pp. 169-190.

Davis, Justin R. 2021. The Air Force's True Expeditionary Roots: Historical Context and Lessons for the Agile Combat Employment (ACE) Concept. Kansas : US Army Command and General Staff College and JAPCC, 2021. pp. 2-62.

Friis, Karsten and Tamnes, Rolf. 2024. The defence of northern Europe: new opportunities, significant challenges. *International Affairs.* 4 March 2024, Vol. 100, 2, pp. 813-824.

Gioe, David, V, Miron, Marina and Ozawa, Mark. 2024. Reassessing NATO's deterrence and defence posture in the Baltics: rebalancing strategic priorities to counter Russian hybrid aggression. *Defense & Security Analysis.* 14 November 2024, Vol. 41, pp. 145-165.

Goodwin, Joe. 2024. *Allied Air Command Lessons from Ukraine.* 37. s.l. : Joint Air Power Competence Centre, 2024. pp. 50-58.

Harper, Christopher, Lawrence, Tony and Sakkov, Sven. 2018. *Air Defence of the Baltic States.* Tallinn : ICDS, 2018.

Hurt, Martin, et al. 2023. *Baltic Defence Development: Adding Value to the Defence of the Baltic Sea Region.* s.l. : International Centre for Defence and Security (ICDS), 2023.

Keränen, Juha Pekka. 2024. The Finnish Air Force. Ensuring Readiness and Leveraging High-End Air Capabilities while Integrating with NATO. 37, 2024, pp. 6-14.

Lawrence, Tony, et al. 2025. Hybrid and High-End Warfare in the Baltic Sea Region. *International Centre for Defence and Security.* 2025.

Muravska, Julia. 2023. European Integrated Air and Missile Defence in NATO: Progress and Persistent Challenges. *Freeman Air and Space Institute*. Paper 16 (2023).

NATO. 2025. NATO Integrated Air and Missile Defence. *Deterrence and defence.* 2025.

Nicastro, Luke A. 2024. *Defense Primer: Agile Combat Employment (ACE) Concept.* USA gov. s.l. : Congressional Research Service, 2024. IF12694.

Oppelaar, Isaiah. 2023. Agile Combat Employment: The Next Big Thing for NATO Air Power. *The Journal of the JAPCC*. 36, 2023, pp. 54-59.

Saab. 2024. Gateway to Europe: why Estonia and Latvia's military capabilities strengthen the entire continent. s.l. : Saab AB, 2024.

Sperling, James and Webber, Mark. 2018. NATO Operations. in [book auth.] **Hugo Meijer and Marco Wyss.** *The Handbook of European Defence Policies and Armed Forces.* Oxford : Oxford Academics, 2018, pp. 888-914.

Surwillo, Izabela and Slakaityte, Veronika. 2025. Northern Horizon: Strengthening Security in the Baltic Sea Region. *DIIS Report.* 2025, Vol. 2025, 5.

Taylor, Zane Jarrett and Long, William Dean. 2024. Maneuvering in Contested Skies: Factors Impacting Air Operations in the European Theater*. Over the Horizon Journal.* 6 October 2024.

US AF Doctrine Note 1-21. 2022. Air Force Doctrine Note 1-21. [book auth.] US Air Force. *Agile Combat Employment.* 2022.

Wall, Collin and Christianson, John. 2023. *Europe's Missing Piece: The Case for Air Domain Enablers.* s.l. : Center for Strategic and International Studies, 2023.

***White Book*. Government of Sweden. 2021.** The Swedish Defence Commission secretariat, 2021, The Swedish Defence Commission's white book on Sweden's Security Policy and the Development of the Military Defence 2021-2025, pp. 2-10.

Wikman, Jonas. 2024. Sweden Strengthens NATO's Presence in Europe. *The Swedish Air Force Commander's View on Joining NATO.* 38, 2024, pp. 6-12.

APPENDIX – 1: Secondary Sources

NATO Allied Air Command. 2025. Estonian and Dutch Collaborate During Agile Combat Employment Training at Ämari. *NATO Allied Air Command.* [online] https://ac.nato.int/archive/2025-2/estonian-and-dutch-collaborate-during-agile-combat-employment-training-at-aamari--estonia. [Accessed: December 2025].

Forces News. 2025. 140 Expeditionary Air Wing Ground Crew Lead Hot-Pit Refuelling Training with NATO Allies. *Forces News.* [online] https://www.forcesnews.com/services/raf/140-expeditionary-air-wing-ground-crew-lead-hotpit-refuelling-training-nato-allies. [Accessed: December 2025].

ERR News. 2025. Canadian Air Force Pilots Practice Debut Road Landings in Estonia. *ERR News.* [online] https://news.err.ee/1609828836/canadian-air-force-pilots-practice-debut-road-landings-in-estonia. [Accessed: December 2025].

Forces.net. 2025. Highway Readiness: Canadian Fighter Jets Touch Down on Public Road in Estonia. *Forces Net.* [online] https://www.forces.net/nato/highway-readiness-canadian-fighter-jets-touch-down-public-road-estonia. [Accessed: December 2025].

NATO Allied Air Command. 2024. French Air and Space Force ACE Exercise to Sweden. *NATO Allied Air Command.* [online] https://ac.nato.int/archive/2024/FRA_ACE_to_SWE. [Accessed: December 2025].

Finnish Air Force (Ilmavoimat). 2025. Finnish Air Force to Participate in Basfunktionsövning 25 in Sweden. Finnish Air Force (Ilmavoimat). [online] https://ilmavoimat.fi/en/-/finnish-air-force-to-participate-in-basfunktionsovning-25-in-sweden. [Accessed: December 2025].

United States Air Forces in Europe (USAFE). 2025. US Air Force F-35 Lightning II Makes Historic First on Highway in Finland. United States Air Forces in Europe (USAFE). [online] https://www.usafe.af.mil/News/Article-Display/Article/3894497/us-air-force-f-35-lightning-ii-makes-historic-first-on-highway-in-finland/. [Accessed: December 2025].

Aerotime Hub. 2025. Finnish Air Force Baana 25 Highway Exercise. *Aerotime.* [online] https://www.aerotime.aero/articles/finnish-air-force-baana-25-highway-exercise. [Accessed: December 2025].

Finnish Army (Maavoimat). 2024. Baana 24 Road Base Exercise in Rovaniemi and Ranua. *Maavoimat.* [online] https://maavoimat.fi/en/-/1951206/baana-24-road-base-exercise-in-rovaniemi-and-ranua. [Accessed: December 2025].

Yle. 2024. Baana 24: Dispersed Base Operations Exercise. *YLE.* [online] https://yle.fi/a/74-20076390 [Accessed: December 2025].

Aviano Air Base (USAF). 2024. Estonia EADR: Expeditionary Airfield Damage Repair Exercise. [online] https://www.aviano.af.mil/News/Display/Article/3892090/estonia-eadr/ [Accessed: December 2025].

Finnish Air Force (Ilmavoimat). 2025. Allied Mechanics on a Hornet Course at the Air Force Academy. [online] https://ilmavoimat.fi/en/-/allied-mechanics-on-a-hornet-course-at-the-air-force-academy. [Accessed: December 2025].

MAJ Raido KUKK: Partners in Tension: Interaction of EU Economic Power and U.S. Hard Power in Transatlantic Security

Supervisor: Mr Louis WIERENGA

Statement on the Use of AI Tools:

This research paper was drafted independently, with all reasoning, arguments, and examples originating entirely with the author except where otherwise indicated, using appropriate references. No AI tools were used to produce substantive content. Large Language Models — including Claude, Gemini, and ChatGPT — were used at the revision stage to rephrase and condense existing sentences for concision, reducing word count while preserving the author's intended meaning. These same tools were additionally used to conduct structured analytical reviews of draft versions, covering aspects such as structural compliance, logical flow, argument coherence, thesis–evidence alignment, and internal consistency — serving as a critical sounding board rather than a content contributor. Grammarly was used as a final step in accordance with Baltic Defence College style recommendations to remove redundancies, correct punctuation errors, and enhance clarity of expression.

Introduction

I. The Transatlantic Power Evolution

Si vis pacem, para bellum - if you want peace, prepare for war. This maxim has long defined strategic thinking, yet Europe chose a different path. Out of the devastation of two world wars, the European Economic Community emerged with one central purpose: to achieve peace through economic integration and control of strategic resources. This vision became Europe's grand design. Across the Atlantic, however, the United States held fast to the logic of hard power, prioritizing military primacy and global force projection. This divergence in strategic culture was the ideal stage for Robert Kagan's (2002) influential provocation, in which his Power and Weakness thesis framed European rejection of power politics as postmodern and the United States as modern and willing to exercise power. Kagan's binary was analytically convenient, but it rested on a static conception of power that left little room for economic instruments as genuine tools of strategic coercion. Two decades later, that binary is under strain when envisioned as an economic project; the EU has evolved into a more credible security actor, with the Lisbon Treaty setting the promotion of peace as its primary objective (European Union, 2012). The EU has started to increase its strategic role by weaponizing its market power and regulations (Farrell, Newman, 2019, pp. 65–70).

These posture changes demand a conceptual clarification. Nye’s expanded soft power framework provides a partial corrective to Kagan, but in his own taxonomy, he explicitly classified coercive economic tools as hard power because they rely on punishment rather than attraction (Nye, 2004, p. 8). The EU's chosen instruments of sanctions, export control, and defence financing are in line with Nye's category of hard power. Rather than positioning Europe between soft and hard power, this paper argues that economic instruments constitute a distinct modality of hard power, challenging the assumption that Europe's influence is only civilian or normative compared to America's. This dynamic, analysed using Mearsheimer’s lens, suggests that all actors ultimately will prioritize security and relative power over institutional commitments (Mearsheimer, 2001, p. 29). This framework clarifies why the EU’s economic instruments have

transitioned from purely normative tools into strategic assets designed to ensure institutional survival and autonomy.

This evolution matters beyond the question of institutional development, as the Ukraine war has transformed the EU from a normative actor into a strategic one, deploying sanctions, utilizing defence financing, and coordinating industry at a scale previously unseen. At the same time, the United States is recalibrating its global posture, demanding European allies assume greater responsibility for their own defence and prioritizing the Indo-Pacific. Nevertheless, coercive power has never been exclusively military. Europe's much-cited weakness, in which leverage is exercised through market access, regulatory standards, and financial architecture, begins to look like a different kind of strength. Kagan's framework was not wrong on its own terms, but his binary did not anticipate the way European power would mature.

II. Theoretical and Analytical Framework

The research framework builds on the literature of interdependence and institutionalism (Keohane, Nye, 2011), recognizing that in a globalized security economy, power operates through networks of mutual dependence rather than unidirectional coercion. Within this context, the paper introduces a ‘complement-versus-friction’ framework to analyse how EU economic instruments interact with U.S. hard power. It also engages with recent scholarship on European strategic autonomy (Kilic, 2023; Česnakas, Juozaitis, 2024; Anghel, Damen, 2025), which situates the EU’s economic policies within a broader quest for self-determination in security affairs.

The study focuses on the EU’s institutional mechanisms, primarily the Common Security and Defence Policy (CSDP), the European Defence Fund (EDF), and the European Peace Facility (EPF), as the operational frameworks through which economic security tools are deployed. It omits non-economic aspects such as intelligence, cybersecurity, and nuclear deterrence to maintain thematic coherence. It also excludes Great Britain, as Brexit renders the UK a separate case that falls outside the paper’s scope. Methodologically, the research adopts a qualitative, case-based approach, examining both complementarity and friction through representative case studies from financial, energy, industrial, and technological sectors, to illustrate the

multifaceted nature of economic security in transatlantic relations. This method is suited to the research question because the complement-versus-friction dynamic is better captured through qualitative analysis than through aggregate data or formal modelling. It manifests in the specific decisions, institutional responses, and political choices that case analysis is designed to examine. To evaluate how strategic autonomy operates across these cases, the analysis uses the threefold distinctions proposed by Fiott (2018), which distinguish between different levels of autonomous capability, and applies them in Chapter 3 to assess what the friction cases reveal about the nature and limits of European strategic agency.

III. Research Question and Thesis

This paper investigates how European economic instruments complement or challenge U.S. security policy, and what this interaction reveals about the nature of Europe's strategic autonomy. It argues that these instruments both reinforce U.S. hard power when objectives converge and constrain the extraterritorial reach of U.S. pressure when autonomy is prioritized. This evolving tension, rather than signalling weakness, supports the argument that the EU is evolving into a strategic actor increasingly capable of shaping global outcomes through economic means.

IV. Outline of the Study

Following this introduction, Chapter 1 establishes the historical baseline of Europe's economic-security orientation, from the Gulf War to the Helsinki Headline Goal. Chapter 2 analyses the EU's current economic-security instruments. In contrast, Chapter 3 focuses on the institutionalization of strategic autonomy by applying the Fiott typology to the 'complement-versus-friction' of selected case studies. The conclusion reflects on whether European economic power represents a cooperative extension of the transatlantic order or the foundation of a distinct, autonomous security identity.

Chapter 1: Historical Foundations of Europe's Economic-Security Orientation

I. The Gulf War & Early Institutional Fragmentation

The 1990–1991 Gulf War revealed a clear gap in Europe's strategic capabilities, highlighting how its expanding economic power was not matched by sufficient military strength. This dynamic was described by Mauer (2011, p. 28), who noted that Europe's inability to stabilise its immediate neighbourhood underscored its persistent reliance on the United States for security. The political context preceding the conflict was defined by the success of economic statecraft, in which the final deal to unify Germany did not rely on military force. Instead, the deal was struck in the Kohl-Gorbachev meeting, where the Federal Chancellor was alone representing the 'West', drawing strength mostly from its economic, not military, power (Freedman, Karsh, 1993, p. 3). Efforts led to several initiatives to reform the Western European Union (WEU) into a defence role and to transform NATO involvement into a political one. However, the actual deployment to the Gulf highlighted a massive capability gap: while the US provided the vast majority of the 660,000 coalition forces, European Community countries contributed only 63,000 troops (Nonneman, 2011, p. 207). Emphasizing the Union's lopsided economic weight, Germany provided no troops but made an enormous financial contribution, covering approximately 10 per cent of the total coalition costs. (Nonneman, 2011, p. 207).

In the Gulf War, Europe's cohesive response materialized primarily as economic coercion, underscoring an early pattern of complementing U.S. strategy without acquiring independent hard-power leverage. During the intensifying crisis, European nations supported decisions at the UN and helped establish an economic embargo on Iraq's oil and the freezing of its monetary assets (Freedman, Karsh, 1993, p. 81). However, this unity was strictly economic. The Gulf episode revealed a structural credibility gap: European diplomacy could not translate its economic weight into agenda-setting influence over U.S. hard power choices. While the UK sought to leverage its direct ties with the U.S. to participate in decision-making, 'none of the European powers had any impact on the U.S. strategic agenda in the Gulf' (Nonneman, 2011, p. 208). This period highlighted a recurring theme where European leaders, particularly in London, overestimated their leverage with Washington. For example, the assumption that standing 'shoulder to shoulder' would yield strategic rewards was later

undermined by U.S. officials like Donald Rumsfeld publicly belittling the British military effort (Mauer, 2011, p. 33).

Institutional design relegated Europe to a supporting role, substituting for absent military capability with economic tools. This fragmentation was primarily due to the WEU's lack of a military command system and to the questionable extension of its area of operations. Furthermore, the means were reactive, implemented after the invasion, and thus had only a limited impact, if any, against a conventional military force. These dynamics also led to situations where European decision-making was neglected on the world stage (Freedman, Karsh, 1993, p. 40). Post-Cold War optimism failed to translate into military capabilities. The institutional answer to this lack of hard power would become the necessary focus for the ensuing decade, culminating in the ambitious Helsinki Headline Goal of 1999. Europe's failure to halt ethnic cleansing in Bosnia and later in Kosovo made it impossible to ignore the political cost of military dependence on the U.S. (Michaels, Sus, 2025, p. 59). These crises showed that economic means carried no deterrent value when mass atrocities required rapid military intervention. The Gulf War had exposed the structural problem, but Bosnia and Kosovo generated the political will to act on it. It was this accumulated frustration that drove European leaders toward the formal institutionalization of a credible military capacity.

II. The Hard Power Attempt and the Strategic Pivot

The institutional failures and the evident lack of a coordinated military response during the Gulf Conflict awakened European leaders, creating a political momentum that led directly to the formalization of the European Security and Defence Policy (ESDP) in 1999. This period marked a significant transition as the EU evolved from a ‘nested security community highly dependent on the US to become a more independent actor’ (Mauer, 2011, p. 32). The strategic realization that a deficit in deployable military hard power greatly limited Europe’s enormous economic weight (Freedman, Karsh, 1993) was codified in the 1999 Helsinki European Council conclusions. The central and most ambitious component of this initiative was the Helsinki Headline Goal (HHG), in which the Union committed to develop and maintain a rapid deployable reaction force of 50,000 to 60,000 troops capable of the full range of Petersberg Tasks (European

Council, 1999). This commitment showed the EU's ambition to match its economic power with a credible military capability. By establishing these specific security structures and crisis management instruments, the EU aimed to reinforce its credibility as a global actor (Musu, 2011, p. 132). This institutionalized that political desire into a concrete force goal. HHG's success or failure would be definitively tested just four years later by the EU's first autonomous military deployment, Operation ARTEMIS.

ARTEMIS tested whether Europe could transcend a reliance on economic instruments by demonstrating credible, autonomous hard power—or whether complementarity with U.S. power would remain the structural default. Operation ARTEMIS, deployed in 2003 to Bunia, Democratic Republic of Congo (DRC), served as the critical and ultimate test of the emerging ESDP. The operation provided a definitive measure of the capacity so far developed under the HHG (Duke, 2011; Tomolya, 2015). Marking the first time the European Union led an autonomous military mission outside the NATO-agreed 'Berlin Plus' framework (Tomolya, 2015). The French-led force achieved immediate military and political success by swiftly stabilizing the humanitarian crisis and bridging the security gap between UN missions (Duke, 2011). The mission represented a significant milestone in the EU's decision autonomy to participate in military operations and crisis management (Musu, 2011, p. 132). However, the French-led framework nation concept used to launch the operation effectively circumvented the complex pooling mechanisms envisioned by the HHG, demonstrating the operational failure of the goal itself, despite the military operational victory. At the same time, the mission simultaneously exposed structural division and systemic failures in the EU's military design. Reliance on France as the sole framework nation confirmed persistent capability shortfalls — strategic airlift above all — and a continuing deficit in hard power (Duke, 2011; Müller, Spencer, 2011, p. 113; Tomolya, 2015). Additionally, the mission revealed profound differences in national interests regarding risk appetite and burden-sharing for intervention outside Europe. The lesson was clear: the EU could stabilize short-term crises but lacked the capacity for complex, long-term conflict management — a gap its economic institutions were better positioned to fill, confirming the pivot toward civilian tools as the primary expression of its strategic identity (Justaert, Keukeleire, 2010).

III The Divergence in Strategic Thought

This historical progression from military fragmentation in the Gulf War to civilian-military imbalance in ARTEMIS establishes the institutional logic for the EU's strategic orientation. Whereas the United States consistently reinforced its global posture through instruments of hard power, implemented using its National Security Strategy (NSS) and National Defense Strategy (NDS), which prioritize military primacy and coercive capability. The EU's failure to operationalize a unified deployable capability through the HHG shifted focus back to economic means. The described institutional dynamic sets the later stage for the push toward strategic autonomy, not as a desire to replicate U.S. military power, but as a necessity to weaponize the Union’s core economic and regulatory strengths. This sets the stage for an analysis of how these instruments have been formalized and deployed in the modern era, focusing on the friction between allies and their use of military and economic power. Having shown why Europe’s strategic identity tilted toward economic instruments, Chapter 2 inventories today’s toolkit - sanctions, financial/energy autonomy, and defence-industrial finance - and evaluates where these complement U.S. power and where they generate friction.

Chapter 2: The Modern Arsenal of European Economic Security

I. The Institutional Shift: From Market Power to Strategic Actor

European security is often defined by a series of *wake-up calls* that were heard but seldom acted upon. Despite internal divisions during the 2003 Iraq war and the subsequent development of the Common Security and Defence Policy (CSDP) to address coherence, the EU aspired to remain a ‘normative actor’ whose security role was viewed as strictly complementary to NATO's. Despite recognizing threats, many member states failed to meet defence spending targets before the war in Ukraine. This confirmed that the EU lacked the mechanism to translate its economic weight into usable security assets (Lațici, Krause, 2021).

The 2022 *Strategic Compass* marks a definitive pivot, transforming the EU into a proactive ‘Security Provider’ (EEAS, 2022, p. 6). Unlike the 2003 Security Strategy or the 2016 Global Strategy, this framework introduces ‘measurable means and actions

with a deadline' to ensure implementation (EEAS, 2022, p. 7). High Representative Josep Borrell notes that the invasion of Ukraine forced the Union to finally 'unite and use the full range of EU policies and levers as instruments of power' (EEAS, 2022, p. 4). By prioritizing 'technological sovereignty' and joint procurement to reduce strategic dependencies, the EU has matured beyond the 'capability gap' of the 1990s, and the transition and weaponization of its regulatory and industrial core should be understood as the primary expression of the EU's strategic identity.

II. Sanctions and Coercive Diplomacy

The Russian invasion of Ukraine was the catalyst described by Timofeev and Chupriyanova (2024, p. 15) as a 'major transformation' in EU sanctions policy and elevating them to the central pillar of European power. Previously characterized by incrementalism, the EU's economic response evolved into a comprehensive system aimed at decoupling the Russian economy from global value chains. Pertiwi (2024, p. 42) argues that European measures serve to close loopholes that U.S. sanctions alone cannot reach, reinforcing U.S.-led strategic objectives through the structural weight of the European Single Market. However, this complementarity is consistently aligned with the EU's strategic interests and its commitment to a rules-based international order. Historical friction, such as the 1990s sanctions against Iraq, illustrates that European states often resist when U.S. policy 'changes the rules of the game' by shifting from disarmament goals to regime change (Nonneman, 2011, p. 221). This tension is institutionalized through the EU Blocking Statute (EC, 1996). This mechanism effectively works 'backwards' to protect European operators from being constrained by third-country sanctions that conflict with EU law. Thus, while sanctions often act as a force multiplier for U.S. goals, they also serve as a tool for the EU to assert its own autonomous strategic identity and legal standards.

III. Financial and Energy Autonomy

Beyond coercive sanctions, the EU is developing several new instruments to secure its energy and financial sectors against external influence. In the energy domain, the pursuit of autonomy centres on diversifying supply chains and reducing strategic dependencies (EEAS, 2022, p. 47). Key regulatory initiatives, such as the EU Energy

Platform, represent a strategic step toward using the Union's collective market weight to negotiate as a single strategic entity. By reducing resource vulnerability, the EU ensures its geopolitical decisions remain insulated from energy-based coercion.

In the financial realm, the EU focuses on strengthening its *Open Strategic Autonomy* by bolstering the international role of the euro to mitigate the impact of third-country extraterritoriality (European Commission, 2021, p. 1). This defensive posture is reinforced by the EU's framework for Foreign Direct Investment (FDI) screening, which coordinates the protection of strategic assets from coercive external acquisitions (European Parliament, Council of the European Union, 2019). While these tools can complement U.S. efforts to secure global supply chains, they primarily serve to give the Union the 'regulatory power' necessary to act independently. By building this independent infrastructure, the EU creates a frictional edge that can directly limit U.S. financial and energy leverage.

IV. The Defence Industrial Pivot

The final pillar of the EU's modern arsenal is the institutionalization of defence financing, which seeks to bridge the 'capability gap' identified in earlier decades by incentivizing a homegrown defence industrial base. The establishment of the European Defence Fund (EDF) through Regulation (EU, 2021a) could be understood as the institutional successor to the failed Helsinki Goal, solving through finance what could not be solved through force. This marks the first time the EU budget is used to co-fund competitive and collaborative projects in defence research and development. The primary objective is to enhance 'technological sovereignty' and reduce strategic dependencies by ensuring that intellectual property remains within the Union (EEAS, 2022, p. 47). This is complemented by the off-budget instrument, EPF, which allows the EU to provide military equipment and infrastructure to partners, effectively transforming the Union into a global security provider (European External Action Service, 2025).

These instruments are a significant source of friction: the EDF's strict third-country rules restrict U.S. contractor access to European funds and ensure interoperability is defined on European terms rather than through NATO-standardized U.S. hardware

(EU, 2021a Article 9; EEAS, 2022, p. 43; Lawrenson, Sabatino, 2024). By prioritizing the development of next-generation aircraft and naval systems within a European framework, these funding tools provide the material basis for Strategic Autonomy, setting the stage for a Union that can sustain its own security identity independent of U.S. industrial dominance.

Chapter 3: Strategic Autonomy and the Transatlantic Interaction

I. From ‘Strategic Comfort’ to ‘Practical Necessity’

The institutional developments examined in Chapter 2 find their clearest expression in the 2022 Strategic Compass (EEAS, 2022), which sets out the roadmap for deploying the EU's economic arsenal, including trade defence and coercive diplomacy, as a primary security modality. The interaction between transatlantic complementarity and friction in the financial sphere is most effectively analysed through the lens of European Strategic Autonomy (ESA). ESA entered EU discourse in 2013 but remains loosely defined as the ‘capacity to act autonomously when and where necessary and with partners wherever possible’ (EC, 2016, p. 2). To operationalize this concept for this paper, the typology (Costa, Soler i Lecha, Vlaskamp, 2025, p. 9) based on Fiott (2018) is employed, which allows ESA to be categorized into three distinct levels: operational autonomy, asset autonomy, and decision autonomy. Applied to the case studies, the typology allows assessment of where EU instruments generate autonomy. An example of these tiers in conflict occurred during the 2022 invasion of Ukraine, when EU Member States sought to provide military support but were initially restricted regarding the transfer of Swiss-manufactured 35mm ammunition for Gepard anti-aircraft systems. In this instance, while the EU possessed the operational means and the physical assets, it lacked ‘decision autonomy’ due to re-export vetoes imposed by a third-party manufacturer (Reuters, 2022).

Michaels and Sus (2025, p. 59) have argued that the necessity of these autonomies has been recognized within the EU since the 1990s, when this ideational shift emerged in response to the Union’s inadequate mechanisms for addressing the escalating conflicts in Bosnia and Kosovo. While this period gave birth to the Common Security and Defence Policy (CSDP) and led to independent operations such as Operation ARTEMIS, progress was ultimately constrained by ‘peace dividends’ and a persistent

reliance on the U.S. security guarantee. However, the transition from ‘strategic comfort’ to ‘practical necessity’ has been dramatically accelerated since 2018 by the realization that U.S. policy increasingly utilizes ‘weaponized commerce’ and ‘market distortions’ to achieve security objectives (Eliasson, Garcia-Duran, 2025, pp. 35–36). This shift in the global environment has effectively terminated the era of ‘naïve’ free trade, compelling the EU to adopt a more ‘assertive trade policy’ to protect its producers and strategic values (Eliasson, Garcia-Duran, 2025, pp. 36–37). While this move toward autonomy creates industrial friction, it simultaneously strengthens the EU's institutional capacity to act as a primary security provider, particularly through coordinated economic sanctions.

II. Complementary Power: The Ukraine/Russia Case Study

The transformation of EU sanctions against Russia since February 2022 marks a definitive shift toward the ‘weaponized interdependence’ of the Single Market, where regulatory power is used to project coercive force (Timofeev, Chupriyanova, 2024, p. 43). No longer merely punitive, these measures have evolved into a multifaceted ‘diplomatic tool’ designed to influence state behaviour and enforce international norms when kinetic confrontation is strategically precluded (Jánošová, 2023, p. 35). By adopting systemic restrictive measures that targeted core economic vulnerabilities, the EU utilized its economic depth as a ‘non-military alternative’ to war (Jánošová, 2023, p. 36). This approach has effectively turned sanctions into the ‘cornerstone’ of the Union's foreign policy, serving as a primary mechanism for projecting ‘EU actorness’ in the global security domain (Pertiwi, 2024, p. 62). Furthermore, the EU’s revised stance on ‘secondary sanctions’ and enforcement demonstrates a growing institutional willingness to align its regulatory core with the coercive requirements of modern geopolitical competition, providing a resilient secondary pillar for transatlantic security (Timofeev, Chupriyanova, 2024, p. 43). Ultimately, the EU’s ability to strategically reduce Russia's economic integration into the Single Market yields results that would be difficult to achieve through military force alone. However, this maturing institutional capacity simultaneously provides the foundational ‘asset autonomy’ required for the Union to protect its own interests, setting the stage for industrial friction regarding the exclusion of third-country contractors.

While the EPF's off-budget design simultaneously advances European asset autonomy by building an independent capacity to equip security partners, its operational effect in the Ukraine context has been unambiguously complementary: the Facility has ‘spurred rapid progress’ in the Union's capacity to deliver military equipment to partners (Clapp, 2022, p. 26). By coordinating these financial and industrial tools, the EU acts as a formidable force multiplier for transatlantic interests, reinforcing the credibility of the broader security architecture through market-based exclusion. This institutional maturation represents a ‘ground-breaking move’ toward a fully-fledged defence union, leveraging the Union’s collective ‘value cohesion’ to ensure the costs of aggression are prohibitive (EEAS, 2022, p. 10). This is largely the capacity that Kagan’s framework did not fully anticipate. His binary assumed that Europe would remain a normative actor, relying on attraction rather than coercion and avoiding the use of power. The Russia sanctions regime demonstrates that when strategic interests demand it, the EU can and does exercise coercive power at a scale that produces outcomes beyond the reach of U.S. military force alone.

III. Frictional Autonomy

While the EU’s sanctions regime primarily serves as a force multiplier for transatlantic security, the Union simultaneously employs its regulatory capability as a defensive shield to mitigate the extraterritorial reach of U.S. policy. This ‘frictional’ dimension of Strategic Autonomy is most evident when the EU perceives that U.S. secondary sanctions threaten its financial and industrial interests. The most direct institutional expression of this defensive posture is the deployment of the Blocking Statute, introduced in Chapter 2 as the legal mechanism that nullifies extraterritorial third-country legislation within EU jurisdiction (Schindler, 2021, p. 28). This defensive posture was operationalized through the creation of INSTEX (Instrument in Support of Trade Exchanges), a special-purpose vehicle established to facilitate non-dollar trade with Iran following the U.S. withdrawal from the JCPOA. Although its practical impact remained limited and it was dissolved in 2023, INSTEX was a powerful show of force in the field of decision autonomy, signalling the EU's intent to uphold its sovereign right to enforce international agreements even when faced with direct U.S. opposition (Schindler, 2021, p. 31).

Friction is further pronounced in the energy and technological domains, where divergent perceptions of ‘security’ create industrial deadlock. The Nord Stream 2 pipeline exemplified this ‘energy security dilemma,’ as Germany defended the project as a vital ‘commercial endeavour’. At the same time, the U.S. condemned it as a ‘geopolitical project’ targeted at Ukraine (Pifer, 2021; Shagina, Westphal, 2021). Despite intense U.S. sanction pressure, the EU initially resisted Washington’s efforts to define European energy parameters, viewing such interference as a challenge to its ‘decision autonomy’ (Russell, 2021). Similarly, the debate over 5G infrastructure and Huawei highlights the EU's struggle to navigate the ‘US-China tech rivalry’ without becoming a ‘mere object’ of external geopolitical contests (Rühlig, Seaman, Voelsen, 2019). By developing the ‘EU Toolbox for 5G Security,’ the Union moved to harmonize its internal market standards to mitigate the risks posed by high-risk suppliers, prioritizing ‘supply-chain resilience’ and ‘strategic security objectives’ over purely bilateral U.S. demands (EU, 2021b).

However, the most structural friction is created in the defence research and procurement. As detailed in Chapter 2 analysis of the Modern Arsenal, the European Defence Fund (EDF) institutionalizes this pivot by prioritizing ‘technological sovereignty’ over simple transatlantic efficiency (EEAS, 2022, p. 47). The Fund’s strict ‘third-country’ rules effectively control the participation of U.S. defence contractors and ensure that intellectual property remains within the Union. Thus, challenging the traditional U.S. expectation of open access to European defence budgets (Lawrenson, Sabatino, 2024). This creates a deliberate industrial deadlock: while the U.S. pushes for increased European spending to support NATO, the EU utilizes these financial instruments to build an autonomous industrial base.

IV. Synthesis

Table 1 maps friction cases exclusively; complementary interactions do not require autonomous capacity and therefore fall outside the Fiott typology's analytical scope.

Case	*Fiott*	*Mechanism*
INSTEX/ Blocking statute	Decision	Asserts sovereign right to define legal and trade parameters independent of U.S. secondary sanctions.
Nord Stream 2	Decision	Resists U.S. attempts to define European energy security parameters as a challenge to independent strategic choice.
EDF third country rules	Asset	Builds an independent industrial and technological base by excluding U.S. contractors and retaining intellectual property within the EU.
Huawei/ 5G toolbox	Asset and Decision	Protects technological infrastructure as a strategic asset while asserting the right to define security standards independently of U.S. bilateral demands.

Table 1. Fiott typology mapped to case studies. Source: Author's own, based on the work of Fiott, 2018.

Notably, operational autonomy is absent from this table. This is not an oversight, but a reflection of a structural reality already established in Chapter 1. Operation ARTEMIS demonstrated that operational autonomy, the capacity to plan and execute independent missions, while briefly achieved, rested on a single framework nation and exposed capability and interest shortfalls that the EU could not collectively sustain. The strategic pivot toward economic instruments that followed was, in this sense, a deliberate substitution: building decision and asset autonomy through regulatory and market means precisely because operational military autonomy had proven largely out of reach. The friction cases here are therefore not a partial picture of European strategic autonomy, but rather presentations of the institutional logic produced by the post-ARTEMIS era.

The recent rise in prominence of European Strategic Autonomy (ESA) has not been a temporary reaction to the volatility of specific U.S. administrations, but a structural response to a long-term ‘ideational shift’ in the transatlantic relationship. While the U.S. historically pursued policies designed to ‘prevent alternatives to NATO’ and maintain sole responsibility for European defence (Dietl, 2009, p. 431)The ‘strategic comfort’ of

this arrangement has eroded as the post-Cold War Liberal International Order (LIO) undergoes a profound process of ‘fragmentation’ (Costa et al., 2025, p. 3). This fragmentation forces the Union to confront its identity as a ‘legal colossus’ that has, until recently, remained ‘impotent in terms of the core coercive powers’ typically associated with states (Kelemen, McNamara, 2022, p. 964).

Even as the transatlantic alliance has been described by many world leaders and scholars alike as the most successful and profitable in human history so far (Stoltenberg, 2019; Mayberry, 2022; Biden, 2024), the friction at the heart of LIO fragmentation is a fundamental clash of strategic modalities. While the EU defines its global role through a commitment to a ‘rules-based global order’ and ‘multilateralism’ (Costa et al., 2025, p. 5). It increasingly perceives U.S. policy as adopting an ‘explicitly bilateral approach that cuts across these aims’. Some European officials have viewed this dynamic as a deliberate sabotage of collective EU policy through the divide-and-conquer strategy, in which Washington strikes bilateral deals with individual member states to undermine the Union’s collective bargaining power (Nonneman, 2011, p. 214). Consequently, ESA is the EU’s necessary evolution into a strategic provider that must ‘weaponize’ its regulatory core to protect its interests in an era in which the U.S. security guarantee is no longer a constant but a variable in a fragmenting world.

Conclusion

This paper examined transatlantic security through a complement–friction lens, focusing on economic instruments as the centre of the debate over Europe’s strategic autonomy. It argued that the EU and the United States approach security from distinct origin stories and strategic cultures: first, a European project designed to embed peace through law, markets, and institutions, versus a U.S. hegemon accustomed to military primacy and global force projection. Reframed in these terms, Europe's reliance on economic statecraft is not Kagan's weakness but a different modality of strength, institutionalized to support European values and interests. The evidence bears this out across a visible developmental arc. Where institutional depth had time to mature, sanctions that decoupled a major economy from the global financial system, an EDF building an autonomous defence industrial base, the Blocking Statute asserting European legal sovereignty, the EU succeeded at operating as a strategic actor.

Nevertheless, where it reached beyond its designed capacity the case studies of INSTEX and Nord Stream 2, outcomes fell short. However, these are not simply failures, as a purely dependent actor does not attempt INSTEX, does not legislate the Blocking Statute, does not restrict its own defence fund against its primary security guarantor. The attempts, however imperfect, are iterative signals of a maturing actor building the institutional memory necessary for more effective future assertion.

This maturation is unfolding precisely as the Liberal International Order fragments, driven by a sustained U.S. pivot to the Indo-Pacific and the shock of Russian aggression, making this divergence ever more salient. The result is a burden-sharing paradox: U.S. pressure on Europe to assume greater responsibility catalyses capacity-building and reform. However, increased capability also expands decision autonomy, which increases friction when worldviews or regional priorities diverge. In short, complement rises with shared ends; friction grows with independent means. The paper's analysis offers one concrete recommendation for the EU's development: to appreciate and institutionalise the natural friction. The Blocking Statute protects European operators from external legal coercion. No equivalent mechanism exists to govern member states internally, leaving collective asset autonomy vulnerable to bilateral defence deals that bypass the strategic logic the EDF was designed to enforce. The recommendation is to institutionalize this protection inward: a code of conduct, backed by a consultative veto and funding priorities. This would limit individual member states from striking bilateral defence agreements that undermine the EU's collective sovereignty – an internal governance tool, not a transatlantic proposal, and an institutional complement to the economic-security architecture this paper has analysed.

Furthermore, the complement-versus-friction dynamic is not unique to EU-U.S. relationship. Parallel signals of allied autonomy and security hedging are visible across the bigger transatlantic space, where Canada provides a prime example of defence diversification efforts (European Commission, 2025; Office of the Prime Minister of Canada, 2025). A realist reading clarifies the mechanism: as Mearsheimer (1994) argues, multilateral architectures persist when they serve significant power interests; when the implicit bargain - sovereignty traded for security - is questioned, actors reinsure with hard power and with economic/regulatory autonomy. With *pacta sunt*

servanda in question and U.S. commitment uncertain, strategic autonomy becomes not just the EU's 2013 ambition but a practical necessity. In that context, Europe's economic instruments become central components of its strategic agency: coercive sanctions, industrial policy, and financial/energy hedges that both amplify transatlantic objectives when aligned and constrain them when autonomy is at stake.

Bibliography

ANGHEL, Susana. and DAMEN, Mario G.H. 2025. The future European security architecture: Dilemmas for EU strategic autonomy. European Parliamentary Research Service (EPRS).

BIDEN, Joe. 2024. Remarks by President Biden on the 75th Anniversary of the North Atlantic Treaty Organization Alliance. [Online]. 9 July 2024. [Cited : 21 January 2026]. https://it.usembassy.gov/remarks-by-president-biden-on-the-75th-anniversary-of-the-north-atlantic-treaty-organization-alliance/. Published: U.S. Embassy & Consulates in Italy.

ČESNAKAS, Giedrius and JUOZAITIS, Justinas (eds.). 2024. *European Strategic Autonomy and Small States' Security: In the Shadow of Power*. Routledge. Routledge Studies in European Security and Strategy.

CLAPP, Sebastian. 2022. Implementation of the Strategic Compass: Opportunities, Challenges and Timelines. *European Parliamentary Research Service*. [Online]. (EPRS).
https://www.europarl.europa.eu/RegData/etudes/STUD/2022/739249/EPRS_STU(2022)739249_EN.pdf.

COSTA, Oriol, SOLER I LECHA, Eduard and VLASKAMP, Martijn C. (eds.). 2025. *EU Foreign Policy in a Fragmenting International Order.* Cham: Springer Nature. The European Union in International Affairs.

DIETL, Ralph. 2009. The WEU: A Europe of the Seven, 1954–1969. *Journal of Transatlantic Studies*. 2009. Vol. 7, no. 4, pp. 431–452. DOI 10.1080/14794010903286292.

DUKE, Simon. 2011. EU Decision-making in CSDP: Consensus Building on Operation Artemis. In: **THOMAS, Daniel C. (ed.)**, *Making EU Foreign Policy: National*

Preferences, European Norms and Common Policies. New York: Palgrave Macmillan. pp. 92–110.

EC. 1996. Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom. *Council of the European Union.* [Online]. 1996. https://eur-lex.europa.eu/eli/reg/1996/2271/oj/eng Published: Official Journal of the European Communities, L 309, 29 November 1996, pp. 1–6.

EC. 2016. Council Conclusions on Implementing the EU Global Strategy in the Area of Security and Defence. *Council of the European Union* [Online]. November 2016. https://www.consilium.europa.eu/media/22459/eugs-conclusions-st14149en16.pdfPublished: 3498th Foreign Affairs Council Meeting.

EEAS. 2022. A Strategic Compass for Security and Defence [Online]. Brussels: European External Action Service. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf.

ELIASSON, L. Johan and GARCIA-DURAN, Patricia. 2025. EU Trade Policy in Light of a Fragmented Liberal International Order. In: **COSTA, Oriol, SOLER I LECHA, Eduard and VLASKAMP, Martijn C. (eds.).** *EU Foreign Policy in a Fragmenting International Order*. Cham: Springer Nature. pp. 27–54.

EU. 2021a. Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092. [Online]. 2021. European Parliament and Council of the European Union. https://eur-lex.europa.eu/eli/reg/2021/697/oj/engPublished: Official Journal of the European Union, L 170, 12 May 2021, pp. 149–177.

EU. 2021b. EU Toolbox for 5G Security: A Set of Robust and Comprehensive Measures for an EU Coordinated Approach to Secure 5G Networks. Luxembourg: European Commission, Directorate-General for Communications Networks, Content and Technology.

EUROPEAN COMMISSION. 2021. The European Economic and Financial System: Fostering Openness, Strength and Resilience [Online]. Brussels: European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0032.

EUROPEAN COMMISSION. 2025. EU and Canada sign landmark Security and Defence Partnership at 20th Summit. [Online]. June 2025.

https://policy.trade.ec.europa.eu/news/eu-and-canada-sign-security-and-defence-partnership-20th-summit-2025-06-24_en.

EUROPEAN COUNCIL. 1999. Cologne European Council Declaration on Strengthening the Common European Policy on Security and Defence. [Online]. June 1999. https://www.consilium.europa.eu/media/21070/57886.pdf.

EUROPEAN EXTERNAL ACTION SERVICE. 2025. The European Peace Facility Factsheet. [Online]. 2 December 2025. https://www.eeas.europa.eu/eeas/european-peace-facility-factsheet_en.

EUROPEAN PARLIAMENT and COUNCIL OF THE EUROPEAN UNION. 2019. Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union. [Online]. 19 March 2019. http://data.europa.eu/eli/reg/2019/452/oj.

EUROPEAN UNION. 2012. Document available on EUR-Lex: Access to European Union Law (CELLAR ID 2bf140bf-a3f8-4ab2-b506-fd71826e6da6). *Publications Office of the European Union*. [Online]. 2012. https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF.

FARRELL, Henry and NEWMAN, Abraham L. 2019. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*. 2019. Vol. 44, no. 1, pp. 42–79. DOI 10.1162/isec_a_00351.

FIOTT, Daniel. 2018. Strategic Autonomy: Towards 'European Sovereignty' in Defence? *EUISS Brief*. 2018. No. 12, pp. 1–8.

FREEDMAN, Lawrence and KARSH, Efraim. 1993. *The Gulf Conflict, 1990-1991: Diplomacy and War in the New World Order*. Princeton, NJ: Princeton University Press. ISBN 0-691-08627-3.

JÁNOŠOVÁ, Viktória. 2023. EU Sanctions Against Russia – The Impact on the Russian and EU Markets. *Slovak Yearbook of European Union Law*. 2023. Vol. 3, pp. 35–50. DOI 10.54869/syeul.2023.3.796.

JUSTAERT, Arnout and KEUKELEIRE, Stephan. 2010. The EU's Security Sector Reform Policies in the Democratic Republic of Congo. *European Integration online Papers (EIoP)*. 2010. Vol. 14, no. 6. DOI 10.1695/2010006.

KAGAN, Robert. 2002. Power and Weakness. *Policy Review*. July 2002.

KELEMEN, R. Daniel and MCNAMARA, Kathleen R. 2022. State-building and the European Union: Markets, War, and Europe's Uneven Political Development.

Comparative Political Studies. 2022. Vol. 55, no. 6, pp. 963–991. DOI 10.1177/00104140211047393.

KEOHANE, Robert O. and NYE, Jr., Joseph S. 2011. *Power and Interdependence. Fourth*. Boston: Longman.

KILIC, Seray. 2023. Half-Hearted or Pragmatic? Explaining EU Strategic Autonomy and the European Defence Fund through Institutional Dynamics. *Central European Journal of International and Security Studies*. 2023. Vol. 18, no. 1, pp. 43–72.

LAȚICI, Tania and KRAUSE, Tristan. 2021. Who does what in security and defence? *European Parliament Liaison Office in Washington DC.* [Online]. Washington, DC: European Parliamentary Research Service (EPRS);. https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/698046/EPRS_ATA(2021)698046_EN.pdf.

LAWRENSON, Tim and SABATINO, Ester. 2024. The Impact of the European Defence Fund on Cooperation with Third-country Entities. *International Institute for Strategic Studies (IISS).* [Online]. https://www.iiss.org/research-paper/2024/10/the-impact-of-the-european-defence-fund-on-cooperation-with-third-country-entities/.

MAUER, Victor. 2011. Iraq 2003: Regime change and European discontent. In: **MÖCKLI, Daniel and MAUER, Victor (eds.)**, European–American Relations and the Middle East: From Suez to Iraq. pp. 26–45.

MAYBERRY, Anthony A. 2022. Defense Integration and Economic Growth in the North Atlantic. *SSRN Electronic Journal*. [Online]. 19 November 2022. [Cited : 21 January 2026]. https://ssrn.com/abstract=4281186.

MEARSHEIMER, John J. 1994. The False Promise of International Institutions. *International Security.* 1994. Vol. 19, no. 3, pp. 5–49.

MEARSHEIMER, John J. 2001. *The Tragedy of Great Power Politics*. [Online]. New York: W. W. Norton & Company. ISBN 0-393-02025-8. https://books.google.com/books/about/The_Tragedy_of_Great_Power_Politics.html?id=jOV9HuCppqwC.

MICHAELS, Eva and SUS, Monika. 2025. Strategic Autonomy in Security and Defence as an Impracticability? How the European Union's Rhetoric Meets Reality. In: **COSTA, Oriol, SOLER I LECHA, Eduard and VLASKAMP, Martijn C. (eds.).** *EU Foreign Policy in a Fragmenting International Order*. Cham: Springer Nature. pp. 55–84.

MÜLLER, Patrick and SPENCER, Claire. 2011. From Madrid to Camp David: Europe, the US, and the Middle East Peace Process in the 1990s. In: **MÖCKLI, Daniel and MAUER, Victor (eds.).** *European–American Relations and the Middle East: From Suez to Iraq*. Oxon; New York: Routledge. pp. 113–123.

MUSU, Costanza. 2011. The Middle East Quartet: A New Role for Europe? In: **MÖCKLI, Daniel and MAUER, Victor (eds.),** *European–American Relations and the Middle East: From Suez to Iraq*. London and New York: Routledge. pp. 124–138.

NONNEMAN, Gerd. 2011. Europe, the US, and the Gulf after the Cold War. In: **MÖCKLI, Daniel and MAUER, Victor (eds.)**, *European–American Relations and the Middle East: From Suez to Iraq*. pp. 203–219.

NYE, Joseph S., Jr. 2004. Soft Power: The Means to Success in World Politics. PublicAffairs.

OFFICE OF THE PRIME MINISTER OF CANADA. 2025. Prime Minister Carney secures Canada's participation in the European Union's SAFE initiative. *Government of Canada*. [Online]. https://www.pm.gc.ca/en/news/news-releases/2025/12/01/prime-minister-carney-secures-canadas-participation-european-unions.

PERTIWI, Lunyka Adelina. 2024. The EU's Approach to Sanctions on Russia: A Critical Analysis of the Existing Literature. Central European Journal of International and Security Studies. 2024. Vol. 18, no. 3, pp. 61–86. DOI 10.51870/NOEX4475.

PIFER, Steven. 2021. *Nord Stream 2: Background, Objections, and Possible Outcomes* [Online]. Washington, D.C.: Foreign Policy at Brookings. https://www.brookings.edu/wp-content/uploads/2021/04/FP_20210412_nord_stream_2_pifer.pdf.

REUTERS. 2022. Swiss block German request to re-export tank ammunition to Ukraine. *Swissinfo*. [Online]. April 2022. https://www.swissinfo.ch/eng/business/swiss-block-german-request-to-re-export-tank-ammunition-to-ukraine/47548036.

RÜHLIG, Tim, SEAMAN, John and VOELSEN, Daniel. 2019. 5G and the US–China Tech Rivalry – a Test for Europe's Future in the Digital Age: How Can Europe Shift from Back Foot to Front Foot? Berlin: Stiftung Wissenschaft und Politik (SWP).

RUSSELL, Martin. 2021. The Nord Stream 2 pipeline: Economic, Environmental and Geopolitical Issues. European Parliamentary Research Service (EPRS). [Online]. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690705/EPRS_BRI(2021)690705_EN.pdf.

SCHINDLER, Hans-Jakob. 2021. An Assessment of the Efforts to Mitigate the Impact of US Secondary Sanctions: The EU Blocking Statute and INSTEX. In: SHINE, Sima (ed.), Iran and the International Arena: Challenges and Opportunities. Tel Aviv: Institute for National Security Studies (INSS). [Online]. pp. 29–39. https://www.inss.org.il/wp-content/uploads/2021/02/IranMonograph_e-29-39.pdf.

SHAGINA, Maria and WESTPHAL, Kirsten. 2021. *Nord Stream 2 and the Energy Security Dilemma: Opportunities, Options and Obstacles for a Grand Bargain*. Berlin: Stiftung Wissenschaft und Politik (SWP).

STOLTENBERG, Jens. 2019. NATO: good for Europe and good for America — Address to the United States Congress. [Online]. 3 April 2019. [Cited : 21 January 2026]. https://www.nato.int/en/news-and-events/events/transcripts/2019/04/03/nato-good-for-europe-and-good-for-america.

TIMOFEEV, Ivan and CHUPRIYANOVA, Polina. 2024. EU Sanctions against Russia after February 2022: Major Transformational Trends. *Contemporary World Economy*. 2024. Vol. 2, no. 2, pp. 43–59. DOI 10.17323/2949-5776-2024-2-2-43-59.

TOMOLYA, János. 2015. Operation ‘Artemis’: The First Autonomous EU-led Operation. *AARMS – Academic and Applied Research in Military and Public Management Science*. 2015. Vol. 14, no. 1, pp. 121–132. DOI 10.32565/aarms.2015.1.11.

MAJ Silvana MELE: Assessing the Role of Generative AI in Shaping Disinformation Strategies within Grey Zone Operations

Supervisor: Dr. Dumitru MINZARARI

Statement on the Use of AI Tools:

In the preparation of this research paper, AI tools were utilised exclusively for editorial assistance and critical review. Specifically, AI (Grammarly and Gemini) was employed to identify grammatical and typographical errors, to refine the diction, and subject the author's arguments to adversarial testing to identify potential logical weaknesses.

The core concepts, research, recommendations, and final text formulation are the sole work of the author.

Introduction

Disinformation campaigns exploit the freedom of the information environment, especially online, by leveraging the characteristics of human cognition. AI-enabled capabilities applied to disinformation campaigns are rapidly evolving, driven by the abundance of data, innovative algorithms, and massive computing power; their most significant impact is likely to be on social media. Western societies, due to their openness, are particularly vulnerable to the malicious effects of AI-powered influence, as they continually struggle to balance free speech with the harmful consequences of disinformation. The primary aim of disinformation, particularly the one conducted by authoritarian regimes, is to exploit the vulnerabilities of democracies, provoking, disrupting, and dividing, while straining individual decision-making, societal cohesion, and the ability to reach consensus; in short, inhibiting democracies from functioning and eroding the underlying pillar of trust. Due to their reach, media organisations are prime targets of disinformation campaigns. (Sedova, et al., 2021a)

Hence, what is the impact of Generative AI on the effectiveness of disinformation campaigns in grey zone operations?

Unlike traditional propaganda, which relies on the manual creation of biased narratives, I argue that Generative Artificial Intelligence (GenAI) in the grey zone could be characterised by four variables: scale, realism, speed and cost. The shift in the effectiveness of disinformation campaigns enabled by GenAI is both quantitative and qualitative; it reduced the production costs of high-fidelity, multimodal, and culturally resonant propaganda, thereby enabling persistent, pervasive, and personalised influence operations that can overwhelm traditional fact-checking and societal resilience. Therefore, it simultaneously amplifies their ability to spread confusion, division, and distrust in target societies. Yet, GenAI also fosters the development of new countermeasures (such as deepfake detection and fact-checking tools), highlighting its double-edged impact: it enhances the offensive effectiveness of disinformation while forcing defensive adaptations in grey zone information warfare.

As highlighted in recent NATO analyses, the strategic objective within this grey zone is no longer merely to deceive, but to destabilise. (Hsu, 2023)

To illustrate this shift, this research employs a qualitative methodology to examine the causal mechanisms by which GenAI enhances the effectiveness of disinformation in grey zone operations. Two micro-case studies were selected based on three criteria: documented forensic evidence from credible institutional sources, divergent strategic objectives between the two state actors, and sufficient operational maturity to allow meaningful analysis. Russia's Operation Doppelgänger and China's Shadow Play network satisfy all three conditions. The primary sources for this analysis consist of open-source reports, forensic analyses published by institutional actors (NATO StratCom COE, EU DisinfoLab, ASPI, RAND Corporation), and peer-reviewed academic literature. A notable limitation of this approach is its reliance on secondary forensic data; the classified intelligence that would provide a complete operational picture of these campaigns remains inaccessible. Additionally, selecting only two micro-case studies limits the generalisability of the findings, though the depth of analysis compensates for this limitation. The research also applies the OODA Loop (Observe-Orient-Decide-Act) model to evaluate how AI-driven velocity disrupts the decision-making cycles of democratic institutions.

This study is organised to advance from theoretical frameworks to empirical analysis and a possible response. The first section introduces the concepts on which the entire analysis rests, capturing the shift in disinformation from the pre-generative era to the present. The second section provides the empirical foundation for this analysis through comparative micro-case studies of Russia's Operation Doppelgänger and China's Shadow Play network, highlighting how state actors operationalise AI-driven interference. Building on this evidence, the third section deconstructs the specific strategic enhancement mechanisms that disrupt the democratic decision-making cycles. The fourth section evaluates the limitations of existing technical and legislative countermeasures and advocates cognitive immunity as a necessary step toward societal resilience. Finally, the last section synthesises the research findings to address the primary research question and suggests future implications and areas of research.

Context of Research and Background

This section defines the conceptual baseline of the research by situating GenAI within the modern geopolitical landscape, specifically in the grey zone. The grey zone is a domain characterised by deliberately calibrated aggressive actions below the threshold of conventional war. Traditional military engagement is bypassed to maintain operational ambiguity and complicate attribution through alternative and unconventional means to exploit and potentially weaponise civilian instruments. For this analysis, I will rely on Watson's (2024) definition of AI, which states that AI is a branch of computer science focused on emulating the human intellect in language comprehension and logical reasoning. These technologies range from basic algorithms to adaptable learning models. The effectiveness of AI in the cognitive domain lies not only in its capacity to emulate human intellect but also in its ability to identify and exploit human cognitive biases, such as confirmation bias. This capability enables tailoring narratives that bypass rational scepticism, thereby creating a personalised reality, as discussed later in this research.

Within this ambiguous environment, disinformation serves as a primary tool for fracturing the information environment and undermining democratic institutions. Formally defined as false information spread deliberately and often covertly to manipulate public opinion, disinformation has historically been a resource-intensive endeavour. To understand the complexity of this threat, it is necessary to categorise the different forms of information interference that it can take. Wardle (2017) provides a foundational taxonomy of seven levels of information disorder, ranging from false connection to fabricated content. This content-based typology highlights that disinformation is a spectrum of manipulation. In the pre-generative era, these operations were characterised by the use of human operators, often referred to as troll farms, in specific departments to create realistic content and high-volume, repetitive messaging that either created a sense of consensus or exhausted authentic users. While effective, these operations were constrained by the biological limitations of human operators. The emergence of GenAI has altered the work structure by automating the time-consuming tasks identified in the Center for Security and

Emerging Technology (CSET) RICHDATA[1] framework.(Sedova, McNeill, Johnson, Joshi, Wulkan, 2021b) This automation may amplify disinformation techniques, increasing their effectiveness in shaping future campaigns.

The technology behind this shift lies in Generative Adversarial Networks (GANs), which, according to Watson (2024), are a class of two distinct artificial neural networks trained together and working as antagonists. The generator aims to produce realistic data, while the discriminator attempts to distinguish it from real data. This process is behind the creation of increasingly convincing synthetic content. This technology, alongside Variational Autoencoders (VAEs), which learn from a compressed probabilistic latent representation of the inputs to generate new outputs, as well as diffusion models, which create data by progressively adding noise to the data and then learn to iteratively denoise the data in an organised fashion to generate new data, provide the foundation for Large Language Models (LLMs) that generate human-like text, audio, and video from training datasets. (Taeihagh, 2025)

These algorithms are trained to provide human-like content, not accurate information. And this is the main feature that makes them a considerable threat if used to spread misinformation, propaganda or hate speech. Given that the primary aim of grey-zone aggression is to weaken a country without resorting to military violence, GenAI acts as an equaliser, particularly for asymmetric actors, allowing them to circumvent traditional barriers and achieve technological parity at an unprecedented pace. (Braw, 2023)

The effectiveness of these technical capabilities is further amplified by the structural features of social media platforms, which define the terrain and shape threat actors' tactics. The open-source culture of the AI research community, which fosters advances, also provides malicious actors with ready access. Disinformation campaigns are asymmetric. Threat actors often operate across multiple platforms, making it difficult to fully understand the scope of their activity. In addition, the lines are blurring between the foreign-manufactured disinformation and the homegrown misinformation. (Sedova, et al., 2021a)

[1] RICHDATA: Reconnaissance, Infrastructure, Content Creation and Hijacking, Deployment, Amplification, Troll Patrol, Actualisation.

Putting all this together, we see that the scale, realism and speed introduced by GenAI constitute a great challenge for modern democratic societies characterised by freedom of speech when it comes down to discerning truth from generated lies. The risk is that people will either believe anything or won't know what to believe. And the main consequence is what is being defined as the liar's dividend: exploiting the lack of trust through manipulation to advance the liar's own end. (Hsu, 2023) Disinformation campaigns leverage the technical, cognitive and social spheres of our lives, eroding the shared baseline of reality required for democratic consensus and societal resilience.

Micro-Case Studies Foundation

This section moves from the conceptual frameworks described so far to the empirical analysis of documented events. By contrasting the divergent methodologies of the Russian Federation and the People's Republic of China (PRC), the two following micro-case studies, Russia's Operation Doppelgänger and China's Shadow Play network, will highlight how AI-driven disinformation is being actively manufactured to achieve specific geopolitical effects.

Russia: Operation Doppelgänger

The investigation into Operation Doppelgänger provides a primary data foundation for characterising the evolution from traditional disinformation to high-fidelity semantic infiltration within the grey zone. According to the NATO Strategic Communications Centre of Excellence (Sessa et al., 2024), Operation Doppelgänger is a Russian-based network that has been operational in Europe since at least May 2022 and has been exposed by EU DisinfoLab. The technique behind this campaign is an architecture of impersonation, in which dozens of internet domain names were purchased to mimic the digital fingerprints of trusted Western institutions (a practice known as typosquatting). Over 17 major news sites, including The Guardian, Le Monde, and ANSA, were targeted. The Official NATO website was not immune either; during the July 2023 Vilnius summit, it was cloned on a different domain to host counterfeit press releases.

These efforts are not limited to deception but also utilise doctored videos, manufactured polls, and articles to perfectly replicate the journalistic tone of the hijacked authentic websites. The operation leveraged social media platforms like Facebook as an amplification engine; the network utilised paid advertisements totalling at least $115,000 USD to boost the visibility of its synthetic content. Despite significant takedowns and legal prosecutions in affected member states, forensic findings from 2023 confirm the campaign is persistent and expanding.

The persistent and decentralised nature of this campaign has led the counter-disinformation community to institutionalise it as a prominent Information Manipulation Set (IMS), as the EU DisinfoLab stated and analysed in its 2026 report. (EU DisinfoLab, 2026) This framework identifies Doppelgänger as a cluster of technically and operationally linked assets used for coordinated interference. The adoption of the IMS model by institutional stakeholders (EU DisinfoLab, Viginum, and the European External Action Service) represents a significant acknowledgement of the systemic threat posed by high-fidelity disinformation. By shifting the analytical focus away from isolated social media incidents toward a wider, decentralised infrastructure, the IMS designation signals that cognitive warfare has moved beyond episodic propaganda into a phase of permanent aggression. This institutional shift addresses the critical vulnerability of duplicate reporting, which often inflates the apparent scale of operations and overwhelms policymakers. It recognises that in the grey zone, the primary target is no longer just the narrative itself, but the institutional capacity to recognise and attribute the underlying mechanisms of interference.

The Doppelgänger IMS thus poses a challenge to institutional situational awareness, limiting defensive efforts to a reactive cycle of technical verification.

China: Shadow Play

While Russia employs a strategy of disruption, the PRC utilises GenAI to shift the narrative. (Keast, 2023) The theoretical writings on the People's Liberation Army (PLA) by researcher Li Bicheng emphasise how Beijing's strategy is transitioning from defensive censorship to offensive algorithmic cognitive warfare. The objective is not

anarchy, but the displacement of Western liberal narratives with a synchronised, authoritarian consensus defined as ’positive propaganda’. (Beauchamp-Mustafaga et al., 2024) The Shadow Play campaign (2023-2024) represents a proactive effort to dominate global normative narratives and shape the international information environment through algorithmic volume.

A forensic analysis by the Australian Strategic Policy Institute (ASPI) identified a network of at least 30 YouTube channels that produced over 4,500 videos, garnering approximately 120 million views and 730,000 subscribers. The campaign utilised AI voice cloning and avatar generation to create accounts that narrated pro-CCP talking points in English, including Chinese technological superiority and Western decline across various sectors. While formal attribution is not yet clear, ASPI suggests it may be a commercial actor operating under some degree of state direction.

This operation demonstrates the removal of human biological constraints, enabling a volume of content that submerges viewers. GenAI is being utilised to create an artificial consensus, leveraging the cost-efficiency of synthetic media to establish strategic narratives that are increasingly difficult for audiences to distinguish from public opinion. The videos covered a consistent set of thematic clusters: Chinese advances in semiconductor manufacturing, electric vehicles, space exploration, and high-speed rail were compared with narratives of American institutional dysfunction, economic fragility, and social division. The AI-generated avatars presented these narratives in fluent, accent-neutral English. The YouTube recommendation algorithm served as an amplifier: once a user engaged with one video, the platform’s engagement-optimisation logic directed them toward an expanding catalogue of related content, creating a self-reinforcing exposure loop without any additional cost to the operators. (Keast, 2023)

The RAND report focuses on extensive original Chinese-language open-source material by Li Bicheng, a Chinese military-affiliated researcher, to understand how the military approaches social media manipulation. The Chinese military likely began developing social media manipulation capabilities by the mid-2010s. The advent of GenAI accelerated a shift from traditional information operations models (psychological, public opinion and legal warfare) toward a more holistic approach that seeks to manipulate how target audiences process information and perceive reality.

GenAI serves as a force multiplier by overcoming cultural nuance and linguistic barriers. According to Li Bicheng's theories, Shadow Play appears to be the practical validation of the evolution of information warfare.

Comparative Synthesis

The two micro-case studies reveal a fundamental divergence in how state actors instrumentalise the same technology. Russia's Operation Doppelgänger operates through a logic of disruption: the objective is to fracture Western cohesion by flooding the information space with contradictory narratives, eroding trust in institutions and media. The campaign is decentralised, opportunistic, and reactive to the news cycle. China's Shadow Play, by contrast, follows a logic of displacement: rather than sowing chaos, it aims to construct a coherent alternative narrative architecture that gradually normalises authoritarian perspectives within global discourse. Where Russia seeks to destroy consensus, China seeks to replace it.

Despite these divergent objectives, both operations share a common reliance on GenAI to overcome the same three constraints: the cost of producing culturally credible content at scale, the linguistic barriers that previously limited the reach of non-English-language actors, and the biological limitations of human operators. These shared enablers constitute the enhancement mechanisms analysed in the following section.

Enhancement Mechanisms

The evidence gathered from Operation Doppelgänger and the Shadow Play network reveals a convergence in the use of GenAI as an enabler and a force multiplier. Russian and Chinese methodologies on the use of GenAI diverge in their geopolitical objectives. Drawing on the mirco-case studies, this research identifies three distinct dimensions of GenAI enhancement: speed, realism, and scale. All of which are enabled and scaled by a fourth overarching variable: the collapse of production costs. These factors affect the human and political levels and democracies, enabling strategic gains (Whyte, 2020) while challenging the ethical dimension (Bontridder et al., 2021). Their combination allows adversaries to synchronise shaping actions across different domains to define the environment in which they occur, while obscuring the

aggressor's ultimate intent. To the defender, the shaping actions might appear as isolated incidents (fake news stories, cyber intrusions, protests). However, to the aggressor, these are tiles of a wider mosaic designed to shape the operational environment. By the time the defender connects the dots, the target nation's cohesion has been degraded. Hence, GenAI becomes a powerful amplification tool, and not only one of deception.

Speed and Asymmetry of Verification

The integration of GenAI into influence operations has created a 'dissemination engine' characterised by machine-speed velocity. As detailed in the RICHDATA framework (Sedova et al., 2021b), the transition from human-operated troll farms to digital GAN armies removes the constraints of fatigue and cognitive load that are typical of human operators. An automated system generates, tests, and deploys thousands of multimodal variations of a narrative in the time it takes a human operator to draft a single tweet. This capability enables saturation of the information environment at a pace that outpaces the natural speed of human discourse while reducing costs.

This velocity introduces an asymmetry of verification. While a generative model can produce a high-fidelity deepfake artefact in milliseconds, forensic verification of that artefact by democratic institutions can take hours or even days (Braw, 2023). The Vilnius summit cloning during Operation Doppelgänger illustrates this gap concretely: counterfeit NATO press releases were circulated and shared across social media platforms well before institutional verification declared them fraudulent. The damage was not in the content of the fake releases themselves, but in the doubt they seeded about the authenticity of legitimate communications. This temporal gap creates a manoeuvre space for malicious stakeholders, where they operate unopposed, exploiting the defender's inability to identify aggression during its early stages (Stockwell et al., 2024). By the time the truth is established, the potential impact of the disinformation has already been internalised by the target audience, rendering the correction potentially irrelevant.

From a doctrinal perspective, this asymmetry functions as a Denial-of-Service (DoS) attack on the defender's OODA Loop. Traditional defensive doctrines rely on the

Observe phase to identify a threat. However, when the observation space is flooded with high-fidelity noise, the Orient phase (the ability to understand the context) collapses. (Stockwell et al., 2024) The defender is forced into a permanent state of reaction, overloading institutional resources on verifying individual artefacts rather than countering the broader strategic intent. Consequently, I argue that the aggressor can effectively and deliberately disrupt the target state's decision-making cycle, seizing the strategic initiative before the defender can even classify the threat. This is a primary objective of aggressors: to achieve surprise in the defender, ideally trapping them in the verification process. This resembles the Electronic Countermeasures (ECM) and Counter-Countermeasures (ECCM) race in traditional warfare, only it’s now being applied to the cognitive domain with the precise intent to identify and exploit societal and institutional vulnerabilities before a defender even perceives the intrusion. This could lead to a reshaping of the defender's decision-making baseline before they can effectively orient to the threat.

Realism through Algorithmic Reframing

Influence operations, while not revolutionary, are significantly evolving, transitioning from the fabrication of fake news to reframing. GenAI, specifically LLMs, now allows adversaries to shift to a more subtle form of language weaponisation. Instead of inventing a crisis, AI agents can now ingest legitimate news reports and rewrite them in specific ideological terms at an unprecedented scale, below a threshold that could trigger alarms or suspicion. This process can be defined as ’algorithmic reframing’. Instead of inventing a fake event, AI takes a true story and rewrites it using different emotional words and angles. While keeping the basic facts true, it changes how the reader feels about them. Because the core facts are technically correct, this slips past the software designed to catch fake news and misinformation. The subtlety lies in a malicious takeover of meaning by using your own reality against you.

This reframing capability is operationalised through automated micro-targeting. AI systems based on machine learning are now capable of analysing vast datasets of user or voter behaviour to identify personality-based vote segmentation: psychometric profiling. (Kertysova, 2018) By combining this data with generative models, aggressors can achieve a level of granularity previously impossible, potentially targeting the

individual, optimising to trigger the specific confirmation bias of their target. This creates a personalised reality in which the user feels validated by the content, thereby lowering their cognitive resistance to the underlying hostile narrative. Individuals become trapped, whether unconsciously or consciously, in filter bubbles and ‘echo chambers’, and become victims of opinion manipulation, limiting their access to information.(Kertysova, 2018)

Traditional defensive architectures, such as independent fact-checkers and platform moderation tools, are optimised to detect factual anomalies. They are not equipped to monitor interpretive nuance. By relying on accurate facts and reframing, AI-driven campaigns operate in a vague area of content moderation that shapes the context while bypassing content removal. This results in a cognitive fracture that could jeopardise democracy through manipulation, rendering political consensus potentially impossible.

Scale and Epistemic Paralysis

The sole existence of generative technology provides state actors with a powerful shield of plausible deniability. In a grey zone context, this advantage allows aggressors to operate with impunity below the threshold of war. Historically, real video evidence has been probative evidence, capable of triggering international condemnation or sanctions. Today, the aggressor can dismiss such evidence as an AI-generated fabrication or a deepfake. This generates a self-reinforcing cycle of distrust within the international security architecture. Moreover, the state’s diminished capacity to authoritatively adjudicate fact from fiction renders democratic institutions structurally vulnerable to partisan weaponisation. (Whyte, 2020)

The cumulative effect of this dynamic is the emergence of a society with no trust. When a population is conditioned to believe that anything can be faked, they paradoxically cease to believe in anything. This suggests that the result is epistemic paralysis: the inability to discern and analyse information. Democratic governance relies on a shared baseline of reality to form consensus. The erosion of a common factual reality undermines the consensus necessary to withstand external influence and manipulation. For the grey zone actor, the primary measure of success shifts from

persuasion to epistemic degradation; the objective is to incapacitate the target population's truth-seeking mechanisms rather than to implant a specific narrative.

It can be argued that the strategic utility of epistemic paralysis lies in its weaponisation, drawing a direct parallel to the physiological fight-flight-freeze survival mechanism. By saturating the information environment with high-fidelity, machine-speed synthetic content, adversaries adopt a deliberate posture to exhaust the defender's analytical capacity. The risk is that the target population ceases to seek objective truth, thereby allowing the aggressor to gain potential decision dominance.

Cost and Economic Asymmetry

Ultimately, the integration of GenAI into influence operations represents a shift from a doctrine of persuasion to a cost-imposition strategy. While scale, speed, and realism define the characteristics of synthetic content, the strategic effect of GenAI functions is equalising, deriving from reduced production costs. The decisive factor is not the sophistication of the narrative but the economic asymmetry between the attacker and the defender, as we are currently witnessing on modern battlefields with homemade drones.

By reducing the cost of propaganda, adversaries can shift from episodic campaigns to industrial-scale aggression, as seen in the Shadow Play network. The $115,000 spent on Facebook advertisements in Operation Doppelgänger achieved a reach and engagement that would have probably required millions in traditional media buys or manual coordination.

The transition from human-operated troll farms to automated generation has reduced the production cost of high-quality disinformation by orders of magnitude. In contrast, the defender's response remains bound to the highly paid intelligence analysts, legal teams, crisis communication experts, and manual fact-checkers: time-consuming, costly, and quickly depletable. This disparity creates a significant asymmetry in the costs to be sustained.

I argue that the strategic goal of this behaviour could be to saturate the defender's attention and deplete their institutional resilience. GenAI turns disinformation into a tool of economic attrition, weaponising the defender's own need for truth against them.

Countering AI-generated Disinformation

The preceding sections have established that GenAI amplifies disinformation through speed, realism, and scale, while reducing production costs. The question that follows is whether existing defensive architectures are adequate to the challenge. This section examines three layers of response: technical detection, legislative regulation, and cognitive resilience.

The immediate defensive response to GenAI disinformation has been the deployment of detection technologies to analyse digital artefacts that might highlight traces of GenAI. Major technology companies have invested significantly in this domain: Google's SynthID embeds imperceptible watermarks in AI-generated content, Microsoft's Content Integrity tools provide provenance verification, and the Coalition for Content Provenance and Authenticity (C2PA) has developed an open standard for attaching cryptographic credentials to media files, enabling viewers to trace an image or video back to its point of capture or creation. However, each of these approaches confronts structural limitations, and since GenAI relies on GANs, this method is, by default, ineffective in the long run because GANs are designed to bypass detection iteratively. The technical defence is therefore structurally unable to achieve a durable advantage. Furthermore, this research has highlighted that one of the critical challenges today is not finding a technical solution to identify synthetic content, but dismantling the influence effect generated by disinformation, which persists even after the content has been uncovered and labelled as fabricated.

Legislative frameworks, such as the European Union's Digital Services Act (DSA) and the AI Act, represent significant attempts to regulate the information space. However, the operational analysis of Operation Doppelgänger reveals a structural vulnerability in this approach: its slow speed. The timeline for identifying a threat, drafting a regulation, and enforcing compliance is measured in years. In contrast, the OODA loop of GenAI is measured in milliseconds. Adversaries actively exploit this latency through

the dissemination engine. The NATO StratCom COE's analysis of Russian operations confirms that while the DSA provides mechanisms for taking down disinformation networks, the procedural requirement from noticing the event to its contrast is too slow to stop a viral cascade.

Given the technical and legislative limitations, the ultimate line of defence is the cognitive sovereignty of societies. Resilience should not be achieved through protection from AI, but through exposure to it. Citizens should be trained to use generative tools and understand how they work, rather than treating them as black boxes, and to use critical thinking. The analysis in this paper advocates to a transition from societies as passive consumers of media to active auditors of content as a defence mechanism against GenAI disinformation. By training users to understand the mechanisms of hallucination or artifacting, they are less likely to anthropomorphise the machine or blindly trust its output. A fluent user develops an intuitive sense for the texture of synthetic text and the gloss of AI imagery. The current asymmetry of verification exists because the tools for detection are localised within specialised state agencies or large technology firms. By developing a system that empowers users to conduct initial verification and allows direct signalling of potential IMSs faster than a centralised bureaucracy could, the inherent latency of the current debunking system could be reduced.

By fostering bottom-up cognitive immunity, democratic societies can reduce the aggressor's strategic advantage while protecting democracy's values. If the target population treats all digital content with a baseline of technical scepticism, out of a sense of understanding, the adversary's influence strategy could be rendered less effective if not countered.

Conclusion

This research has evaluated the shift in disinformation campaigns enabled by the advent of GenAI within grey zone operations. By deconstructing the transition from human-intensive troll farms to automated, industrial-scale aggression, the analysis identified three primary variables and a fourth overarching one that have fundamentally altered the information environment. Through the examination of Operation

Doppelgänger and the Shadow Play network, it was highlighted that these technological force multipliers do not only aim to deceive but to systematically induce epistemic paralysis and disrupt the decision-making cycles of democratic institutions.

The research question regarding the impact of GenAI on the effectiveness of these campaigns has been addressed by highlighting the emergence of an asymmetry of verification. Generative models enable adversaries to saturate the information environment with high-fidelity, deceptive information at low implementation cost, forcing defenders into a permanent state of forensic reaction that depletes institutional resources. Ultimately, the strategic measure of success in the grey zone has shifted from influencing or persuading an audience to potentially the degradation of truth-seeking mechanisms, weaponising the openness of Western democracies to erode the baseline of trust required for collective defence.

Several limitations constrain the scope and generalisability of this research. First, the analysis rests on two micro-case studies; hence, they cannot be representative of the full spectrum of state-sponsored AI-enabled disinformation. Operations conducted by Iran, North Korea, or non-state actors may follow significantly different patterns. Second, the reliance on open-source forensic reports, while methodologically transparent, excludes the classified intelligence that would provide a more complete operational picture. Third, this research has focused exclusively on the targeting of Western democratic audiences; the dynamics of AI-driven disinformation in non-democratic information environments or in the Global South remain unexamined.

The implications of this shift suggest that the primary threat in the coming decade will be the further development and exploitation of algorithmic reframing, using AI to leverage emotional and ideological interpretations of true events and further exploit biases. Future research should focus on the long-term depletion of human cognitive resilience in environments dominated by synthetic media. As the boundary between the authentic and the synthetic continues to blur, the survival of democratic governance will depend less on the hardening of digital borders and more on cultivating a cognitively immune society capable of maintaining intellectual sovereignty in a world of manufactured consensus. Further research is required to understand how to strengthen this resilience.

Perhaps the most significant danger lies in the domestic application of these tools and could be expanded as a future research direction. The same mechanisms used in foreign interference (micro-targeting, linguistic mirroring, and manufactured consensus) can be exploited by domestic actors as well. There is a growing risk that state leaders will utilise propagandistic AI campaigns to lure citizens into supporting their electoral campaigns. When these tools are used to manufacture a false mandate, the distinction between a healthy democracy and an autocracy in disguise blurs.

Bibliography

Beauchamp-Mustafaga, Nathan, Green, Kieran, Marcellino, William, Lilly, Sale and Smith, Jackson. 2024. *How China Learned to Stop Worrying and Love Social Media Manipulation: Insights into Chinese Use of Generative AI and Social Bots from the Career of a PLA Researcher.* RAND Corporation. [Online]. 1 October 2024. [Cited: 18 January 2026]. https://www.rand.org/pubs/research_reports/RRA2679-1.html

Bontridder, Noémi and Poullet, Yves. 2021. The role of artificial intelligence in disinformation. *Data & Policy*. 2021. Vol. 3, pp. e32. DOI 10.1017/dap.2021.20.

EU DisinfoLab, CheckFirst, Viginum, Cassini, the Auswärtiges Amt, the European External Action Service (EEAS), the DFR Lab. 2026. Building a common operational picture of FIMI, using IMS to strengthen technical attribution and disruption. 16 January 2026. [Online]. [Cited: 14 March 2026]. https://www.disinfo.eu/building-a-common-operational-picture-of-fimi

Hsu, Tiffany. 2023. Interview about misinformation and AI. Distrust of Everything: Misinformation and AI. Center for Strategic & International Studies, 18 July 2023. [Online]. [Cited: 28 November 2025]. https://www.csis.org/analysis/distrust-everything-misinformation-and-ai

Braw, Elisabeth. 2023. AI and Gray-Zone Aggression: Risks and Opportunities. *American Enterprise Institute - AEI*. [Online]. July 2023. [Cited: 27 September 2025]. https://www.aei.org/research-products/report/ai-and-gray-zone-aggression-risks-and-opportunities/

Keast, Jacinta. 2023. *Shadow Play: A pro-China technology and anti-US influence operation thrives on YouTube* [Online]. [Cited: 18 January 2026]. https://www.aspi.org.au/report/shadow-play/

Kertysova, Katarina. 2018. *Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation is Produced, Disseminated, and Can Be Countered. Security and Human Rights*. 12 December 2018. Vol. 29, no. 1–4, pp. 55–81. DOI 10.1163/18750230-02901005.

Sedova, Katerina, McNeill, Christine, Johnson, Aurora, Joshi, Aditi and Wulkan, Ido. 2021a. *AI and the Future of Disinformation Campaigns Part 1: The RICHDATA Framework* [Online]. Center for Security and Emerging Technology. [Cited: 28 November 2025]. https://cset.georgetown.edu/publication/ai-and-the-future-of-disinformation-campaigns/

Sedova, Katerina, McNeill, Christine, Johnson, Aurora, Joshi, Aditi and Wulkan, Ido. 2021b. *AI and the Future of Disinformation Campaigns Part 2: A Threat Model* [Online]. Center for Security and Emerging Technology. [Cited: 29 November 2025]. https://cset.georgetown.edu/publication/ai-and-the-future-of-disinformation-campaigns-2/

Stockwell, Sam, Hughes, Megan, Swatton, Phil, Zhang, Albert, Hall, Jonathan, Kieran. 2024. AI-Enabled Influence Operations: Safeguarding Future Elections. *CETaS Research Reports*. [Online]. November 2024. [Cited: 18 January 2026]. https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-safeguarding-future-elections

Taeihagh, Araz. 2025. Governance of Generative AI. *Policy and Society*. 4 January 2025. Vol. 44, no. 1, pp. 1–22. DOI 10.1093/polsoc/puaf001.

Sessa, Giovanna, Raquel, Miguel. 2024. *The Doppelganger case - Assessment of Platform Regulation on the EU Disinformation Environment*, 2024. Riga [Latvia]: NATO Strategic Communications Centre of Excellence. ISBN 978-9934-619-64-9.

Wardle, Clare and Derakhshan, Hossein. 2017. *Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe* [Online]. Council of Europe. [Cited: 8 March 2026]. https://firstdraftnews.org/glossary-items/pdf-wardle-c-derakshan-h-2017-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making-council-of-europe/

Watson, Nell. 2024. *Taming the Machine: Ethically Harness the Power of AI*. 1st ed. London: Kogan Page, Limited. ISBN 978-1-398-61432-1.

Whyte, Christopher. 2020. *Deepfake news: AI-enabled disinformation as a multi-level public policy challenge.* Journal of Cyber Policy. 3 May 2020. Vol. 5, no. 2, pp. 199–217. DOI 10.1080/23738871.2020.1797135.

MAJ David THOMPSON: How to Pursue Rare Earth Elements in Greenland to Advance U.S. National Security Interests without Alienating Allies if Greenland Declares Independence?

Supervisor: Dr. George Spencer TERRY

Statement on the Use of Artificial Intelligence (AI) Tools:

Tools: *Perplexity, ChatGPT, Copilot, and Notebook Large Language Models were used in the creation of this document.*

Purpose: *AI tools were used to improve author-developed content, including the paper outline and written content, by recommending edits. AI tools were also used to summarise research material, search the author's curated research library, and cross-check other AI tool responses.*

Process: *The above-mentioned AI tools were used in an iterative process starting after the author defined the research topic, question, and thesis (The strategic significance of Greenland's rare earth elements to the U.S.) from 11 August 2025 to 14 March 2026. First, AI tools were used to assess the feasibility of the proposed topic by identifying relevant literature and potential cases to research. Then, the author generated the body of the content. Then, guided AI to enhance the work. When using AI, the author defined the roles, tasks, and functions of AI assistants. Then, the author built an initial source library of research material and writing guidance for AI to reference. After leveraging the author's subject-matter expertise, the author guided AI through an iterative process of prompting, reviewing, narrowing, and verifying AI output to increase the efficiency of the research and writing process. Finally, the Author conducted the*

critical thinking, judgment, and writing of the research. AI processed large amounts of information and offered assessments when asked.

Ownership: *The Author used their knowledge to generate the research topic, identified the primary reference material, curated the reference library, wrote the content, generated the prompts to guide AI, conducted the analysis of cases, edited all content, and verified all content. Therefore, the author takes full ownership of this research paper.*

1. Introduction

Modern life is dependent on a stable supply of rare earth elements (REE). The United States (U.S.) depends on its primary rival, China, for this critical raw material. The Chinese Communist Party (CCP) can use this dependence to disrupt the U.S. economy and military.

China has a near-monopoly over the REE supply chain and could restrict exports to the U.S. and Europe. Rare earth elements are critical building blocks of modern life and are used across industries (GSEU, 2024, p. 1). They are fundamental to defence, aerospace, medical, automotive, renewable energy, and most future electronic technology, including AI. The Chinese Communist Party has threatened and limited the supply of REE as a coercive tactic. For example, multiple sources reported that China stopped shipments to Japan in 2010 over territorial disputes (Evenett, Fritz, 2023, pp. 68–69; Sutter, 2019; Select Committee, 2023, p. 3,43-47). In 2025, China implemented export controls on REE to the U.S. in response to U.S. tariffs on Chinese exports (Perera, 2025; Baskaran, Schwartz, 2025a). During a visit to a Rare Earth Element Magnet (REEM) facility in Jiangxi province in 2019, Chinese President Xi Jinping publicly stated that, ‘(In) waging a trade war against China, the United States risks losing the supply of materials that are vital to sustaining its technological strength’ (Sutter, 2019). In the great power competition, China will likely restrict or limit the export of REE to coerce the U.S. from intervening in a Chinese invasion of Taiwan or actions in the Arctic.

Because of this rare earth element vulnerability, Greenland has become strategically significant to the U.S. Geographical surveys indicate that Greenland has some of the largest undeveloped rare earth reserves on the planet, and it could become a fully independent country from Denmark. The U.S. has one significant rare earth mine and insufficient processing capacity to meet demand. Therefore, the U.S. must import 90% of REE, making it dependent on China (Cordier, 2024). To mitigate this risk, the U.S. is focused on securing a REE supply chain as a matter of national security, and Greenland is an attractive option for three reasons. First, REE are abundant. Second,

its location in the Arctic is strategically significant. Third, U.S. control of Greenland denies China the opportunity to expand its REE monopoly or influence in the Arctic.

How to pursue rare earth elements in Greenland to advance U.S. national security interests without alienating allies if Greenland declares independence? The United States uses an indirect, soft-power approach with an independent Greenland to improve national security by strengthening the U.S. and EU rare earth supply chains and denying Chinese influence. China imposed export controls on REE to the U.S. in response to the Trump Administration’s tariffs in 2025, exposing this national security vulnerability (Perera, 2025). Thus, a secure rare earth supply chain is critical to the U.S., and Greenland's rare earth reserves are strategically significant because the U.S. requires an external source of REE independent of China to reduce China’s influence on the U.S. economy and military. First, this research paper analyses the strategic significance of REE. Second, this paper analyses soft, hard, and smart power options for the U.S. to pursue developing a secure REE supply chain in Greenland through a comparative case study. Finally, it makes a recommendation and discusses potential associated risks.

2. Methodology

This research employs a qualitative approach due to the complexity of international security policy, which is influenced by multiple variables and human subjectivity. A comparative case study, across cases and time, is the qualitative method utilised to analyse policy options using historical cases with similar subjects: strategically significant geography, critical resources, and great power competition. The comparative case studies are:

1. U.S. relations with Saudi Arabia to access oil from 1930 to the present.
2. U.S. relations with Iran to secure oil through Operation AJAX.

These cases are viewed through the concepts of soft, hard, and smart power to analyse stakeholder actions and outcomes.

2.1 Analytical Framework

This paper utilises international relations concepts of Hard Power, Soft Power, and Smart Power to analyse how the U.S. has approached securing critical raw materials

and the outcomes from those approaches. The outcomes of cases are compared to inform how the U.S. should approach securing rare earth elements in Greenland. Rather than testing these concepts, this paper uses case studies to illustrate their effectiveness within the limits of these cases.

Hard Power

Hard power focuses on employing instruments of national power to force, coerce, or induce others. In this paper, the instruments of national power are Diplomacy, Information, Military, and Economics (DIME). Some means of employing hard power are tariffs, military force, the threat of military force, economic sanctions, diplomatic sanctions, extraditions, and payments. The defining characteristics are immediately actionable, prioritised short-term gains over long-term losses, observable, and/or transactional (Nye, 2004, pp. 1–10). Operation AJAX, the clandestine U.S. operation in Iran, is a case in this research that illustrates the application of hard power to secure a critical raw material, oil.

Soft Power

Soft power utilises attraction or persuasion through the employment of the instruments of national power and society, including culture, to achieve outcomes; this attraction or persuasion develops through alignment of internal motivation with the other party(s). Means of employing soft power include, but are not limited to, military humanitarian operations, institutional values, adherence to values and norms through diplomacy, perceived fair economic policy, and exchange programs. Examples of U.S. soft power include the history of peaceful transfer of power, technological advances, the public education system, and successful higher education systems. The characteristics of soft power are generally indirect, delayed effects, less quantitative or measurable, sustainable, and enduring (Nye, 2004, pp. x–xiii, 1–10). The case used to illustrate soft power is the U.S and Saudi Oil development. The U.S. Marshall Plan in Europe after World War II and the E.U. enlargement are also examples of soft power but are not used as cases in this work.

Smart Power

Smart power is the optimal combination of hard and soft power. The optimal integration of hard and soft power resources is situation-dependent, but not always an option.

Means include projecting military power through multilateral exercises, combined with cooperative economic development programs established through enduring diplomatic actions, or economic sanctions coordinated with allies that support the rules-based world order (Armitage, Nye, 2007, pp. 7–9).

Additionally, this paper examines the direct or indirect application of hard, soft, or smart power. In this analysis, ‘direct’ means that a nation's government employs instruments of national power directly toward the intended nation, organisation, non-state actor, or population without an intermediary. Conversely, ‘indirect’ means that a nation employs instruments of national power through a third-party national government, organisation, non-state actor, or population. Hard power is typically direct, while soft power is typically indirect (Nye, 2004; 2023). However, this is not always true. For example, Hard military power is being applied indirectly against Russia in the Russo-Ukraine War by the U.S. and EU through training, advising, and funding programs to support Ukraine.

2.2 Case Selection Criteria

Cases were selected based on three criteria: the subject nation was a major power[2], the critical raw material was a variable, and there was competition between nations for the critical raw material. Major powers include the U.S. after 1900, England in 1700-1800, China after 1990, and the Soviet Union 1940-1991. Major power status is desired to be more comparable with future U.S. engagement with Greenland regarding REE. The existence of critical raw materials is desired in the cases to be comparable to Greenlandic REE because they are critical raw materials and a variable in the current U.S.-China great power competition. Finally, competition is included to provide the county with critical alternative raw material options. Greenland has multiple options, and the competition between the U.S. and China has arguably given it more options, as Denmark and the EU feel obligated to offer counteroffers. Prior to any competition, there was less incentive for Denmark and the EU to allocate more resources to Greenland.

[2] The subject nation is the nation seeking the critical resource from another nation. For example, the U.S. is the subject nations seeking oil from another nation, the Kingdom of Saudi Arabia, in the first case.

2.3 Justification and limitations

This qualitative and theory-informed approach is appropriate for two reasons. First, the research question is strategic and forward-looking; it attempts to identify the optimal international policy option for a hypothetical future scenario, an independent Greenland. Second, there is no objective means to measure an observable outcome. Therefore, qualitative methods, grounded in theory, are the best option for exploring such scenarios. Soft, hard, and smart power are the theoretical frameworks employed to exercise theoretical knowledge.

The limitation of the research is the reliance on publicly available sources; classified assessments of Greenland's resources or great power competition are beyond its scope. Additionally, this research cannot fully account for differences in selected cases (Saudi Arabia and Iran) and Greenland, including indigenous rights, environmental concerns, leadership personalities, and domestic politics, that affect strategic policy. These limitations are minimised through explicit assumptions, multiple sources where possible, and by focusing on policy options available to leaders in the case studies and to leaders now.

3. Strategic Importance of Rare Earth Elements

Rare earth elements are critical raw materials for several strategic industries: defence, aerospace, automotive, renewable energy, and advanced electronic technology, including Artificial Intelligence (AI). All branches of the U.S. military rely heavily on REE for current and next-generation systems. For example, the F-35 requires 900 pounds (408 kg) of REE. Every Arleigh Burke DDG-51 requires 5200 pounds (2359 kg), and the Virginia Class of submarines requires 9,200 pounds (4173 kg) (CRS, 2013, p. 4). The weapon systems and radars that these platforms carry also require REE: Joint Direct Attack Munition (JDAM) or 'smart bombs,' Tomahawk cruise missiles, Surface to Air missiles, Air to Air missiles, and radar systems like the Army's Patriot Air Defence system all require REE (Lopez, 2024). The manufacturing requirement of REE for these platforms and weapons systems means that a supply disruption would prevent the ability to replace them, causing operational and strategic effects for the U.S.

The 2022 and 2025 U.S. National Security Strategies prioritise military modernisation of advanced weapons systems, which further increases the U.S. demand for REE

(Biden, 2022, p. 8; Trump, 2025a, p. 3). For example, the U.S. Navy plans to order 364 manned 'battle force ships' over the next 30 years, from 2025 through 2054, to modernise the fleet (Labs, 2025). This does not include an unknown number of unmanned vessels. According to the plan, the construction of 23 Arleigh Burke DDG-51 and 28 Next Generation DDG(X) large surface combat ships will consume around 265,200 pounds (120 metric tons) of refined REE alloys or rare earth element magnets. Similarly, 542,800 pounds (246 metric tons) of REE and REEM are needed to construct the planned number of Virginia Class and Next Gen attack submarines. See figure 1. Public figures are not available for every ship in the Navy's modernisation plan, nor the DoD as a whole. However, a logical assessment is that U.S. military modernisation will increase U.S. demand for REE.

	2025 Plan	REE per Ship		REE per Type	
	Number of Ships	lbs	kg	lbs	m tons
Aircraft Carriers (with out aircraft)	6	10,120	4,590	60,720	28
Ballistic Missile Submarines	10	9,200	4,173	92,000	42
Large Payload Submarines	6	9,200	4,173	55,200	25
Attack Submarines (Virginia, Next Gen)	59	9,200	4,173	542,800	246
Large Surface Combantants (DDG -51, DDG-X)	51	5,200	2,359	265,200	120
Small Surface Combantants	81	2,600	1,179	210,600	96
Large and Midsize Amphibious Warfare Ships	25	2,600	1,179	65,000	29
Medium Landing Ships	55	520	236	28,600	13
Combat Igistics and Support Ships	71	520	236	36,920	17
Unmanned Surface and Subsurface Ships	unknown				
Total	364			1,357,040	616
Consumption Per year				45,235	21

Figure 1: Estimated Consumption of REE based on the U.S. Navy's Ship Modernisation Plan: Developed by the author (CRS, 2013; Labs, 2025; LaGrone, 2016; Lopez, 2024)

The increase in demand for rare earth elements in the defence industry will be greater for certain elements. There are 17 REE; each has a unique utility in modern technology. Neodymium Iron Boron (NdFeB) and Samarium-Cobalt (SmCo) are critical raw materials for manufacturing REEM, which retain magnetic properties at high temperatures. Therefore, they are used in radar systems, aircraft, and missiles (GAO, 2016, pp. 1-2,3-6; CRS, 2013, pp. 44–45). Because Neodymium Iron Boron and Samarium-Cobalt are irreplaceable in modern weapons systems, their supply chains are strategic chokepoints for the U.S. defence industry and U.S. national security. Greenland has essentially all the magnet-critical light and heavy rare earths:

neodymium, praseodymium, dysprosium, terbium and others, in addition to large volumes of more abundant REE (Baskaran, Schwartz, 2025b). Thus, Greenland's deposits are a potential solution to the U.S. defence vulnerability.

3.1 China's strategy

Decades ago, China recognised the strategic importance of rare earth elements and pursued a strategy to dominate the REE supply chain (Hearty, Alam, 2019). China's control of the REE supply creates a strategic vulnerability for the United States, the European Union, and NATO. China controls 90% of mine production, 85-95% of separation, and 97% of refined REE, including the REE magnet production (Select Committee, 2023; Baskaran, Schwartz, 2025b). The U.S.'s dependence on and China's control over supply enable the Chinese Communist Party to influence the U.S. and advance its goals. The CCP strategically subsidises Chinese companies to produce low-cost REE. This creates a competitive disadvantage to produce REE in the U.S. or EU (Kefferpütz, 2010; Select Committee, 2023). This competitive advantage led U.S. consumers to shift to Chinese suppliers, while U.S. producers closed facilities.

China's manipulation of the REE supply confirms that this dependency is a vulnerability and poses a risk to U.S. economic and defence interests. In 2010, China reportedly halted shipments of REE to Japan over disputed territory to secure national interests, causing production slowdowns and cost increases for REE-dependent industries (Waters, 2016, pp. 33–34). China implemented export restrictions on certain U.S. defence companies in 2025 (Baskaran, Schwartz, 2025a). Additionally, Russia's manipulation of energy supplies from Russia to Europe after the invasion of Ukraine further reinforces that adversaries are weaponising critical supply chains to achieve their objectives. Manipulation resulted in price surges in energy and contributed to inflation across multiple sectors of the European economy (Struk, 2024; Khudaykulova, Khudaykulova, Obrenovic, 2022). To avoid coercion and build resilient economies, the U.S. and Europe need to develop independent, secure supply chains, including REE supply chains.

3.2 U.S. REE Supply Chain Challenges

Recognising the threat posed by Chinese control of REE production, this sub-section explains why U.S. domestic efforts are insufficient to close the REE production gap.

The U.S. produces fewer rare earth materials than it consumes. The U.S. consumption of refined rare earth oxides (REO) and alloys is on the order of 6,000–10,000 metric tons annually. The U.S. imports 80-95% of its refined rare earth materials and rare earth magnets; 70% of these imports are from China. The Mountain Pass mine, owned by MP Materials, is the only significant producer of REO in the U.S., averaging 40,000 metric tons of unprocessed REO per year from 2019-2024 (Cordier, 2024, pp. 144–145; 2025, pp. 144–145). The U.S. exports most of its domestic rare earth production due to a lack of processing capacity. According to the USGS, 43,000 tons of the 45,000 tons of rare earth ore produced in 2024 were exported (Cordier, 2025, p. 144). Most of the ore is exported to China for processing and magnet manufacturing. Thus, the U.S. needs to develop domestically and allied REE reserves, independent of Chinese influence, to secure a REE supply chain.

Unfortunately, developing an integrated REE supply chain takes decades. The U.S. Government acknowledged this vulnerability in 2010 and invested $400 million in a domestic REEM supply chain in 2022 to meet the defence industry requirements by 2027 (Lopez, 2024; Waters, 2016, pp. 33–34). However, this goal may not be achievable. First, current MP mine production only supports 1000 m-tons of NeFeBn magnets. Second, U.S. domestic Heavy Earth Element (HEE) processing is in the pilot phase and not ready for production at scale (Baskaran, Schwartz, 2025a). This suggests that increasing domestic capacity takes 5 or more years and millions to billions of dollars. Additionally, the U.S. has limited economically viable REE deposits outside the MP mine. Therefore, the U.S. is seeking alternative mining, separating, and refining capability in Greenland as an option to speed REE production.

4. Greenland’s Strategic Importance

Greenland is strategically relevant for multiple reasons: access to the Arctic, location between the U.S. and Europe, and critical raw materials. For this paper, Greenland’s rare earth element deposits are the central analytical element of U.S. policy toward Greenland. Greenland is a self-governing territory of Denmark. In the last decade, the possibility of Greenland voting to declare independence has become more probable. A poll conducted in January 2025 indicated that 85% of eligible voters want independence, but the desire varies with the level of consequences (Marx, 2025). Thus, potential U.S. interests with an independent Greenland are relevant because it’s

probable that Greenland declares independence; Greenland has significant REE deposits; the U.S. needs external sources of rare earths; the U.S. will attempt to deny China to Greenland's REE; the U.S. will engage Greenland prior to independence to shape international agreements; and the U.S. has historical and continued interest in Greenland.

5. Case Study Analysis

This section analyses U.S. hard, soft, and smart power approaches to securing critical raw materials in Saudi Arabia and Iran to identify an optimal approach with Greenland. Similarly, Saudi Arabia and Iran were both young nations with critical raw materials seeking support like a potentially independent Greenland. There are two differences. First, Saudi Arabia was a hereditary monarchy, unlike Iran in the past and Greenland today, which are democracies. Second, public opinion of the U.S. in Saudi Arabia and Iran was positive, whereas Greenlanders now have a more sceptical view of the U.S.

5.1 Case: U.S. relations with Saudi Arabia to access oil.

Justification

The U.S. and Kingdom of Saudi Arabia relationship is an example of how the U.S. has employed national instruments of power directly to secure access to critical raw materials, oil, deemed necessary for national security. In accordance with the case study selection criteria, first, the U.S. was a major power after World War I. Second, oil was the emerging critical raw material. Economies and industries were undergoing a paradigm shift from coal to oil, similar to the strategic emergence of REE today. Third, the U.S., the World, and later the Soviet Union were all competing to secure oil. In line with the case study typology, the subject is the U.S. employment of instruments of national power with the Kingdom of Saudi Arabia to secure stable oil supplies for the U.S. The object is the direct or indirect application of soft, hard, and/or smart power through diplomatic, informational, military and economic instruments.

Analysis

The United States applied soft power both directly and indirectly in its international relations with Saudi Arabia. The overall categorisation is indirect soft power because the principal mechanism for securing oil was the U.S. Petroleum Industry and the Arabian American Oil Company (ARAMCO). Direct U.S. diplomacy, such as the 1945

U.S. Quincy Agreement, supported the 1933 Concession Agreement between Standard Oil of California (SOCAL) and the King. The creation of ARAMCO also allowed U.S. workers to influence Saudi Arabia through culture and education. Saudi Arabia could have aligned with the British, who had historically operated and controlled the region, but instead chose the U.S. initially by agreeing to let SOCAL explore for oil, arguably demonstrating the effect of previously executed U.S. soft power around the world. However, the defining U.S. action was the U.S. Treasury approving the ARAMCO foreign tax credit that enabled Saudi Arabia to be an equal beneficiary of its nation's natural resources. This legitimised the U.S. and probably prevented a hard-power conflict over Saudi Arabia's nationalisation of ARAMCO, as demonstrated by Iran's nationalisation of the Anglo-Iranian Oil Company and the subsequent conflict in Iran.

Outcome

The United States achieved reliable access to Saudi oil while fostering political goodwill and regime stability then and into the future. First, this is demonstrated by ongoing positive U.S. and Saudi relations. Second, access was enduring, laying the foundation for ARAMCO's growth. Third, the costs were minimal and largely limited to foregone opportunities for tighter political control. The U.S. accepted a short-term $44 million tax reduction, which minimised the risk of long-term loss of ARAMCO tax revenue if the company was nationalised. This case demonstrates that indirect soft power alone can be sufficient to secure access to and benefits from critical raw material development in a permissive environment where interests are aligned. Relative to Greenland, this implies that indirect soft power via U.S. companies can secure a durable rare earth supply because Greenland is looking for technical and investment partners to develop its national resources and is a historic partner with the U.S.

5.2 Case: U.S. relations with Iran to access oil around 1953

Justification

The U.S.-led Operation AJAX to overthrow Iranian Prime Minister Mohammad Mosaddeq in August 1953 exemplifies how major powers employ instruments of national power directly to secure access to critical raw materials deemed necessary for national security. In accordance with the case study selection criteria, first, the United States and the United Kingdom (U.K.) were both major powers during the early

Cold War period. The U.S. had emerged from World War II as a global superpower with unparalleled economic and military capabilities. Britain, despite post-war decline, maintained significant imperial influence and extensive overseas economic interests. Second, Iranian oil was a strategic critical raw material. The U.S. government determined that Iran's production was critical not only for British energy requirements but also for sustaining the broader Western alliance structure and global capitalist economy as the Cold War intensified. Third, multiple nations competed for access to Iranian oil resources.

The United Kingdom sought to preserve the Anglo-Iranian Oil Company's (AIOC) monopoly over Iranian production. The U.S. sought expanded access for American oil companies and regional stable oil production. The Soviet Union served as the third counter competitor (Rahnema, 2013, pp. 12–14, 289–294). In line with the case study typology, the subject is the U.S. employment of instruments of national power to secure Iranian oil for the U.K. and the broader global market. The object is the analytical framework of soft, hard, and smart power applied through all four DIME instruments. In this case, the specific mechanisms of DIME are diplomatic deception, information warfare, covert military operations, and economic sanctions, to coerce and then ultimately overthrow Iran’s nationalist government to secure critical resources.

Analysis

During Operation AJAX, the U.S. employed hard power directly on Iran and specifically the Mossedaq government. As a primary instrument, the Eisenhower Administration directly employed military power by pursuing regime change, planning and conducting a coup d’état. A Central Intelligence Agency (CIA) agent worked directly with the Iranian opposition, not through external organisations or states. Other instruments supported this principal instrument of direct military power. This case illustrates the employment of direct hard power. First, the covert nature of the operation enabled U.S. Informational power that was employed directly in Iran and indirectly in the international community to mitigate damage to U.S. legitimacy. The information was intended to coerce or deceive because it was hypocritical to American Ideals. Second, U.S. diplomatic support for the Shah as Mossedaq’s successor was transactional. The implicit deal required the Shah to denationalise AIOC, allowing British and American oil companies to regain control. Third, U.S. and British economic sanctions against

Iranian oil sales were intended to weaken and coerce Mosaddeq and the Iranian Parliament (Majlis). In summary, this is a clear example of direct hard power.

Outcome

Context is important to understanding the Outcome of Operation AJAX. Before, the U.S. held a unique status in international relations due to its ideology and historical record. Woodrow Wilson's principle of self-determination and the U.S. contribution to free Europe in the two World Wars from authoritarian powers stood in contrast to European Imperialism and the emerging Soviet authoritarian power. Iranians were altruistically drawn to America as a potential ally to balance against European colonial powers due to the perceived lack of U.S. territorial ambitions during decolonisation (Wright, 2021). Mosaddeq sought to align himself with the U.S. by visiting Truman and Eisenhower, voicing his agreement with American values and requesting economic assistance amid British sanctions. Simply, the U.S. held an advantageous position.

As a result of Operation AJAX, the U.S. countered Soviet influence in Iran and obtained access for American Oil companies to Iranian oil in the short to medium term (26 years). In this case, there were two long-term costs of employing direct hard power. First, the U.S. relinquished influence in Iran to the Soviet Union (now Russia) and China, beginning in 1979 and continuing to the present. More relevant to the subject, the U.S. and the U.K. lost long-term access to and revenue from Iranian oil; those resources were sold to competitors at a discount.

The tragic paradox is that Mosaddeq was genuinely attracted to American democratic principles, representing the positive effect of previous U.S. soft power in Iran, but the Eisenhower administration rejected the opportunity to partner with Mosaddeq under suspicion of his susceptibility to communist influence. The administration decided to overthrow the democracy and establish an authoritarian client state, which degraded U.S. legitimacy. The Iranian people were excluded from benefiting from their country's natural resources; the Shah remained the primary Iranian beneficiary. Because the Shah wasn't the legitimate leader, he utilised the secret police (SAVAK) to violently suppress domestic opposition. Despite the covert nature, Iranians largely attribute the coup to the U.S., which gave rise to anti-American sentiment that ultimately exploded in the 1979 revolution and hostage crisis. In the long term, the U.S. lost influence in

Iran to the Soviet Union (now Russia) and China. The costs of Operation AJAX are still being felt. The 911 attacks, the Afghanistan War, the Iraq War, and the continued instability in the Middle East are logical residual effects of Operation AJAX (Kilcullen, 2016). This case reveals that short-term resource security achieved through direct hard power intervention can destroy the very soft power that initially provided influence, ultimately destabilising the access it sought to secure. This implies that U.S. employment of hard power on a friendly, independent Greenland could undermine soft power options and push Greenland toward competitors like China or Russia.

6. Case Study Comparison

The case comparison reveals four findings. First, the application of direct hard power can secure critical resources in the short-term but will likely result in long-term consequences or costs that negate the short-term gain. The U.S. secured access to Oil in Iran by employing direct hard power in its relations with the Iranian government. Second, the degree of resulting costs also correlates to whether the application of power is within international and national accepted norms. With respect to Iran, Operation AJAX was counter to the U.S. ideals of self-determination and democracy, and the Iranian public opinion shifted from pro-American to anti-American.

Third, the second and tertiary-level consequences of hard power are likely not fully understood and difficult to predict. In the case of Iran, U.S. support for an illegitimate authoritarian leader created conditions for a chaotic future transfer of power; Khomeini replaced the Shah during a popular uprising, turning Iran into a long-term U.S. adversary. Fourth, the international environment can mitigate hard power costs and/or enable soft power. Countries not directly affected may still view the aggressor as a legitimate or viable partner relative to worse alternatives. For example, Saudi Arabia continued its relationship with the U.S. after Operation AJAX. Compared with former European imperialist powers or the Soviet Union, the U.S. remained a viable partner for Saudi Arabia. Regarding soft power, it will likely succeed in securing critical raw materials in a favourable competitive environment. For example, the U.S. leveraged its positive image during decolonisation to wield indirect soft power through U.S. commercial entities. This led to a long-lasting mutually beneficial relationship between the U.S. and Saudi Arabia.

7. Recommendation

To make a policy recommendation, this paper limits argumentation about U.S. actions to gain access to REE in Greenland by setting two conditions. First, U.S. actions occur after Greenland declares independence. However, current U.S. foreign policy actions are considered because the international environment preceding a referendum on independence influences the political will to pursue independence, and the international agreements made post-independence. For example, Greenland may not declare independence without security or economic assurances from Denmark, the U.S., or the EU.

Second, the U.S. must act in a manner that doesn't damage relations with allies; how the U.S. pursues REE in Greenland matters because the benefits of a secure supply must outweigh the costs to U.S. legitimacy, NATO cohesion, reserve currency status, and relations with Europe. During the paper's development, the Trump Administration alienated allies while unsuccessfully applying direct diplomatic hard power to secure U.S. interests in Greenland, including REE. Trump threatened tariffs and wouldn't rule out military action to gain U.S. control of Greenland (Trump, 2025b; Trump, 2026). The Administration's rhetoric and coercive tactics alienated European and Canadian leaders, prompting numerous officials, including Canadian Prime Minister Mark Carney and EU Vice President Kaja Kallas, to condemn U.S. actions as a threat to the rules-based international order (Carney, 2026; Kallas, Kaja, 2026). See Annex B for details on the Trump Administration's actions towards Greenland.

These statements signal potential European distrust and erosion of U.S. legitimacy. Polling in 2026 indicates that more Europeans now view the U.S. as a 'necessary partner', not an ally, and 34-61% view the U.S. as a threat (Zerka, 2025; Smith, 2026). However, this thesis remains relevant because transatlantic alliances are likely to rebound post-Trump, and U.S. interest in Greenland will remain. Polls show European public opinion of the U.S. rebounding after the first Trump administration (Smith, 2026). Historically, the U.S. has sought to control Greenland, attempting to purchase it in 1867, 1946, and 1955. The Trump Administration's foreign policy is a continuation of this historical interest. Therefore, if U.S.-EU relations are repaired, this recommendation will remain relevant.

Given these two conditions and the case analysis, the best approach is for the U.S. to pursue an indirect, soft-power strategy to develop a rare-earth element supply chain in Greenland. The U.S. government should encourage U.S. companies to lead the development of Greenland's rare earth resources. Similar to how ARAMCO's cooperative structure benefited both Saudi Arabia and the U.S., all parties can benefit. Greenland benefits from co-ownership, increased tax revenue, employment, and economic growth. U.S. companies would benefit from the profits generated. The U.S. government benefits from a REE supply chain that is independent of China.

8. Conclusion

In conclusion, this paper presents four key findings. First, because rare earth elements are an emerging critical raw material, control of the supply is a strategic priority for great power competitors. Secure REE supply reduces national vulnerability to external influence, and conversely, control enables influence over nations without independent supply. Under the grand strategy to regain standing as a great power, the Chinese Communist Party strategically developed a REE supply chain capable of supplying the global economy (Goldstein, 2020). Currently, 85-95% of the global REE supply comes from mining, processing, or refining in China. The U.S. and other nations were willing to depend on China because they could offshore the environmental costs and buy REE at artificially low prices (Kefferpütz, 2010, pp. 1–5; Baskaran, Schwartz, 2025c). However, this dependency enables Xi Jinping to restrict REE, disrupt economies, and limit military options of the U.S. and EU. This shapes the world for China's rise.

Second, U.S. and European geological surveys indicate that Greenland has significant undeveloped REE reserves with the potential to create an REE supply independent of China. Thus, the U.S. is interested in Greenland because it needs external sources. In addition to its REE, the U.S. is more attracted to Greenland than other locations because of Greenland's strategic geographic position in the Arctic and the competition with China for influence there. Finally, history shows that the U.S. has an enduring interest in Greenland. Actions from the Trump Administration are a continuation of this interest. ARAMCO and Operation AJAX shows that how the U.S. conducts international relations to access other nations' critical resources matter. Using hard power can potentially gain short-term access to critical raw materials, but there are high long-term costs. If the U.S. continues to break established norms by employing

hard power against Denmark or an independent Greenland, it risks degrading NATO, the United Nations, EU relations, and the U.S. dollar reserve currency status.

How to pursue rare earth elements in Greenland to advance U.S. national security interests without alienating allies if Greenland declares independence? The United States uses an indirect, soft-power approach with an independent Greenland to improve national security by strengthening the U.S. and EU rare earth supply chains and denying Chinese influence. The U.S.'s indirect soft power approach toward Saudi Arabia, through the creation of ARAMCO, provides a good example. The U.S. should proceed by empowering U.S. companies to partner with Greenland and develop a REE supply chain that benefits all parties. Greenland benefits from U.S. investment, technology, and the REE revenue. U.S. employment of diplomatic hard power by the first and second Trump Administrations caused allies to doubt U.S. intentions and commitments to NATO, limiting direct U.S. government DIME options in the short term. However, there is an opportunity for the U.S. government to make amends and, in the future, indirectly support U.S. companies and Greenland.

Bibliography

ARMITAGE, Richard and NYE, Joseph. 2007. *CSIS Commission on Smart Power: A smarter, more secure America*. Washington, D.C: Center for Strategic and International Studies. ISBN 978-0-89206-510-3.

BASKARAN, Gracelin and SCHWARTZ, Meredith. 2025a. The Consequences of China's New Rare Earths Export Restrictions. *Center for Strategic and International Studies (CSIS)*. [Online]. 14 April 2025. [Cited : 17 September 2025]. https://www.csis.org/analysis/consequences-chinas-new-rare-earths-export-restrictions.

BASKARAN, Gracelin and SCHWARTZ, Meredith. 2025b. Developing Rare Earth Processing Hubs: An Analytical Approach. *Center for Strategic and International Studies (CSIS).* [Online]. 28 July 2025. [Cited : 15 October 2025]. https://www.csis.org/analysis/developing-rare-earth-processing-hubs-analytical-approach.

BASKARAN, Gracelin and SCHWARTZ, Meredith. 2025c. Developing Rare Earth Processing Hubs: An Analytical Approach. *Center for Strategic and International Studies (CSIS).* [Online]. 28 July 2025. [Cited : 21 October 2025]. https://www.csis.org/analysis/developing-rare-earth-processing-hubs-analytical-approach.

BIDEN, Haris Administration. 2022. National Security Strategy. 12 October 2022. White House.

BULI, Nora. 2026. The exchange of messages between Norway's prime minister and President Trump. *Reuters.* [Online]. 19 January 2026. [Cited : 15 February 2026]. https://www.reuters.com/world/europe/exchange-messages-between-norways-prime-minister-president-trump-2026-01-19/.

CARNEY, Mark. 2026. Davos 2026: Special address by Mark Carney, PM of Canada. *World Economic Forum.* [Online]. 20 January 2026. [Cited : 27 January 2026]. https://www.weforum.org/stories/2026/01/davos-2026-special-address-by-mark-carney-prime-minister-of-canada/.

CORDIER, Daniel J. 2024. Mineral Commodity Summaries 2024. U.S. Geological Survey.

CORDIER, Daniel J. 2025. Mineral Commodity Summaries 2025. U.S. Geological Survey.

CRS. 2013. Rare Earth Elements in National Defense: Background, Oversight Issues, and Options for Congress. Washington, DC: Congressional Research Service. CRS Report.

EVENETT, Simon and FRITZ, Johannes. 2023. Revisiting the China–Japan Rare Earths dispute of 2010. *CEPR*. [Online]. 19 July 2023. [Cited : 26 October 2025]. https://cepr.org/voxeu/columns/revisiting-china-japan-rare-earths-dispute-2010.

GAO. 2016. Developing a Comprehensive Approach Could Help DOD Better Manage National Security Risks in the Supply. Washington, DC: GAO.

GASIOROWSKI, Mark and BYRNE, Malcolm. 2004. *Mohammad Mosaddeq and the 1953 Coup in Iran*. Syracuse, NY: Syracuse University Press.

GOLDSTEIN, Avery. 2020. China's Grand Strategy under Xi Jinping: Reassurance, Reform, and Resistance. *International Security*. 2020. Vol. 45, no. 1, pp. 164–201. DOI https://doi.org/10.1162/isec_a_00383.

GSEU. 2024. European Critical Raw Materials. [Online]. Brussels: Geological service for Europe. [Cited : 29 November 2025]. https://www.geologicalservice.eu/upload/content/1753/egs_gseu_all_crm_maps.pdf.

HEARTY, Grace and ALAM, Mayaz. 2019. Rare Earths: Next Element in the Trade War? [Online]. 20 August 2019. [Cited : 1 March 2026]. https://www.csis.org/analysis/rare-earths-next-element-trade-war.

KALLAS, Kaja. 2026. We want strong trans-Atlantic ties. But Europe needs to adapt to new realities. It is no longer Washington's primary centre of gravity. It's time for Europe to step up and act with urgency. We must strengthen our instruments, end fragmentation, close our gaps and join forces https://t.co/wnrmXOXCnB. Twitter. [Online]. 28 January 2026. [Cited : 15 February 2026]. https://x.com/kajakallas/status/2016504895071773024.

KALLAS, Kaja. 2026. Kaja Kallas (@kajakallas) / X. X (formerly Twitter). [Online]. 2 February 2026. [Cited : 15 February 2026]. https://x.com/kajakallas.

KEFFERPÜTZ, Roderick. 2010. Unearthing China's Rare Earths Strategy. *Centre for European Policy Studies (CEPS)*. [Online]. November 2010. [Cited : 16 October 2025]. DOI 10.2139/ssrn.1711320.

KHUDAYKULOVA, Madina, KHUDAYKULOVA, Akmal and OBRENOVIC, Bojan. 2022. Economic Consequences and Implications of the Ukraine-Russia War. *The International Journal of Management Science and Business Administration*. May 2022. Vol. 8, no. 4, pp. 44–52. DOI 10.18775/ijmsba.1849-5664-5419.2014.84.1005.

KILCULLEN, David. 2016. *Blood Year: The Unraveling of Western Counterterrorism.* 1st. New York, NY: Oxford University Press. ISBN 978-0-19-060054-9.

LABS, Eric J. 2025. An Analysis of the Navy's 2025 Shipbuilding Plan. *Congressional Budget Office*. [Online]. 6 January 2025. [Cited : 5 October 2025]. https://www.cbo.gov/publication/61155.

LAGRONE, Sam. 2016. Inside the Carrier Air Wing. *USNI News*. [Online]. 28 April 2016. [Cited : 5 October 2025]. https://news.usni.org/2016/04/28/the-basics-inside-the-carrier-air-wing.

LOPEZ, Todd C. 2024. DOD Looks to Establish "Mine-to-Magnet" Supply Chain for Rare Earth Materials. *U.S. Department of War*. [Online]. 11 March 2024. [Cited : 17 September 2025]. https://www.war.gov/News/News-Stories/Article/Article/3700059/dod-looks-to-establish-mine-to-magnet-supply-chain-for-rare-earth-materials/.

NYE, Joseph. 2004. *Soft Power: The means to Success in World Politics*. New York, NY: Public Affairs. ISBN 1-58648-225-4.

NYE, Joseph. 2023. *Soft Power and Great-Power Competition: Shifting Sands in the Balance of Power Between the United States and China.* Cambridge, MA: Springer. ISBN 978-981-9907-13-7.

PERERA, Ayeshea. 2025. Why China curbing rare earth exports is a huge blow to the US. *BBC.* [Online]. 17 April 2025. [Cited : 30 September 2025]. https://www.bbc.com/news/articles/c1drqeev36qo.

RAHNEMA, Ali. 2013. *Behind the 1953 Coup in Iran : Thugs, Turncoats, Soldiers, and Spooks.* Cambridge, England: Cambridge University Press. ISBN 978-1-107-07606-8.

SELECT COMMITTEE. 2023. Reset, Prevent, Build: A Strategy to Win America's Economic Competition with the Chinese Communist Party. 2023. U.S. Congress.

SMITH, Matthew. 2026. Many Europeans now see US as a threat to Europe. YouGov. [Online]. 13 February 2026. [Cited : 4 March 2026]. https://yougov.com/en-gb/articles/54102-many-europeans-now-see-us-as-a-threat-to-europe.

STRUK, Oleksandra. 2024. The Effect of the War on European Economy. In: The Economics of Russia's War in Ukraine: Impact Analysis of Economic Policy and Finance. In **Nataliya STRUK, Maryana PROKOP, Oleksandra STRUK**. *The Economics of Russia's War in Ukraine.* London: Routledge, pp. 52–95.

SUTTER, Karen. 2019. Trade Dispute with China and Rare Earth Elements. *Congressional Research Service*. [Online]. 28 June 2019. [Cited : 26 October 2025]. https://www.congress.gov/crs-product/IF11259.

TRUMP, Donald J. 2025a. National Security Strategy of the United States of America. [Online]. November 2025. The White House. [Cited : 4 March 2026].

TRUMP, Donald J. 2025b. Remarks by President Trump in Joint Address to Congress. U.S. Embassy & Consulates in Italy. [Online]. 7 March 2025. [Cited : 15 February 2026]. https://it.usembassy.gov/remarks-by-president-trump-in-joint-address-to-congress/.

TRUMP, Donald J. 2026. Davos 2026: Special Address by US President Donald J Trump. *World Economic Forum*. [Online]. 21 January 2026. [Cited : 27 January 2026]. https://www.weforum.org/stories/2026/01/davos-2026-special-address-donald-trump-president-united-states-america/.

VELA, Veronica. 2026. Europe stands firm against Trump's push for Greenland as he threatens new tariffs. *PBS News*. [Online]. 19 January 2026. [Cited : 15 February

2026]. https://www.pbs.org/newshour/show/europe-stands-firm-against-trumps-push-for-greenland-as-he-threatens-new-tariffs.

WATERS, Kristin. 2016. *Rare Earth Elements: Supply Chain Risk and National Defense Issues*. New York, NY: Chemistry Research Applications.

WRIGHT, David. 2021. *Oil Money: Middle East Petrodollars and the Transformation of US Empire, 1967–1988*. Ithaca, NY: Cornell University Press. ISBN 978-1-5017-1572-3.

YERGIN, Daniel. 1991. The Prize: The Epic Quest for Oil Money and Power. New York, NY: Simon & Schuster. ISBN 0-671-502248-4.

ZERKA, Pawel, PUGLIERIN, Jana, VARVELLI, Arturo. 2025. Transatlantic twilight: European public opinion and the long shadow of Trump. *European Council on Foreign Relations (ECFR)*. [Online]. 12 February 2025. [Cited : 4 March 2026]. https://ecfr.eu/publication/transatlantic-twilight-european-public-opinion-and-the-long-shadow-of-trump/.

Annex A: Case Background Information

Case Background: U.S. relations with Saudi Arabia to access oil.

U.S. and Saudi relations originated in the early 1930s through commercial oil exploration rather than formal government-to-government engagement. American firms, particularly Standard Oil of California (SOCAL), now Chevron, secured oil exploration rights through an agreement with King Abdulaziz ibn Saud. This 1933 concession agreement led to the discovery of oil and the formation of the Arabian American Oil Company, one of the most valuable companies today. Unlike European colonial models, U.S. engagement emphasised technical expertise, long-term investment, and respect for Saudi sovereignty, fostering elite legitimacy and domestic stability within the Kingdom. During World War II and the early Cold War, U.S. policymakers increasingly viewed Saudi oil as indispensable to global energy markets and Western security. The 1945 meeting between President Franklin D. Roosevelt and King Abdulaziz aboard the USS *Quincy* symbolised the informal strategic bargain that would define the relationship: U.S. access to oil in exchange for American security assurances and petroleum engineering knowledge and technology required to develop the newly formed Kingdom's valuable resource. Over time, this understanding expanded to include arms transfers, diplomatic protection, and coordination on oil production levels within OPEC.

The earliest phase of U.S. and Saudi relations emerged through indirect soft power through commercial engagement rather than formal direct government-to-government diplomacy. This period coincided with Saudi state formation, making oil development inseparable from regime consolidation. As an example of indirect Soft Power, American oil companies secured exploration concessions in 1933, and their technical and business expertise led to the creation of the Arabian American Oil Company (Aramco), which benefited all parties (Yergin, 1991). The U.S. Government benefited through tax revenue and access to oil. The Kingdom and American companies benefited from shared profits; however, the initial profit-sharing arrangement was skewed toward the U.S.

In 1950, the U.S government executed direct soft power through the 'Golden Gimmick,' a decision to follow U.S. tax law by approving a foreign tax credit. The mechanism enables Saudi Arabia to receive 50% of ARAMCO profits (Yergin, 1991) In 1950, the U.S. Treasury collected $50 million in taxes from ARAMCO, while Saudi Arabia received $66 million in royalties and taxes. In 1951, Saudi Arabia received $110 million in taxes and revenues, while U.S. tax collection shrank to $6 million (Gasiorowski, Byrne, 2004). An action that affirmed U.S. adherence to Saudi sovereignty and the rule of law at a time when European powers relied on colonial governance and coercive extraction. In summary, U.S. involvement during this phase emphasised contractual legitimacy, technical expertise, and respect for Saudi sovereignty, characteristic of soft power. Additionally, the U.S. diplomatic engagement remained deliberately limited, reinforcing the perception that American involvement posed no threat to political independence. Finally, Aramco's role extended beyond oil extraction to healthcare, education, environmental engineering, and workforce training, embedding U.S. influence socially and institutionally rather than coercively (Yergin, 1991; Wright, 2021). No military force or overt threats were employed to secure access. Again, this contrasted with the British threat of military force against Iran in disputes of the Anglo-Iranian Oil Company in 1951.

Case Background: U.S. relations with Iran to access oil around 1953

Since 1913, the British controlled the Anglo-Persian Oil Company and later the Anglo-Iranian Oil Company (AIOC), which maintained control of Iranian oil while extracting enormous profits, while Iran received only a fraction of the revenues. The British imperialist and colonial mindset viewed and treated Iranian resources with the understanding that the U.K. should be the primary benefactor. The company mistreated Iranian workers, subjecting them to inadequate housing, unsafe work conditions, low wages, and segregated facilities. If Iranian workers protested, the AIOC violently suppressed labour strikes. As a long-term strategy to maintain control, AIOC management barred Iranians from holding management positions, thereby preventing them from acquiring the necessary skills to manage or operate the company (Rahnema, 2013, pp. 35–41; Gasiorowski, Byrne, 2004; Wright, 2021, pp. 13–18). British actions contrasted with American actions. Namely, the U.S. Treasury agreement with ARAMCO that enabled Saudi Arabia to achieve a fifty-fifty share of company profits. Prior to this, the U.S. oil companies struck a fifty-fifty deal with

Venezuela and more equitable deals followed in Iraq and Kuwait. Yet Britain's AIOC ‘refused to adopt a fifty-fifty profit-sharing deal’ despite the U.S. provision of over $83 million in aid to stabilise Iran (Wright, 2021, pp. 16–17). The British controlled Iran by installing a weak monarch, Mohammad Reza Shah Pahlavi, which created the conditions for corruption and public resentment. These British actions set the conditions for a change in Iranian leadership and nationalisation of AOIC (Gasiorowski, Byrne, 2004, pp. 2–4, 12–14, 56–68; Rahnema, 2013, pp. 235–236, 265–267; Wright, 2021, pp. 15–18).

In April 1951, Mohammad Mosaddeq (alternatively Mossadegh) became Prime Minister after leading Iran's parliamentary movement to nationalise the British-controlled oil industry. The Iranian parliament ratified oil nationalisation on April 29, 1951, directly threatening Britain's largest overseas commercial enterprise. The British government owned 51% of AIOC, which generated £170 million in profit in 1950 alone. British Foreign Secretary Herbert Morrison immediately asserted on May 5, 1951, that Britain could ‘retaliate economically or militarily against Persia.’ By July 1951, Britain deployed three brigades of airborne troops to Iraq and strengthened its Persian Gulf naval squadron in preparation for Operation Buccaneer to seize the AIOC’s Abadan refinery (Rahnema, 2013, pp. xv–xvi, 289–290).

However, opposition from President Truman and Assistant Secretary of State George McGhee persuaded the British military not to invade. Britain then orchestrated a comprehensive international oil embargo coordinated with major oil companies, called the ‘Seven Sisters’. This caused Iranian oil exports to plummet 97% and devastating government revenues. Additionally, the British organised a clandestine coup in the Iranian parliament, called the Majlis, to oust Mosaddeq. Despite this economic and military pressure, Mosaddeq remained domestically popular through mid-1953, implementing non-oil economic strategies that prevented total collapse (Gasiorowski, Byrne, 2004, pp. 229–231, 271–273, 319–320). At the time, the Iranian view was positive and arguably a result of American soft power; however, the U.S. approach to Iran would change with the U.S. president and British framing of Iranian nationalism as a communist threat.

The Eisenhower administration, which assumed office in January 1953, shifted U.S. policy from supporting Mosaddeq to authorising regime change. In coordination with British intelligence, U.S. officials concluded that Iran's deteriorating political situation and Mosaddeq's inability to settle the oil dispute created conditions where the communist Tudeh Party could rise to power and enable Soviet control of Iran (Gasiorowski, Byrne, 2004, pp. 229–233). Between February and April 1953, Secretary of State John Foster Dulles and CIA Director Allen Dulles approved a joint CIA-SIS Operation TPAJAX or AJAX, allocating $1 million to ‘bring about the fall of Mosaddeq’ and re-install Rhesah Shah with General Fazlollah Zahedi's support. The primary stated justification was preventing Iran from ‘falling into Soviet hands,’ though securing Western access to Iranian oil resources was equally critical to U.S. and British strategic interests (Wright, 2021, pp. 18–19; Rahnema, 2013, pp. xx–xxiii, 27–30, 290–293).

On 19 July 1953, Kermit Roosevelt, from the newly formed U.S. Central Intelligence Agency, arrived in Iran and successfully executed the plan to overthrow Mosaddeq’s government. Roosevelt used covert funding, information warfare, bribery, and orchestrated violence through Iranian proxies. The initial attempt failed. Yet, Roosevelt persisted, and the second attempt succeeded. On 19 August 1953, General Fazlollah Zahedi declared himself the temporary leader until the Shah returned from exile (Rahnema, 2013, pp. xxiii–xxv, 60–66, 1–3; Gasiorowski, Byrne, 2004, pp. 249–256, 259–261, 263–265). After returning, the Shah and Zahedi consolidated power by arresting and crushing opposition, extinguishing the fledgling and only democracy in the region. With the support of the U.S., the Shah ran an authoritarian state until 1979, when a revolution enabled Ayatollah Khomeini to seize power as the Supreme Leader of the new Islamic Republic of Iran, using an anti-American message (Gasiorowski, Byrne, 2004, pp. 258–263; Wright, 2021, pp. 123–129).

Annex B: Recommendation Background

Consequences of Trump's Hard Power approach to Greenland

While writing this paper, President Trump and his Administration applied diplomatic hard power directly on Denmark, Greenland, the EU, and NATO allies. During his second term, President Trump made Greenland a major foreign policy priority. Stating during his State of the Union address on 4 March 2025, 'I think we're going to get it [Greenland] one way or the other. We're going to get it' (Trump, 2025b). Then, International relations concerning Greenland spiked after the successful operation to capture and bring Venezuelan President Nicolas Maduro to the U.S. on drug trafficking charges. Emboldened by this successful demonstration of U.S. military hard power, President Trump implied that annexing Greenland by force was an option. Second, He threatened additional tariffs against Denmark and European Countries opposing his demands (Vela, 2026). In addition to other statements, President Trump texted the Prime Minister of Norway on 19 January 2026, 'Dear Jonas: Considering your Country decided not to give me the Nobel Peace Prize for having stopped 8 Wars PLUS, I no longer feel an obligation to think purely of Peace, although it will always be predominant, but can now think about what is good and proper for the United States of America. Denmark cannot protect that land from Russia or China, and why do they have a 'right of ownership' anyway? There are no written documents, it's only that a boat landed there hundreds of years ago, but we had boats landing there, also. I have done more for NATO than any other person since its founding, and now, NATO should do something for the United States. The World is not secure unless we have Complete and Total Control of Greenland. Thank you! President DJT'(Buli, 2026; Vela, 2026).

These actions have alienated European and NATO allies. The resulting consequences are yet to be realised. However, the Prime Minister of Canada, Mark Carney, delivered a speech at the 2026 World Economic Forum the following week, indicating that potential long-term damage to U.S. legitimacy and the current World Order has been done. Carney stated, 'It seems that every day we're reminded that we live in an era of great power rivalry, that the rules-based order is fading, that the strong can do what they can, and the weak must suffer what they must…. On Arctic sovereignty, we stand firmly with Greenland and Denmark, and fully support their unique right to determine

Greenland's future… We know the old order is not coming back. We shouldn't mourn it. Nostalgia is not a strategy, but we believe that from the fracture, we can build something bigger, better, stronger, more just'(Carney, 2026). The Foreign Minister of Denmark and Kaja Kallas, the Vice President of the European Commission, issued similar statements condemning President Trump's actions. President Kallas stated, 'We [the EU] have no interest to pick a fight, be we will hold our ground [against the U.S. coercion to acquire Greenland],' and 'We [the EU] want strong trans-Atlantic ties. But Europe needs to adapt to new realities. It's no longer Washington's primary centre of gravity…'(Kallas, 2026).

Ms. Māra Maija VĒBERE: NATO's Strategic Edge in AI: Leveraging Export Controls for Technological Superiority

Supervisor: Mr. Louis WIERENGA

Statement on the Use of AI Tools:

This research paper was developed with assistance from AI tool – M360 Copilot for the purpose of editorial support, including checking grammar, improving clarity and coherence. AI was also used to narrow down the research topic that would fit within the set word count and to search for source materials from publicly available sources, which were later reviewed independently. All analysis, argumentation, and conclusions are my own.

INTRODUCTION

On NATO's eastern flank, where the pressure of the Russian military remains a persistent threat, technological superiority is not a luxury but a strategic necessity. Artificial intelligence (AI) has rapidly become a decisive factor in modern warfare, shaping everything from intelligence collection and targeting to autonomous systems and logistics. However, AI superiority fundamentally depends on access to advanced AI chips – the specialised processors required to train and deploy modern machine-learning systems. As a result, export controls on these chips have become a central instrument of strategic competition in the post-2022 security environment.

Following Russia's full-scale invasion of Ukraine, the United States (U.S.) and its Allies imposed restrictions on the transfer of advanced semiconductors and manufacturing equipment. These measures now target not only Russia but also China, the world's largest semiconductor consumer and Russia's most important technological partner. As a result, these restrictions limit Russia's access to high-end chips while simultaneously slowing China's technological progress.

This paper examines the strategic role of export controls on advanced AI chips in shaping Russia's and China's capabilities and NATO's technological advantage. The analysis primarily focuses on the post-2022 environment and the sanctions that followed, assessing how these restrictions influenced the development of AI-enabled systems in the ongoing war in Europe. It further assesses whether such controls constrain Russia's military AI innovation and identifies what additional measures NATO must take to maintain its technological edge.

Against this background, the following research question is proposed: How can NATO strategically leverage export controls on AI chips to maintain technological superiority over Russia and China in an evolving military technological competition? This paper argues that export controls offer NATO a temporary but significant strategic edge, however, to sustain long-term superiority, NATO must pair export controls with

proactive investments in defence innovation, strengthened Alliance interoperability, and robust counter-AI strategies.

Export controls may slow the technological progress of both China and Russia, but they cannot guarantee long-term superiority. For NATO, the challenge is to exploit the current window of advantage created by export restrictions while adversaries try to adapt. The relevance of this research stems from the accelerated militarisation of AI and the extent to which semiconductor supply chains now directly influence operational outcomes and long-term strategic stability.

The roadmap for the paper proceeds as follows. Chapter 1 outlines the conceptual foundation for the use of AI in the military and the strategic importance of AI chips. Chapter 2 analyses Russia's AI trajectory and the impact of export controls, including China's role as a significant supplier. Chapter 3 examines NATO's AI integration efforts and the relative advantage created by its access to advanced semiconductors. Chapter 4 offers strategic recommendations for sustaining NATO's technological edge.

CHAPTER 1: CONCEPTUAL FRAMEWORK

AI has rapidly become an important component of modern military power. In the defence context, AI refers to computer systems capable of performing tasks that traditionally require human cognition (Morgan, 2020, p. 9), but at a speed and scale not attainable by human operators. Military forces worldwide are integrating AI into operations, particularly through systems such as unmanned autonomous vehicles, robotic platforms, and decision-support tools that process vast amounts of battlefield data at unprecedented speeds (Reinhold, 2025, p. 14).

AI systems do not function in isolation; they depend on the computational power provided by specialised hardware. AI chips such as graphics processing units (GPUs), field programmable gate arrays (FPGAs), and application-specific integrated circuits (ASICs) are designed to handle the intensive processing required for training and deploying machine-learning models. IBM defines these chips as computer microchips specially designed to execute complex AI tasks that exceed the capabilities of traditional CPUs (Flinders and Smalley, 2025). GPUs are widely used for deep

learning, image recognition, and large-scale data analysis, including swarm-coordination tasks (Flinders et al., 2025). FPGAs, being versatile and reprogrammable, support specialised tasks involving signal processing and data acquisition, which makes them widely used in UAVs, performing flight control, sensor processing, and communications (Schneider, Smalley, 2025). ASICs, optimized for specific tasks, can support both training and inference in high-performance systems (Khan, Mann, 2024). Unlike earlier defence innovations, military AI development is driven primarily by the commercial sector. AI companies generate breakthroughs that rapidly advance applications relevant to defence. This dynamic creates both opportunities and vulnerabilities, as states with access to advanced commercial AI products gain significant military advantages, while those without access face structural limitations in their ability to develop competitive AI systems (Reinhold, 2025, p. 15).

Earlier assessments of military AI, such as RAND's 2020 report *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World*, identified three primary areas where AI was expected to transform warfare:

1. operational effectiveness, including acceleration of the OODA loop and improved targeting;
2. data processing and analysis, enabling the exploitation of massive ISR datasets; and
3. resource optimization through automation of routine tasks, predictive maintenance, and supply-chain management (Morgan, 2020, pp. 15-20).

At the time, these applications were largely speculative, however, the war in Ukraine has demonstrated that AI-enabled systems, especially autonomous platforms, now deliver tangible battlefield advantages. Ukraine's use of AI-supported drone operations, including long-range autonomous missions such as the 'Spiderweb', illustrates how AI can shift elements of warfare away from direct human involvement and enable deeper penetration into enemy territory.

Because AI chips are essential for advanced military AI applications, several countries have imposed export controls on their manufactured AI chips and semiconductor equipment. Since 2022, the U.S. has led coordinated efforts to restrict access to advanced semiconductors, focusing primarily on China but with significant effects on

Russia as well. These controls target chips that exceed a specific Total Processing Performance (TPP) threshold, particularly GPUs and certain high-bandwidth memory (HBM) accelerators which are important for training large-scale AI models. The U.S. has also extended restrictions to AI chips manufactured abroad using U.S. technology, significantly tightening global compliance requirements (Allen and Goldston, 2025, pp. 2-5).

Recent actions by the U.S. Bureau of Industry & Security (BIS) include closing regulatory loopholes (OCPA 15 Jan 2025), expanding the Entity list by adding parties attempting to enhance China's computing capabilities, issuing multi-million-dollar penalties (Last 2025), and strengthening enforcement through the Disruptive Technology Strike Force. In 2024 alone, BIS Export Enforcement reported 26 criminal cases involving export-control violations linked to China, Russia, and Iran (OCPA 2 Jan 2025). In January 2025, the U.S. announced additional restrictions on advanced computing semiconductors, reinforcing due-diligence requirements for foundries to prevent diversions to China (OCPA 15 Jan 2025).

Allied efforts have aligned unevenly with U.S. export restrictions, with some partners hesitant to apply bigger pressure on Russia's access to AI hardware. The EU remains constrained by the Wassenaar Arrangement, where Russia retains veto power over any meaningful amendments concerning AI chips (Allen and Goldston, 2025, p. 6). However, key partners such as the Netherlands and Japan have tightened restrictions. On 15 January 2025, the Netherlands announced restrictions on advanced semiconductor equipment, including lithography tools essential for the manufacturing of AI chips (Netherlands 15 January 2025). Japan soon followed with similar measures, prompting China to release a statement about 'certain countries' abusing export control measures to suppress China's semiconductor industry (Allen and Goldston, 2025, p. 20). South Korea and Taiwan also mostly comply with U.S. restrictions due to supply chain dependencies (Allen and Goldston, 2025, pp. 20-25).

These controls create a temporary window of strategic advantage for NATO. However, this advantage is time-limited and may incentivise Russia and China to accelerate domestic innovations that could eventually erode or surpass the current Western lead.

CHAPTER 2: RUSSIA'S AND CHINA'S MILITARY AI TRAJECTORIES UNDER EXPORT CONTROLS

Russia presents itself as an aspiring AI power. Its 2019 National AI Strategy, updated in 2023, set two milestones: to improve Russia's global AI standing by 2024, and to eliminate its lag behind developed countries and achieve 'leadership in certain AI-related areas' by 2030 (GINC, 2026). This ambition is reinforced at the political level. On 1 September 2017, Vladimir Putin met with students in Yaroslav, Russia, and stated that the development of AI raises 'colossal opportunities and threats that are difficult to predict now'. He warned that 'the one who becomes the leader in this sphere will be the ruler of the world' (AP News, 2017). Almost six years later, on 7 March 2023, in a conversation with Sberbank CEO German Gref in Moscow, Putin said that '[AI] is absolutely the future. If we talk about the importance for the country, for any country, it is on par with atomic or missile projects of the Soviet Union in the mid-1940s and 1950s' (Reuters, 2023).

However, Russia's AI ambition rests on a structurally weak foundation. Even before 2022, Russia depended heavily on Western semiconductors, foreign manufacturing, and imported electronics. After the invasion of Ukraine, sanctions severed access to these technologies, forcing Russia to rely on domestic products or to import from non-Western intermediaries (Bergmann et al., 2023, p. 22). According to a Russian media news article from 1 October 2024, Russia announced plans to invest up to 240 billion RUB (approximately USD 2.5 billion) by 2030 in a project focused on developing equipment and materials for domestic chip manufacturing, however, there is no evidence that Russia is close to closing the gap with global leaders in AI hardware or semiconductor production (Trueman, 2024).

As a result, Russia's AI ecosystem suffers from limited domestic semiconductor components, dependence on foreign components, industrial bottlenecks, and a widening gap between political rhetoric and technological reality. These weaknesses have been amplified by export controls, which restrict access to the advanced chips required for AI development.

China occupies a unique position in the global AI landscape. It is both a strategic competitor to NATO and a major supplier of commercial electronic components to Russia. Yet China's own semiconductor ecosystem faces significant constraints. Despite massive state investment, China still cannot produce AI chips that match the performance of leading U.S. designs. In a study published on 15 December 2025, researchers compared AI chips produced by Nvidia and Huawei and found that the best Nvidia chips significantly outperform Huawei's, with U.S. made chips demonstrating up to five-fold performance advantage over the best of China's, with the gap projected to probably grow in next two years' time (McGuire, 2025). Chinese researchers themselves acknowledge that the AI chips from China have performance shortcomings (Wu and Ren, 2025).

Although China pushes its tech companies to use domestic AI chips (Chang, 2025), a study from August 2025 shows that China's tech firms are reluctant to use Huawei's chips themselves. Chinese AI developers overwhelmingly prefer using Nvidia chips and go to great lengths to try to obtain them, with Chinese companies spending USD16 billion to stockpile Nvidia's H20 chips ahead of a potential U.S. ban on their sales to China (Chan, 2025).

China's broader AI ecosystem, however, is far more advanced than Russia's. According to the World Economic Forum's *Blueprint to Action: China's Path to AI-Powered Industry Transformation* (January 2025), China has built one of the world's largest AI infrastructures, supported by national computing grids, extensive 5G coverage, and a rapidly expanding data environment (Na et al., 2025, p. 12). The report states that China is investing heavily in strategic infrastructure, sector-specific AI models, and talent cultivation, creating a robust foundation for long-term AI development.

China's 2025 national AI strategy further accelerates this trajectory. According to the Global Tech Council (August 2025), China has launched a comprehensive national AI plan, supported by CNY 60 billion (approximately USD 8.2 billion) national AI fund, extensive regional level investments, and targeted support for generative AI, robotics, smart manufacturing, and quantum technologies (Tosh Marketing, 2025). These

initiatives reflect China's intent to reduce foreign dependence, strengthen domestic innovation capacity, and build a vertically integrated AI ecosystem.

Despite continued dependence on foreign lithography equipment, U.S. export controls on advanced GPUs and semiconductor equipment, and performance gaps in domestic AI chips, China remains far more technologically capable than Russia.

Following the 2022 invasion of Ukraine, Western technologies were cut off to Russia through extensive sanctions, pushing Russia to exploit loopholes through China, EAEU countries, and non-Western intermediaries such as Türkiye and several Central Asian states (Zayakin, 2025). Most notably, Kazakhstan emerged as the main middleman. Research from January 2025 shows that microelectronics exports to Russia have surged from USD 791,890 in June to USD 2,285,227 in July, with post-invasion (from February 2022 to February 2024) averages (USD 1,405,244) reflecting a 567% increase over pre-invasion (January 2020 to January 2022) averages (USD 210,681) (Ruth 2025). These numbers illustrate the scale of sanctions evasion but do not indicate access to advanced AI chips.

China became Russia's largest supplier of semiconductors after announcing its 'no-limits' partnership with Russia 20 days before the 2022 invasion, with exports of semiconductors increasing by USD 75.3 million from 2020 to 2023 (Ruth, 2025). However, research from April 2025 suggests that these flows may have slowed down. In 2024, electronic imports from China dropped from USD 1.6 billion to USD 260 million, while imports from countries that adhere to the sanctions more strictly, like, EU/EEA, Switzerland, the UK, U.S., Canada, Australia, New Zealand, South Korea, and Japan, had dropped below USD 200 million (Zayakin, 2025). In the end these evasion tactics have failed to deliver any advanced AI chips to Russia.

Overall, sanctions have intensified pre-existing structural weaknesses in Russia's military industry, accelerating technological stagnation, hardware shortages, and production degradation (Boulègue, 2025, p. 3). With innovation stagnation and hardware shortages, as well as degradation of production, Russia is seeing regression rather than progress, substituting higher-end components from Western countries with lower-quality alternatives, forcing reliance on attritional warfare using large quantities

of inexpensive munitions rather than high technology manoeuvres and operations, a contrast pointed out by Ukraine's more technologically enabled approach (Bergmann et al., 2023, p. 36-39). In the AI competition anticipated by Putin, Russia is evidently lagging, with noticeable operational impact.

CHAPTER 3: NATO'S AI INTEGRATION AND THE RELATIVE ADVANTAGE

NATO's approach to AI is anchored in a robust, Alliance-wide governance framework. The 2021 NATO AI Strategy established the Alliance's strategic vision for AI adoption, setting four aims: 1) responsible development and use, 2) accelerated adoption and interoperability, 3) protection/monitoring of AI and innovation, and 4) safeguarding against malicious use. It also introduces Principles of Responsible Use (PRUs) to ensure lawfulness, responsibility, accountability, explainability, traceability, reliability, governability, and bias mitigation (NATO, 2024), to ensure that AI-enabled systems deployed by NATO member states uphold transparency and human oversight, even in difficult operational situations. These principles were reaffirmed and operationalised in the 2024 Revised AI Strategy, which emphasises accelerating AI adoption, enhancing interoperability, protection of innovation, and safeguarding against adversarial AI use, including risks arising from new capabilities such as generative AI and AI-enabled information tools. By establishing shared standards and governance mechanisms, NATO enables its 32 members to integrate AI systems across domains (Clement, 2024, p. 11). This creates a coordination advantage: NATO can use common principles and shared implementation efforts to pursue interoperability across Allies, even though national approaches and capabilities still vary.

NATO's innovation ecosystem is designed to accelerate the development and adoption of dual-use technologies across the Alliance. The Defence Innovation Accelerator for the North Atlantic (DIANA) serves as a bridge between governments, industries, and academia, identifying and supporting promising innovators through accelerator programmes (Clement, 2024, p. 6). It gives them access to an Alliance-wide network of accelerator sites and test centres to help de-risk, validate, and demonstrate solutions (NATO, 2024). The NATO Innovation Fund (NIF) complements DIANA by providing long-term investment to scale these technologies, with NATO describing it as a multi-sovereign venture capital fund with 15-year timeframe, intended to back

early-stage dual-use technologies relevant to Alliance security (NATO, 2025). DIANA and the NIF are legally separate but mutually reinforcing – DIANA focuses on problem-driven challenge calls and acceleration, while the NIF provides larger capital and prioritizes investment in DIANA accelerated companies located in participating nations (NATO DIANA, n.d.). Together they are meant to shorten the road from innovation to adoption by combining problem driven challenge calls, testing and evaluation capacity, and scale-up capital aligned with NATO and national demand signals (NATO, 2024; NATO DIANA, n.d.).

NATO's operational integration of AI is noticeable across multiple mission critical domains. In intelligence, surveillance, and reconnaissance (ISR), the Alliance employs AI-driven orchestration systems such as the STAR (Sharing Tasks with Autonomous Resources) system to coordinate manned and unmanned assets, enabling real-time task allocation and improved coordination under human oversight (Paul et al. 2025, p.1). NATO experimentation activities, such as the Digital Backbone Experiment (DiBaX2025) hosted in Latvia, focused on testing the use of unmanned systems in complex and contested environments and on assessing how AI can support detection and decision-making tasks within multi-domain operations (Latvia MoD Press Division, 27 Oct 2025).

For decision support, digital assistants like AI FELIX, as well as initiatives like AIDA and AI CLAIR, are being developed under NATO ACT to support information management, documentation handling, and knowledge discovery across NATO structures, with the aim of reducing routine staff workload and improving access to relevant information (NATO ACT, 2025).

NATO's approach to AI is not limited to policy development but also reflects on the operational level. In its *Science & Technology Trends 2025-2045* report from April 2025, NATO Science and Technology Organisation (STO) states that, in the military context, AI can support strategic planning and tactical decision-making support, strengthen intelligence, surveillance, and reconnaissance (ISR) capabilities, and improve cyber network monitoring and defence, etc. (Sweeney, 2025, p. 17). Within this framework, AI-enabled orchestration tools, such as the STAR (Sharing Tasks with Autonomous Resources) system, are intended to support planning, tasking,

orchestration, and execution of coordinated multi-domain operations. In a proof-of-concept implementation, the STAR system achieved tasking accuracy up to 89% in modelling and simulation environments, while retaining human control over final decision (Paul et al., 2025, p. 12).

Building on NATO's AI governance framework, innovation ecosystem, and emerging operational use cases already discussed above, the Alliance's relative advantage lies primarily in its capacity for multinational integration under conditions of strategic competition. Unlike Russia, whose AI development is constrained by sanctions and industrial limitations, and China, whose AI trajectory remains heavily state centric and nationally bounded, NATO operates as a coalition that must translate technological capacity into interoperable and trusted military effects across multiple sovereign actors, to achieve common and national AI goals (RUSI, n.d.).

While the need for prioritisation of interoperability imposes coordination costs, it also creates a comparative strength, as AI systems designed, tested, and governed for coalition use are more readily scalable across allied operations than nationally optimized solutions (Huisman, 2025, pp. 5-6). The strategic environment, created by export controls on advanced AI chips and semiconductor manufacturing equipment, further amplifies NATO's relative advantage. The controls themselves do not generate technological superiority, but they shorten adversarial AI advancement timelines and increase the strategic value of NATO's existing strengths in integration, experimentation, and Alliance-wide adoption. The controls work as a force multiplier rather than a decisive instrument (Allen, 2025, pp. 2-7).

Despite NATO's emerging integration advantage, the adoption of AI-enabled capabilities introduces a set of persistent challenges and risks that could limit operational effectiveness if left unaddressed. For example, interoperability across human, technical, and procedural dimensions is not automatic and imposes significant coordination costs, which may be aggravated as AI systems become more complex and data dependent (Huisman, 2025, pp. 5-6). Related challenges arise from data governance and information sharing constraints. AI-enabled decision support systems may risk producing degraded or misleading outputs when data is fragmented, outdated, or inaccessible across national boundaries, potentially undermining Alliance

decision making rather than enhancing it (Reynolds 2024). There are also governance, legal, and accountability risks. Uneven national approaches to AI procurement, oversight, and ethical standards may slow down adoption and erode trust among Allies, particularly where responsibility for AI assisted decisions remains unclear (Clement, 2024, pp. 2-5). Finally, digital infrastructure dependencies, including reliance on cloud-based systems, introduce independence and resilience concerns in crisis or wartime scenarios (Sylvia, 2025). Together these challenges mean that NATO's AI advantage remains conditional and contingent on sustained efforts to manage integration risks alongside capability developments.

CHAPTER 4: SUSTAINING LONG TERM SUPERIORITY: STRATEGIC RECOMMENDATIONS

4.1 Strategic implications of AI and Export Controls for NATO

The analysis in Chapter 1-3 demonstrates that export controls on advanced AI chips and semiconductor manufacturing equipment have altered the strategic environment in which NATO, Russia, and China pursue military AI development. However, these controls do not determine outcomes by themselves. Rather they create a temporary window of opportunity during which NATO can consolidate its relative advantage while adversaries face delayed access to advanced AI chips (Allen, 2025, pp. 1-2). Sanctions and export restrictions have reinforced Russia's pre-existing industrial weaknesses. They have contributed to shortages of advanced AI chips and substitution with lower quality alternatives. China, although constrained by export controls, continues to advance through scale, state coordination, and infrastructure investments (Bergman et al., 2023, p. 4) (Na et al. 2025, pp. 5, 11-12).

For NATO, the main problem is that technological denial alone is not enough. Export controls function primarily as instruments for buying time. Their strategic value depends on what the Alliance does during the time these controls are in effect. The effectiveness of these controls is also dependent on allied alignment, enforcement capacity, and political willingness. But even then, the controls cannot guarantee long term technological superiority over competitors (Allen, 2025, pp. 1-2). There is

significant uncertainty around the military impact of AI. NATO should not assume linear advantage or automatic dominance (Black, 2024, p. 3).

NATO's relative advantage is conditional and can disappear. It rests not on permanent denial of adversary capabilities. Instead, it depends on the Alliance's ability to translate time into durable gains in integration, interoperability, and operational learning. Failure to do so risks wasting the strategic space created by export controls. This would allow competitors, especially China, to adapt and narrow the gap.

4.2. Policy Option I: Deepening Alliance Wide AI Integration

The first and most important policy option for NATO is to deepen Alliance-wide AI integration. This reinforces the core advantage identified in Chapter 3 – NATO's capacity to coordinate and operationalize AI across the Alliance. Interoperability in this context goes beyond purely technical compatibility. It also includes procedural and human dimensions (Huisman, 2025, p. 1). AI-enabled systems that heavily depend on shared data, mutual trust, and assurance mechanisms. As a result, they tend to amplify these challenges rather than mitigate them.

The case for prioritizing integration is grounded in the specific challenges identified in Chapter 3: uneven digital readiness across Allied states, data governance fragmentation that risks degrading AI-assisted decision-making across national boundaries (Reynolds, 2024), and the gap between the STAR system 89% simulation accuracy and the messier conditions of real coalition operations (Paul et al., 2025, p. 12). From a strategic perspective, prioritizing integration means embedding interoperability requirements more systematically into NATO's defence planning, experimentation, and capability development processes. NATO's existing transformation structure provides a foundation for this approach. However, integration must extend beyond isolated pilot projects, central HQs, or small-scale systems. The goal is not uniformity but coherence, ensuring that AI-enabled systems developed by different Allies can operate together under shared standards, governance frameworks, and command arrangements.

Deepening integration also requires addressing disparities in digital readiness across the Alliance. Uneven development of cloud infrastructure, data architecture, and AI processing capacity risks fragmenting NATO's digital ecosystem. This fragmentation could undermine operational effectiveness and political trust. Preventing such outcomes requires deliberate coordination, sustained investment in enabling infrastructure, and the development of human capital across all member states (Horan, 2025, p. 2).

This policy option would build directly on NATO's existing strategies rather than replacing them. It treats AI not as a stand-alone capability, but as an enabling technology. Its military value emerges only when embedded within interoperable systems capable of supporting collective defence and joint operations.

4.3. Policy Option II: Aligning Export Controls with Alliance Innovation

The second policy option concerns aligning export controls more closely with NATO's innovation and integration efforts. As established in Chapters 1 and 2, the need for better Allied coordination is demonstrate by specific failures, including the 567% surge in microelectronics routed through Kazakhstan that exposed enforcement gaps (Ruth, 2025), and the uneven Allied alignment with U.S. restrictions, that has left coordination structurally incomplete (Allen and Goldston, 2025, p. 6). These restrictions have constrained Russia's access to advanced AI chips and complicated China's ability to obtain high-end AI systems. At the same time, the analysis in Chapter 3 shows that these measures do not by themselves generate NATO's relative advantage. Rather, they delay adversaries and shape the strategic environment in which competition unfolds.

From a strategic standpoint, export controls are most effective when they are coordinated among Allies and fixed within broader strategic objectives. Their impact depends not only on formal legal authorities, but also on enforcement capacity, political willingness, and consistency across participating states. Where alignment is weak, whether due to uneven implementation, regulatory loopholes, or divergent national priorities, the effectiveness of controls is diminished. In some cases, this may accidentally accelerate adversary efforts to develop new alternatives. On the other

hand, overly rigid or unilateral restrictions risk disrupting allied innovation ecosystems. This is particularly true in areas where commercial AI development provides the technological base for military capabilities.

For NATO, this implies that export controls should be treated as a supporting instrument rather than a substitute for capability development. Controls must be adjusted to preserve Allied access to critical technologies, protect shared innovation pipelines, and avoid creating disincentives for cooperation within the Alliance. Achieving this balance requires close coordination with national export controls authorities. It also requires engagement with key partners outside NATO whose industrial capabilities constitute critical nodes in the global semiconductor supply chain. Therefore, the strategic objective is not permanent technological denial, but strategic delay. Export controls should buy time for NATO to strengthen its integration advantage. At the same time, the Alliance must manage the risk of industrial fragmentation and unintended spillover effects.

4.4. Policy Option III: Managing Risk, Governance, and Trust

The third policy option focuses on managing the risks that accompany AI adoption within the multinational Alliance. As established in Chapter 3, these risks can be seen within the data governance fragmentation, that may cause AI decision support tools to produce degraded outputs when information is inaccessible across national boundaries (Reynolds, 2024), also in legal ambiguity surrounding accountability for AI assisted decisions and divergent national procurement standards risk slowing down Alliance wide adoption (Clement, 2024, pp. 2-5), and within cloud infrastructure dependency introduced resilience vulnerabilities in crisis or wartime conditions (Sylvia, 2025). If left unaddressed, such risks can erode trust among Allies and undermine operational effectiveness, particularly in time-sensitive and high-consequence decision making environments.

AI-enabled decision-making support systems are especially sensitive to quality, accessibility, and timeliness of data. Where data is fragmented, outdated, or unevenly shared across national systems, AI tools may degrade rather than enhance decision making. This amplifies coordination challenges in coalition operations. These risks are

compounded by persistent information sharing constraints and variations in national data governance frameworks. These factors can limit the reliability and legitimacy of AI assisted outputs in multinational settings.

Beyond technical considerations, uneven national approaches to AI procurement, oversight, and ethical governance introduce additional challenges. Legal ambiguity surrounding responsibility for AI-assisted decisions, combined with divergent national standards, can slow down adoption. These issues can also complicate coalition operations, particularly where accountability for outcomes remains unclear. Managing these issues is essential to maintaining political confidence and operational trust within the Alliance.

Digital infrastructure dependencies further shape the risk environment. They increase reliance on cloud-based services. Cross-border digital architecture introduces vulnerabilities related to independence, resilience, and continuity of operations, especially during crisis or wartime conditions. Differences in national risk tolerance can complicate collective action and expose critical dependencies at the peak operational demand. These dynamics underline that effective AI integration depends as much on governance, assurance, and resilience as on technical performance.

Managing these risks does not imply slowing AI adoption. Rather, it requires clarifying accountability structures, reinforcing meaningful human oversight principles, and ensuring that governance mechanisms scale alongside operational use.

4.5. Strategic Trade-offs and the Cost of Inaction

The policy options outlined above involve unavoidable strategic trade-offs. Deepening Alliance-wide AI integration imposes coordination costs. Aligning export controls with innovation requires security balanced with industrial capability. Strengthening governance frameworks may also constrain rapid deployment.

In an environment characterised by rapid technological change and compressed decision-making timelines, inaction does not preserve the status quo. Instead, it increases the likelihood of fragmented adoption, uneven capability development, and

diminishing interoperability across the Alliance. Strategic advantage in AI is neither automatic nor durable. It depends on institutional adaptation and integration. Delays in addressing integration and governance create opportunities for competitors to narrow gaps. And they may also exploit weaknesses, even under continued technological constraint.

AI-enabled military systems also interact with strategic stability. Poorly coordinated or weakly governed adoption can amplify misperception, alter escalation dynamics, and increase uncertainty in crisis situations. The cost of inaction is therefore not neutrality, but strategic erosion. In the end, NATO's challenge is not whether to adopt AI but how to do so in a way that sustains Alliance cohesion and operational credibility. The analysis above suggests that NATO's relative advantage lies in integration, not dominance. This advantage must be actively maintained.

CONCLUSION

This research paper set out to answer the following research question: How can NATO strategically leverage export controls on AI chips to maintain technological superiority over Russia and China in an evolving military technological competition?

The analysis shows that NATO does possess a relative advantage in military AI development, but this advantage is conditional, time-bound, and organisational, rather than technical. Chapter 1 established the conceptual framework, demonstrating that AI is commercially driven, data and hardware dependent technology, making access to advanced semiconductors and effective governance central to military relevance. Chapter 2 examined Russia's and China's AI trajectories under export controls, showing that while Russia's AI development has been significantly constrained by sanctions and industrial weakness, China retains the capacity to adapt and advance despite external restrictions. Chapter 3 demonstrated that NATO's advantage does not derive from superior national capabilities but from its ability to integrate AI across the Alliance through shared governance frameworks, innovation mechanisms, and emerging operational applications.

Chapter 4 combined these findings and turned them into strategic implications. It showed that export controls function as a force multiplier rather than a decisive instrument, buying time for NATO, rather than determining outcomes. The analysis further demonstrated that NATO's advantage depends on deepening Alliance-wide integration, aligning export controls with innovation, and managing governance, trust, and infrastructure risks. Failure to address these areas would erode interoperability and undermine collective effectiveness, even in the absence of a rapid breakthrough in adversarial AI.

This paper argued that export controls offer NATO a temporary but significant strategic edge, but to sustain long-term superiority, NATO must pair export controls with proactive investments in defence innovation, strengthened Alliance interoperability, and robust counter-AI strategies. The analysis supports the thesis that export controls alone are insufficient and that NATO's advantage is conditional and depends on how effectively the Alliance uses the time bought by export controls to build interoperable, trusted, and resilient military capabilities.

The relevance of these findings lies in their implications for Alliance strategy in an era of rapid technological diffusion. Military advantage in AI will increasingly favour those capable of coordinated governance and collective adaptation rather than those relying solely on denial. Future research should focus more on the operational level and examine how NATO's AI integration performs under crisis conditions, how counter AI strategies evolve alongside adversarial adaptation, and how Alliance governance mechanisms adjust as AI becomes more deeply embedded in military operations.

BIBLIOGRAPHY

PRIMARY SOURCES/LEGAL ACTS:

OFFICE OF CONGRESSIONAL AND PUBLIC AFFAIRS. 2025. Commerce Strengthens Restrictions on Advanced Computing Semiconductors to Enhance Foundry Due Diligence and Prevent Diversion to PRC. *Bureau Of Industry and Security.* [online]. 15 January 2025. Available at: https://www.bis.gov/press-

release/commerce-strengthens-restrictions-advanced-computing-semiconductors-enhance-foundry-due-diligence-prevent.

OFFICE OF CONGRESSIONAL AND PUBLIC AFFAIRS. 2025. Export Enforcement Releases 2024 Year in Review. *Bureau of Industry & Security.* [online]. 2 January 2025. Available at: https://www.bis.gov/press-release/export-enforcement-releases-2024-year-review.

GOVERNMENT PRESS RELEASES:

LATVIA MOD. 2025. In the largest NATO 'Digital Backbone Experiment' the use of unmanned systems in complex environments will be tested. *The Latvian Ministry of Defence Press Division*. [online]. 27 October 2025. Available at: http://www.mod.gov.lv/en/news/largest-nato-digital-backbone-experiment-use-unmanned-systems-complex-environments-will-be.

NATO. 2024. Summary of NATO's revised Artificial Intelligence (AI) strategy. *The North Atlantic Treaty Organization*. [online]. 10 July 2024. Available at: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy.

NATO. 2025. Defence Innovation Accelerator for the North Atlantic (DIANA). *The North Atlantic Treaty Organization*. [online]. 26 June 2025. Available at: https://www.nato.int/en/about-us/organization/nato-structure/defence-innovation-accelerator-for-the-north-atlantic-diana?selectedLocale=.

GOVERNMENT OF NETHERLANDS. **2025**. Klever: export controls on advanced semiconductor manufacturing equipment to be tightened. *Government of Netherlands*. [online]. 15 January 2025. Available at: https://www.government.nl/latest/news/2025/01/15/klever-export-controls-on-advanced-semiconductor-manufacturing-equipment-to-be-tightened.

RESEARCH:

ALLEN, Gregory C.; GOLDSTON, Isaac. 2025. Understanding U.S. Allies: Current Legal Authority to Implement AI and Semiconductor Export Controls. *The Center for Strategic and International Studies*. [online]. 14 March 2025. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-03/250314_Allen_AI_Controls.pdf.

BERGMANN, Max; SNEGOVAYA, Maria; DOLBAIA, Tina; FENTION, Nick. 2023. Out of Stock? Assessing the Impact of Sanctions on Russia's Defense Industry. *The Center for Strategic and International Studies*. [online]. April 2023. Available at:

https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230414_Bergmann_Out_Stock.pdf?VersionId=6jfHCP0c13bbmh9bw4Yy2wbpjNnfeJi8

BOULÈGUE, Mathieu. 2025. Russia's struggle to modernize its military industry: How sanctions, war and 'innovation stagnation' are weakening Moscow's capabilities. London: *Royal Institute of International Affairs*. [online]. 21 July 2025. Available at: https://doi.org/10.55317/9781784136468

CHANG, Wendy. 2025. Domestic substitution in AI chips: China's big gamble. *MERICS*. [online]. 4 December 2025. Available at: https://merics.org/en/comment/domestic-substitution-ai-chips-chinas-big-gamble

CLEMENT, Sven. 2024. NATO and Artificial Intelligence: Navigating the Challenges and Opportunities. Luxembourg: *The NATO Parliamentary Assembly*. [online]. 24 November 2024. Available at: https://www.nato-pa.int/document/2024-nato-and-ai-report-clement-058-stc

HUISMAN, Judith; LUCAS Rebecca; PALICKA Ondrej; WINDER, Sarah; SILFVERSTEN Erik. 2025. Interoperability in the Digital Environment: Opportunities and Challenges. *RAND Corporation*. Enabling NATO Digital Capabilities Series: Paper 3. [online]. 21 May 2025. Available at: https://www.rand.org/pubs/research_reports/RRA3831-3.html.

HORAN, Hans; ROMANSKY, Sofia; ELLISON, Davis. 2025. Securing the Digital Backbone: NATO's Quest for Interoperability in the Age of Emerging Disruptive Technologies. *The Hague Centre for Strategic Studies*. [online] June 2025. Available at: https://hcss.nl/wp-content/uploads/2025/06/05-Securing-the-Digital-Backbone-NATOs-Quest-for-Interoperability-in-the-Age-of-Emerging-Disruptive-Technologies-v7.pdf.

MORGAN, Forrest E. et al. 2020. Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World. *RAND Corporation*. [online]. 28 April 2020. Available at: https://www.rand.org/pubs/research_reports/RR3139-1.html.

MCGUIRE, Chris. 2025. China's AI Chip Deficit: Why Huawei Can't Catch Nvidia and U.S. Export Controls Should Remain. *Council on Foreign Relations*. [online]. 15 December 2025. Available at: https://www.cfr.org/articles/chinas-ai-chip-deficit-why-huawei-cant-catch-nvidia-and-us-export-controls-should-remain

NA, Na; GU, Sophia; TONG, Freda; XU, Bella; YU, Ya. 2025. *Blueprint to Action: China's Path to AI-Powered Industry Transformation*. *World Economic Forum &*

Accenture. [online]. January 2025. Available at: https://reports.weforum.org/docs/WEF_Blueprint_to_Action_Chinas_Path_to_AI-Powered_Industry_Transformation_2025.pdf

PAUL, Tanya; DUCLOS-HINDIE; Nicolas; LAFOND, Daniel. 2025. Orchestrating Manned-Unmanned Missions Using AI-Based Tasking System Across Multi-Domain Operations in M&S. *NATO Science and Technology Organization*. [online]. 27 November 2025. Available at: https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-MSG-229/MP-MSG-229-11.pdf

REINHOLD, Thomas. 2025. Artificial Intelligence, Semiconductors, and the Chip Wars: Reviewing the Geopolitics of AI in the Military and in International Security. *The CNTR Monitor: New Realities of AI in Global Security*. [online]. 2025, pp. 14–21. Available at: https://monitor.cntrarmscontrol.org/en/2025/artificial-intelligence-semiconductors-and-the-chip-wars-reviewing-the-geopolitics-of-ai-in-the-military-and-in-international-security/.

SWEENEY, Jordan; BAYLISS, Daniel; BUTCHER, Fiona; CALABRO, Salvatore; COX, Lucas; DRAGOMIR, Georgiana; EHLERT, Ulf; MARTIN-BLANCO, Alvaro; SIMON, Sascha. 2025. Science & Technology Trends 2025-2045. Brussels, Belgium: *The NATO Science and Technology Organization*. [online]. Available at: https://sto-trends.com/.

WU, Jiaqing; REN, Dapeng, 2025. Development of Artificial Intelligence Chips in China. *Strategic Study of Chinese Academy of Engineering*. [online]. 22 February 2025. Vol. 27, no. 1, Available at: https://www.engineering.org.cn/sscae/EN/10.15302/J-SSCAE-2024.10.028.

ONLINE ARTICLES:

BERG, Joshua. 2025. Cyber Deterrence in the Age of AI: How NATO is Adapting to Intelligent Threats from Russia and China. *New Geopolitics Research Network*. [online]. 28 May 2025. Available at: https://www.newgeopolitics.org/2025/05/28/cyber-deterrence-in-the-age-of-ai-how-nato-is-adapting-to-intelligent-threats-from-russia-and-china/.

CHAN, Kyle; WANG, Ray. 2025. Leashing Chinese AI Needs Smart Chip Controls. *The RAND Corporation*. [online]. 7 August 2025. Available at: https://www.rand.org/pubs/commentary/2025/08/leashing-chinese-ai-needs-smart-chip-controls.html.

FLINDERS, Mesh; SMALLEY, Ian. 2025, What is an AI chip? *IBM* [online]. 17 November 2025. Available at: https://www.ibm.com/think/topics/ai-chip.

FLINDERS, Mesh; SUSNJARA, Stephanie; SMALLEY, Ian. 2025. What is a GPU? *IBM* [online]. 17 November 2025. Available at: https://www.ibm.com/think/topics/gpu

GINC. 2026. Russia's National AI Strategy. *Global Institute for National Capability*. [online]. Available at: https://www.ginc.org/russias-national-ai-strategy/.

JAMISON, Miles. 2026. NATO's DIANA Launches 2026 Program to Accelerate Defense Innovation. *GovCon Exec International*. [online]. 4 February 2026. Available at: https://www.govconexec.com/2026/02/nato-diana-2026-program/

KHAN, Saif M.; MANN, Alexander. 2024. AI chips: What they are and why they matter. *Center for Security and Emerging Technology* [online]. 8 January 2024. Available at: https://cset.georgetown.edu/publication/ai-chips-what-they-are-and-why-they-matter/.

LAST, Ryan. 2025. BIS Export Enforcement's 2024 Year in Review: Strengthening US National Security Through Strategic Action. *Troutman Pepper Locke*. [online] 8 January 2025. Available at: https://www.troutman.com/insights/bis-export-enforcements-2024-year-in-review-strengthening-us-national-security-through-strategic-action/.

NATO DIANA. n.d. What is the difference between DIANA and the NATO Innovation Fund? How will they work together? *The Defence Innovation Accelerator for the North Atlantic (DIANA)* [online]. Available at: https://www.diana.nato.int/faq/difference-diana-nato-innovation-fund-work-together.html.

NATO DIANA. n.d. DIANA Accelerator Programme. *The Defence Innovation Accelerator for the North Atlantic (DIANA)* [online]. Available at: https://www.diana.nato.int/accelerator-programme.html.

NATO ACT. **2025**. Harnessing Artificial Intelligence: Allied command transformation at the forefront of NATO Innovation. *NATO ACT.* [online]. 16 April 2025. Available at: https://www.act.nato.int/article/harnessing-artificial-intelligence/.

RUTH, Oliver. 2025. The Impact of Sanctions and Alliances on Russian Military Capabilities. *The Royal United Services Institute*. [online]. 10 January 2025. Available at: https://www.rusi.org/explore-our-research/publications/commentary/impact-sanctions-and-alliances-russian-military-capabilities.

RUSI. n.d.. Artificial Intelligence (AI) and National Security. *The Royal United Services Institute*. [online]. Available at: https://www.rusi.org/explore-our-research/topics/artificial-intelligence-ai-and-national-security.

REYNOLDS, Ian; ATALAN Yasir. 2024. Calibrating NATO's Vision of AI-Enabled Decision Support. *The Center for Strategic and International Studies*. [online]. 8 July 2024. Available at: https://www.csis.org/analysis/calibrating-natos-vision-ai-enabled-decision-support.

SCHNEIDER, Josh; SMALLEY, Ian. 2025. What is a field programmable gate array (FPGA)? *IBM* [online]. 17 November 2025. Available at: https://www.ibm.com/think/topics/field-programmable-gate-arrays.

SYLVIA, Noah. 2025. Cloud Interoperability Between Allies During Crisis. *The Royal United Services Institute*. [online]. 5 November 2025. Available at: https://www.rusi.org/explore-our-research/publications/insights-papers/cloud-interoperability-between-allies-during-crisis.

TOSH MARKETING. **2025**. China Launches Comprehensive National AI Strategy. *Global Tech Council*. [online]. 1 August 2025. Available at: https://www.globaltechcouncil.org/ai/china-launches-comprehensive-national-ai-strategy/.

ZAYAKIN, Andrey. 2025. Tightening loopholes: Russia finally sees sharp drop in restricted industrial imports propping up its military-industrial complex. *The Insider*. [online]. 10 April 2025. Available at: https://theins.ru/en/inv/280451

NEWS ARTICLES:

AP NEWS. 2017. Putin: Leader in artificial intelligence will rule world. [online]. 1 September 2017. Available at: https://apnews.com/article/bb5628f2a7424a10b3e38b07f4eb90d4.

REUTERS. **2023**. Sberbank CEO tells Putin of huge returns on its AI Investments. *Reuters* [online]. 19 July 2023. Available at: https://www.reuters.com/technology/sberbank-ceo-tells-putin-huge-returns-its-ai-investments-2023-07-19/.

TRUEMAN, Charlotte. 2024. Russia to invest $2.5BN on developing home-grown chip making equipment. *DCD* [online]. 5 October 2024. Available at: https://www.datacenterdynamics.com/en/news/russia-to-invest-25bn-on-developing-home-grown-chip-making-equipment/.

BEST ESSAY OF THE HIGHER COMMAND STUDIES COURSE (HCSC)

LTC Katrin TÕUGJAS: Breaking the Freeze: Russian Aggression in Ukraine Reshapes Moldovan-Transnistrian Dynamics

HCSC Writing Award

Supervisor: Dr. Dumitru MINZARARI

Use of AI Statement and Tools:

This research paper was prepared by me with some AI support to meet higher academic standards.

Tools: ChatGPT, Grammarly.

Purpose: content refinement/enhancement, grammatical fluency, and correction.
Process: ChatGPT assisted in identifying and reducing repetitive text, improving overall clarity and analytical precision of the research paper. The Grammarly app helped proofread the text by correcting grammatical and spelling errors and improving overall clarity and readability in English (UK).

Ownership: All conceptual structures originate in my personal investigation of academic publications and original sources. My intellectual contribution encompasses the analysis, breakdown, argumentation, and conclusions of academic articles and other resources. For academic accuracy and precision, I analysed AI-created suggestions. Overall decisions about content, build-up, and research logic were mine.

Introduction

The European Union (EU) and the Republic of Moldova face an increasingly complex security environment as Russia's full-scale invasion of Ukraine reshapes regional dynamics in Eastern Europe. Within this evolving context, Transnistria, the narrow strip beyond the Dniester River bordering Ukraine, remains Moldova's primary internal security challenge and Russia's lever for exerting influence over Moldovan domestic and foreign policy (Fylypenko, 2017).

When the Soviet Union collapsed, Transnistria remained unresolved for more than three decades and was often treated as a peripheral or 'managed' conflict in European security discussions (Belinschi, 2024). In 1990, this breakaway province declared its independence and after a brief but violent conflict in 1992, Transnistria became *de facto* autonomous (De Liedekerke, 2015). A ceasefire agreement, military coerced by Russia, signed by the presidents of Moldova and Russia, ended active hostilities, but Russian forces stayed in Transnistria as part of a peacekeeping mission (O'Loughlin, Kolossov, Tchepalyga, 1998, p. 334). Russia used two justifications for this military presence: one is to act as a so-called peacekeeping force and another is to protect the Cobasna arms depot, known as the Operational Group of Russian Forces (OGRF) (Shevchuk, 2023). Since 1997, the Organization for Security and Co-operation in Europe (OSCE) has sought to facilitate a political settlement through the so-called '5+2' format, but without durable success (OSCE, 2015).

In international relations theory, *de facto* countries rely on patron states for political, military, economic and social survival (Isachenko, 2010, p. 21). Since 1992, Russia's patronage has played a decisive role in sustaining Transnistria's institutions and insulating the region from reintegration into Moldova (Caspersen, 2009, p. 58). Over time, the enclave has been characterized as '[…] a "diplomatically isolated heaven" for transnational criminals and possibly terrorists, a "black hole" making weapons, ranging from cheap submachine guns to high-tech missile parts' (Isachenko, 2010, p. 1). For Moscow, Transnistria has functioned as a strategic foothold, an instrument for

maintaining influence in the Western post-Soviet space and constraining Moldova's Euro-Atlantic ambitions (Ukrinform, 2025).

Russia’s invasion of Ukraine in February 2022 marked a turning point in this long-standing situation. While the war initially heightened security concerns around Transnistria, it also constrained Russia's ability to sustain its traditional control mechanisms in the region. Military flexibility was reduced, economic patronage became limited, political legitimacy and social coherence within the separatist regime began to erode. As a result, this transformation has created a narrow but significant window of opportunity for Moldova and the EU to reassess the prospects for reintegration. Within this delicate geopolitical process, an important element to consider is the perceived personal risk that the Transnistrian elite feels from Moscow. A risk that can fuel the resistance or even armed backlash in any reintegration attempt. Between 2022 and 2025, constrained as it is by elite caution, Moldova's accelerating EU process has sought to exploit this strategic opening. Moldova accelerated dramatically when it moved from an ‘associated’ country to a partner ready to negotiate accession. EU documents repeatedly emphasise Moldova's territorial integrity and identify Transnistria as a source of instability not only for Moldova, but for the EU as a whole (Cenusa, 2026; European Council, 2025a). In this sense, Moldova's EU accession process has internationalised the Transnistrian issue, embedding it within the broader framework of European security and enlargement policy (Całus, 2023, p. 2).

Against this backdrop, this research paper addresses the main question: how has Russian aggression in Ukraine affected the prospects for Transnistria's reintegration into Moldova? To answer this question, the dynamics of the Russian influence in the separatist entity are analysed across the political, military, economic, and social domains, each of which has undergone changes since 2022. This paper argues that Russia's 2022 invasion of Ukraine has improved the prospects for Transnistria's reintegration into Moldova while simultaneously expanding Moldova's structural leverage over the region. However, reintegration remains constrained by the Transnistrian elites' acute fear of Kremlin retaliation, which will require credible and enforceable security guarantees as a precondition for any durable settlement.

The paper is organised into three chapters. The first chapter maps the identified shifts that have occurred since the outbreak of the Russian-Ukrainian war, allocating the discussion to the four domains. The second chapter analyses how these changes have reshaped dynamics in Transnistria and influenced relations with Moldova and the EU. Conclusions and future recommendations for the region's convergence are offered in the third chapter of this research paper.

Transformations in Transnistria since the outbreak of the war in Ukraine

'In 2025, the left bank of the Dniester River entered the deepest economic and social crisis in at least the last 25 years. Industry has collapsed, GDP has fallen dramatically, exports are at a historic low, and the population lives worse than a decade ago,' presented Veaceslav Ioniță, economic expert, in his analysis (Procopciuc, 2026). Moreover, the EU is concerned about the region's security and the presence of military forces in Transnistria, therefore the EU is keen to support conflict resolution to draw Transnistria more in line with Moldova and the West. Since 2022, Transnistria has transformed from a static frozen conflict into a more dynamic element in the EU-Russia strategic competition. This chapter explains the main shifts visible in Moldova's favor across the different domains.

Political domain

For a long time, political legitimacy in Transnistria has been created rather than earned. The regime survived on the basis of large turnouts in carefully controlled elections where there was little possibility of genuine opposition. Since 2022, this manufactured consensus has visibly collapsed.

The Freedom House poll indicates that Transnistria is not a democratic entity and non-citizens of Moldova cannot vote in Moldovan elections nor the democratic basis for their elite (Freedom House, 2025). In November 2025, a year-long electoral cycle began in Transnistria that will end with presidential elections in December 2026 (Smith, 2025). It is analysed that Transnistrian elections have made a deep curve: voter turnout has dropped from 78.6% in the 2006 elections to about 60% in the presidential elections of 2016, then to less than 30% in the 2020 legislative elections, and finally to a record low of 26% in 2025 (Vieru, 2025). In addition, as in non-democratic countries,

there is no room for a real opposition - 'voting without options' does not indicate stability but instead the authority over the administration (Dirun, 2025). Even minor dissent, such as a slogan at an FC Sheriff Tiraspol football match calling for fair elections, was quickly suppressed during the last elections. The main reason for that is the fear among the Transnistrian political elite of any overt European reorientation, as such a shift is perceived as a threat of retaliation from the Kremlin. In this sense, political paralysis is not only a product of authoritarian control but also a defensive strategy, as local decision-makers seek to avoid provoking Russian coercive measures. Consequently, for many individuals, non-participation is the sole form of 'protest vote' that carries minimal risk. Therefore, it is not a misinterpretation that the Ukrainian Foreign Intelligence Service is presenting the 2025 elections as an indication of a 'deepening gap' between the populace and the government in charge (Vieru, 2025). Such actions indicate growing cracks in the political system (Smith, 2025), which, in turn, is reinforced by the Russian military presence in the region.

Military domain

Before 2022, Russia's contingent of 1,500 troops and 20,000 tonnes of military equipment and armaments (Necsutu, 2022) in Transnistria served as a strategic deterrent, which prevented any Moldovan efforts at reintegration. The full-scale invasion of Ukraine has altered this calculus. Russia's peacekeeping forces in Transnistria are estimated as small, weak and poorly equipped with little combat experience (Deen, Zweers, 2022, p. 23) and the military significance of the ammunition depots at Cobasna is also likely minimal; the ammunition has either expired, been deported to Russia, or been illicitly sold (Baumgardner, 2022). This shift is caused by the impossibility to receive Russian logistical support or to rotate officers to Transnistria after Ukraine's border closure (Kubica, 2024, p. 22; Korshak, 2025). Without a Russian logistical network, the training of the troops also remained limited and unrealistic. Aside from a few enthusiasts, the Russian troops do not operate even hobby-sized drones, not to mention any operable aircraft or helicopter (Korshak, 2025). Furthermore, they likely choose local strategic interests over those of Russia (Baumgardner, 2022), because approximately 90% of the combatants are inhabitants of Transnistria (Deen, Zweers, 2022, p. 23). Consequently, soldiers are more motivated by financial compensation than by a sense of belonging (Foster, 2024, p. 123), and many would probably desert rather than engage in conflict (Deen, Zweers, 2022, p. 23). It is claimed

that 'Transnistria poses no concern for Moldova' (TCB, 2023) and Moldova's Prime Minister Dorin Recean described Russian forces in Transnistria as 'almost meaningless' (Korshak, 2025).

This operational decrease has strengthened diplomatic callings. Moldova's President, Maia Sandu, has persistently called for the withdrawal of Russian troops from Transnistria. 'We are an independent country that does not want foreign troops to stay on its territory,' she told reporters. 'This is not just a declaration; it is a necessity,' she added (BBC, 2020). A recent EU document has also called for an end to Russia's military presence and deployments in Moldova (Onea, 2026). Nevertheless, the Russian and Transnistrian administrations claim that the presence of this contingent is necessary to guard the ammunition depots at Cobasna and to maintain the peacekeeping mission in Transnistria (Hedenskog, 2022, p. 7). Officially, Russia continues to occupy the country, contrary to the populace's will and in violation of international regulations and principles (Miklasova, 2023, p. 11; Korshak, 2025) with the military called a 'force without a power', capable of the greatest utility in securing logistics and transportation (Korshak, 2025). Russia's diminished military capabilities have also been exacerbated by the collapse of economic patronage.

Economic domain

When Transnistria declared secession from Moldova, it retained the region's most robust economy. Transnistria accounted for 30% of the industry (Center for Strategic Studies and Reforms, 2005, p. 10) and compared to Moldova, Transnistria was wealthy.

Before the full-scale Russian-Ukrainian war, Transnistria was the hotbed for drug and arms trafficking, as well as nuclear materials (Rădulescu, 2006, p. 3). Trade data indicate that Russia and the EU formed the predominant portion of trade in 2020 and 2021. The primary share of Transnistrian goods went to Moldova and the EU. Nevertheless, Transnistria's largest import trade partner was Russia, accounting for 44% of total imports (Ministry of Economic Development of the Pridnestrovian, Moldavian Republic, 2021). After Ukraine closed its border in 2022, Transnistria was cut off from both its legal and illegal revenue streams. Now, Moldova is the only route for Transnistria to access the outside world (Yoko, 2024, p. 16) and trends indicate a

heightened importance of the EU and the Moldovan market for the region. In 2025, around 77% of Transnistria's exports were sent towards the EU and Moldova, and only 7% to Russia. Moreover, almost 50% of its imports originated from the EU (Government Republic Of Moldova, 2025).

Against this backdrop, the Moldovan authorities have used the situation to advance Transnistria's economic transition and strengthen customs inspections. The Moldovan government has required Transnistrian enterprises to remit a fee for customs processes that have irritated the Transnistrian authorities (Całus, 2023, p. 5), but also highlighted a new reality as Transnistrian companies require Moldovan approval to export and thereby affects the democratisation (Parmentier, 2024, p. 3). Additionally, the economic shift has created a dilemma for the Sheriff, Transnistria's dominant business conglomerate, regarding whether to align with Russia or pursue deeper cooperation with Moldova and the EU.

Gas was the instrument that Russia used to exert leverage over Transnistria. Russian cheap gas boosted the artificial competitiveness of Transnistrian producers by allowing them to manufacture and sell goods at reduced prices and gas gained approximately 60% of the region’s budget (Kieff, 2026). Weapons production, for example, was a strategy: 'The arms industry is one of the pillars of the Transnistrian economy, which is supported by Russian firms involved in arms manufacture in Transnistria' (MacLean, 2019). In January 2025, Transnistria encountered its most acute energy crisis in years. The sudden end of Russian gas supplies revealed the region's economy's critical vulnerability, and without this vital support, the area had to face its isolation (Byrne, 2025). The region's main power plant resulted in power interruptions, industries were shut down (Kieff, 2026) and the impact on the economy was drastic. During one year, the production fell by over 30% (Procopciuc, 2026) and exports dropped by around 60% (Kieff, 2026). The aid package of €60 million was provided then by the EU, demanded with progressive tariff rises, human rights advancements and political reforms for Transnistria to comply (Kovalenko, 2025). This shift, including Moldova's strengthened energy links and invested alternatives, has weakened Transnistria's bargaining power (Comai, Venturi, 2024). In principle, the system functioned as long as Russian support was continued. Alongside this economic situation, the social

sphere is reshaped by accelerating changes that further undermine the separatist regime's legitimacy.

Social domain

Population integrity, social well-being and loyalty are key factors for any country to ensure national stability, security, and future growth (Yevseiev et al., 2025, p. 33). In Transnistria, all three are now under strain. Developments in Transnistria's demographic situation indicate that it will enter the final stage of demographic decline. The *de facto* country's population has been dropping drastically already since the 1990s. According to the final Soviet census, Transnistria's population was 679,000 persons in 1989. By 2017, the population had decreased to 469,000 individuals. The most recent data confirm the long-term demographic decline, where Transnistria's population continues to decrease by around 465,800-375,000 people (Kemp, 2025). Some policy analyses estimate the real resident population to be as many as 350,000 people (Anisimova, 2024) and according to recent studies, the pensioners make up over 50% of them, reflecting a shrinking workforce and a growing dependency ratio (Całus, 2023, p. 6). Regarding Russian citizenship, it has always been allowed to possess multiple nationalities in Transnistria, which permits travel outside the *de facto* borders. Recent administrative data show an increase in the number of Transnistrians acquiring Moldovan citizenship – over 360,000 people registered as Moldovan citizens (Government Republic Of Moldova, 2024). Even if the people of Transnistria are continuously in Moscow's interest, the increasing integration with Moldova and migration to the EU jeopardise the future viability and influence of the *de facto* state. In addition to the above, in 2025, the average monthly salary in Transnistria is estimated to be half that in Moldova. The situation of pensioners is even more alarming: the average monthly pension in Moldova reached 4,200 lei, while in Transnistria it was under 1,900 lei, which is more than 2 times lower. Furthermore, real pensions increased by 2,5% in Moldova but decreased by 8,9% in Transnistria. Therefore, it is claimed that the real standard of living is similar to that of 25 years ago (Procopciuc, 2026) and there is a growing perception among the population that Transnistria has been abandoned by its traditional patron. Those deficiencies have created difficulties for households, leading many individuals to travel to Moldova to buy products that are 25% to 40% less expensive and available in a greater variety than in the Sheriff-controlled retail market of the separatist region. Public testimonies indicate widespread

dissatisfaction: 'It seems to me that Moldova is developing more [...]. Everything is lost here', one of the residents of the Transnistrian claimed (Gorbatovschi, 2025). As a result, Russia continues to influence Transnistrian society and maintain its impact, but growing dissatisfaction with living standards and declining trust in local authorities contribute to an identity shift in which Moldova appears more stable and prosperous. Taken together, these four domains reveal a pattern; each of Russia's traditional instruments of control has been weakened since 2022, setting the stage for the following analytical assessment.

Growing convergence between Transnistria and Moldova since 2022

This chapter examines how Russia's full-scale invasion of Ukraine in 2022 has reshaped dynamics in Transnistria and influenced relations with Moldova and the EU. Using a domain-based analytical approach, it identifies shifts that have weakened Russia’s traditional mechanisms of control and expanded Moldova's opportunities for maneuvre. The analysis draws on the calculus aspect across the four domains and explains how the Russian-Ukrainian war has disrupted established patterns of Transnistria's behavior so far and which new opportunities it has created for Moldova. Thus, it describes the factors shaping Transnistria’s current trajectory and the conditions for any future integration with Moldova.

Political calculus

'Moldova can find a gap to influence the region by paying attention to internal political legitimacy. Historically, Russia is the one that makes and controls the choices in Transnistria, and separatist leadership has maintained control through high turnout and tightly managed elections. Last election statistics indicate a deep demoralisation and loss of trust in the political system. It is a wake-up call, contemporary, while in 2006, the entire population confirmed its political course. This means that the Tiraspol leadership is no longer a strong and confident negotiator but rather an internally weakened structure. It is not just a matter of apathy reflex here; the belief persists that election results are preplanned and that participating has no effect on the individuals in power. While Russia still maintains a Kremlin-focused government and continues to stoke fear in the region, its position is now facing increasing criticism from the Transnistrian people, the Moldovan government, and international actors. A

weakened, demobilised electorate leaves the authorities in Transnistria with reduced political capital, making them less able to resist pressure from Moldova, although the consequentiality of this shift is debatable, given that it is an authoritarian regime and it explores coercion to keep popular protests under control. Negotiations now involve a fragmented authority apparatus struggling to maintain basic legitimacy. Concretely, declining electoral participation shifts the reintegration calculus in Moldova's favor: a Transnistrian leadership that commands the loyalty of only 26% of eligible voters that the regime's internal legitimacy is less than the official discourse suggests (Vieru, 2025). This creates a narrow but significant opening for Moldova and the EU to advance democratisation conditions as part of any negotiated settlement.

Military calculus

Russia's prewar 'security guarantee' gave Moldova little negotiating power; any attempt to alter the *status quo* was a risk of direct Russian retaliation. In military terms, Russia's influence in Transnistria still exists, but its practical capabilities have decreased. Although Russian troops remain in the region, Moscow's incapacity to secure logistical supply channels or troop rotations has left them operationally and strategically isolated. The closure of the Ukrainian border after 2022 transformed Transnistria from a so-called 'grey zone' into a controlled space where Russia can no longer covertly support its presence and the Russian soldiers' capabilities are low with outdated Soviet-era equipment. Certainly, this needs to be viewed against the limited military capabilities of Moldova, with a standing military force of 5,000-6,000 active military personnel. However, since the invasion of Ukraine, Moldova invested in the modernisation of its armed forces, backed up by the EU (European Council, 2025b) and therefore the practical implication for reintegration is significant: the military risk that historically paralysed Moldovan policy has decreased. Moldova can now pursue phased demilitarisation demands, starting with the Cobasna depot, without the same fear of triggering a Russian military response that limited earlier negotiating positions. It has also been concluded that in the event of a real conflict, many Russian soldiers, who are mainly local residents, would seek refuge in Moldova rather than resist. This supports the Moldovan security environment, indicating that the military capabilities in Transnistria cannot be considered reliable and the weakening of the Transnistrian military's cohesion is in Moldova's favor. That allows Moldova to articulate its security

interests, including calls for withdrawal and demilitarisation with far greater confidence and less fear of military escalation.

Finally, despite the operational constraints, Russia retains escalation capacity through hybrid strategies, long-range weapons (e.g., drones and ballistic missiles), as well as a persistent strategic posture; the combination of Russia's strategic weakening and Transnistria's internal decline in the military sector has created space for a more assertive position by Moldova for deeper integration into EU security frameworks.

Economic calculus

An even more pronounced shift has occurred in economic terms. Before 2022, the Transnistrian economy functioned on the back of Russian subsidies, free gas and the shadow economy; Moldova's influence was limited in the region. However, since the start of Russian-Ukrainian war in 2022, the entire basis of Transnistria's economic autonomy began to crumble, creating structural conditions that decreased Russia's influence (Belinschi, 2024). The most significant shift was Transnistria's isolation from Russian economic corridors. After the Ukrainian border was closed, the region lost the informal economic channels that supported the Transnistrian shadow economy. This culminated in a structural dependence on Moldova and now Transnistrian companies have to use Moldova's registration and customs system to export and meet the EU requirements. As a result, Moldova became the gatekeeper of Transnistria's access to the global market, increasing Moldova's economic control. Crucially, this structural shift changes the terms of any reintegration negotiation. Whereas before 2022, Moldova had little economic leverage over Transnistria, it now effectively controls Transnistria's access to export markets, energy mediation and financial lifelines. This asymmetry provides Moldova with a durable bargaining tool that does not require coercion to be effective.

The 2025 gas crisis further deepened this dependence. The disruption of Russian energy supplies led to a sharp decline in Transnistria's industrial production. In this new environment, Moldova became the only actor capable of mediating energy access. In practical terms, Moldova gained something it had never possessed - the veto power over Transnistria's energy security. Russia's inability to deliver gas and finance left the region without its traditional patron and further deepened Transnistria's

dependence on the West, complemented by the Moldovan and the EU financial support that Transnistria was ultimately forced to accept. This acceptance marked a symbolic concession: Transnistria could no longer rely solely on Russia for its economic survival and needed to cooperate with Moldova to avoid social collapse.

Finally, even though Russia is exerting strong influence over the Transnistrian government and elite, a critical factor is the shifting loyalties of the Sheriff conglomerate. The decision is challenging: maintain a shaky alliance with Russia or pursue negotiations with Moldova, which seeks EU membership. The Sheriff might maintain its significant assets through cooperation with Moldova and the EU to become a more respectable economic stakeholder (Sydorenko, 2025). Therefore, any convergence plan that fails to consider the Sheriff's networks of patronage would be inadequate (Plești, Kingston-Cox, 2026). The elite's access to the benefits of the EU accession process creates an opportunity for Moldova to exert indirect influence over Transnistria's internal dynamics in a way that was impossible before 2022.

Taken together, these developments represent a recalibration of dynamics. Russia may be able to exert indirect influence through well-established networks, energy leverage and elite ties that may make a full economic reorientation difficult, but Moldova has unique economic leverage, not through coercion, but through the structural dependencies that emerged once Russia could no longer sustain the separatist economy. The key for Transnistria will be to frame economic integration as a mutually beneficial partnership supported by EU-funded development.

Social calculus

The transformation of the social landscape of Transnistria after the Russian-Ukrainian war has not been as strong as in the economic domain. Nevertheless, changes in the social sphere are evident. The Russian-Ukrainian war has undermined the ideological foundations of the separatist regime, thereby weakening Russian identity and encouraging the population to integrate with Moldova.

While in previous years the social environment was characterised by a deeply rooted 'Russian world' identity, strict control over civil society, and demographic decline,

recent developments disrupted these structures and created new opportunities for Moldova to increase its influence. The decline in living standards in Transnistria since the start of the Russian-Ukrainian war is one of the most significant shifts in the social domain. Rising unemployment, falling wages and a dramatic decline in purchasing power have forced residents to seek affordable goods and services in Moldovan cities. Thus, a society that perceives better living standards on the Moldovan side becomes more receptive to reintegration narratives and less loyal to local elites. It reflects the social advantage based on credibility 'They are all beginning to understand that the future of this region is only as part of the Republic of Moldova,' said Moldovan deputy prime minister for reintegration (Gridina, 2024). Furthermore, even though many residents hold multiple passports, the growing importance of Moldovan citizenship creates a demographic landscape that is structurally linked to Moldova rather than Transnistria or Moscow. Furthermore, the separatist regime is unable to maintain a functioning society due to an aging demographic and significant labor mobility. The population of Transnistria is crucial to Russia, as it justifies the need to safeguard the inhabitants of a separated country. Thus, these are structural vulnerabilities that Moldova can exploit by presenting itself as a reliable partner in achieving long-term stability and development. The scale of these social shifts is captured in data. From the declining proportion of the population, 50% are pensioners and the separatist regime cannot sustain without external support (Całus, 2023). The economic divergence is equally sharp: the average pension is decreasing in Transnistria and creates a gap of more than two to one compared to Moldova (Procopciuc, 2026). These conditions have produced visible behavioral change. The number of Transnistrian residents registered as citizens of Moldova in recent years signals a demographic realignment. Together, these factors demonstrate that the social feasibility of reintegration has never been higher, even if the political conditions for it remain unresolved.

Finally, the cracks in the separatist identity system are expanding the impact of Moldova. The population's greater openness to alternative narratives, especially those promising social stability and a higher standard of living, reinforces Moldova's position. Russia still exerts a specific 'soft power' impact over the *de facto* state, and there are elements of pro-Russian identity influence on Transnistria, which slow down the pace of social transition; nevertheless, the social environment is more favorable to

convergence, not through force but through the daily experiences and choices of the population.

These developments should guide policymaking in the upcoming years. Overall, military, political, economic, and social developments show that after 2022, Transnistria has moved away from the Russian sphere of influence towards greater dependence on Moldova and the EU. The changes are not complete or irreversible, but Russia’s ability to control the region has diminished, while Moldova's influence has grown, primarily through structural, rather than coercive, mechanisms.

Conclusions and policy recommendations for Moldova and the EU

Despite the fact that Moldova's unofficial reintegration plan (Sydorenko, 2026) highlights the 'Russian Federation's propensity to use military force as a foreign policy tool,' and that 'Russia has not lost interest in the region [...]' (Solovyov, 2026), it would be misleading to view Transnistria as completely monolithic or subordinate to Moscow. Since the start of the Russian-Ukrainian war, Transnistria's position in the domains has changed significantly. In the political domain, the fear of retaliation from the Kremlin regime continues to haunt the Transnistrian elite, but political legitimacy has decreased, as evidenced by declining voter turnout and the growing disengagement of the public sector. Moreover, it has reduced the regime's ability to act as a confident negotiating partner. In the military domain, Russia still has a presence in Transnistria but its practical capabilities are limited. Russian forces have remained isolated; their operational effectiveness and logistical sustainability are constrained. As a result, Moldova now faces a much lower risk of military escalation. An even clearer shift is visible in the economic sector. In the pre-war times, the Transnistrian economy was largely dependent on Russian subsidies, cheap gas supplies, and informal trade networks. After the Ukrainian border closure and the gas crisis in 2025, the vulnerabilities of the region's economy were exposed and Transnistria is dependent more on Moldova and the EU, primarily for markets, energy and financial support. Moldova has gained unprecedented influence over trade flows, regulatory frameworks, and energy security. In the social sphere, changes have been somewhat more gradual, but no less significant. Prolonged demographic decline, economic hardship, and falling living standards have undermined the ideological foundations of the separatist regime.

Moldovan citizenship can help many Transnistrians to participate in Moldova's economic and social life. This fosters a growing perception of Moldova and the EU in general as a more stable and viable future. Taken together, these developments illustrate important changes. Russia's role has shifted from a dominant patron to a limited actor with the main focus on maintaining its shrinking foothold in the region. In contrast, Moldova, supported by the EU, has gained influence through structural dependencies rather than direct coercion. As a result, it is evident that Russian aggression in Ukraine has affected the prospects for Transnistria's reintegration into Moldova, but a successful reintegration plan has to address the fear of retaliation from Moscow while simultaneously demonstrating credible, enforceable guarantees that those elites will be safe under a Moldovan-EU framework.

Mutual recommendations for the EU and Moldova

For the feasible approach the EU and Moldova should implement the following recommendations: develop an internationally recognized 'special status' document granting Transnistrian elites and business leaders' immunity from prosecution for political crimes; expand consular support mechanisms for Transnistrian elites threatened abroad, to increase assurance without formal recognition; continue the pressure for the withdrawal of Russian forces, using international law and diplomatic channels; strengthen Moldova's security and resilience through EU cooperation; scale up the EU-Moldova Security and Defense Partnership to train Moldova military and security forces and last but not least, to continue to develop a comprehensive energy security strategy, including the use of renewable energy sources. These mutual recommendations should align with separate suggestions for Moldova and the EU.

Recommendations for the Republic of Moldova

On a political level, recommendations are the following: expand the rule of law and standards of human rights; establish inclusive participation in elections for Transnistrian citizens; link EU accession benefits to constructive engagement by Transnistria and form a working group to monitor developments in the Transnistrian area. Moldova should also negotiate gas debts in exchange for the withdrawal of troops and the prohibition of targeted threats to Transnistrian elites. In the military domain, Moldova should disband all Transnistrian military and security forces and integrate them into Moldovan institutions, also strengthen legal frameworks to support the

demilitarisation of the Cobasna depot. Economic recommendations include the implementation of 'strategic investment' in Transnistrian state-owned assets, with the elite retaining ownership and tying their wealth to a stable, EU system; phasing out of the privileges of the Tiraspol regime and integration of the businesses into the national budget, including the Sheriff conglomerate and consolidation of Moldovan customs procedures as the sole gateway for Transnistrian trade. The social domain includes the following suggestions: implement a program that allows for the relocation of at-risk individuals and provides a secure means of communication; accelerate the issuance of Moldovan passports, while preserving dual-citizenship options, and emphasise Moldova's role as a provider of stability and welfare. Also, address the decreasing demographic and aging population by establishing targeted pension and healthcare schemes financed through EU assistance.

Recommendations for the European Union

The EU should focus on tailored diplomatic, economic, and social measures to support Transnistria, including dedicated reintegration funds. Political suggestions are as follows: deploy a modest, transparent and non-combatant EU civilian security mission to the region, tasked with monitoring human rights violations and responding rapidly to threats by creating a visible safety net for the elite by the presence of EU observers; expand the EU's role from observer to active mediator in the settlement process, and increase the visibility of EU investments in the region. Military recommendations are to prepare for a possible international civilian mission to manage a post-demilitarisation transition when conditions permit. From an economic perspective, the EU should provide access to EU markets and strengthen cross-border trade facilitation by simplifying customs procedures; offer preferential for Transnistrian businesses and financial assistance. For social coherence, it is important to prioritise the welfare of Transnistria's residents; to intensify the dialogue between Moldova and Transnistria to support societal integration; to fund community development and projects that improve living standards and make the Moldovan side a visible source of stability; and last but not least, to support programs that address demographic decline and encourage diaspora return.

The Russian invasion of Ukraine has unintentionally created a strategic opportunity for Moldova to approach Transnistria. A well-developed reintegration plan is the key to

translating this opportunity into a viable settlement that ensures security, stability and credible guarantees for all stakeholders.

Bibliography

ANISIMOVA, Anna. 2024. Moldova's EU Integration and the Special Case of Transnistria. *Free Network*. [Online]. 13 October 2024. [Cited : 11 April 2026]. https://freepolicybriefs.org/2024/10/14/moldovas-eu-integration/.

BAUMGARDNER, Will. 2022. What Russia's Failed Coercion of Transnistria Means for the Annexation of Occupied Territory in Ukraine. *Critical Threats*. [Online]. 20 September 2022. [Cited : 11 April 2026]. https://www.criticalthreats.org/analysis/what-russias-failed-coercion-of-transnistria-means-for-the-annexation-of-occupied-territory-in-ukraine.

BBC. 2020. Moldova's new president calls for Russian troops to withdraw from territory. [Online]. 30 November 2020. [Cited : 11 April 2026]. https://www.bbc.com/news/world-europe-55135213.

BELINSCHI, Daniela. 2024. Transnistria: A Relic of Russian Imperialism at a Geopolitical Crossroads. *Maastricht Journal of Politics & Economics*. [Online]. 11 November 2024. [Cited : 10 April 2026]. https://www.pesmaastricht.com/post/transnistria-a-relic-of-russian-imperialism-at-a-geopolitical-crossroads.

BYRNE, Brianna M. 2025. Transnistria's Art of Survival: Navigating the 2025 Gas Crisis, GJIA. *Georgetown Journal of International Affairs*. [Online]. 23 April 2025. [Cited : 11 April 2026]. https://gjia.georgetown.edu/conflict-security/transnistrias-art-of-survival-navigating-the-2025-gas-crisis/.

CAŁUS, Kamil. 2023. Transnistria in the new international reality. *OSW Centre for Eastern Studies*. [Online]. 29 December 2023. [Cited : 10 April 2026]. https://www.osw.waw.pl/en/publikacje/osw-commentary/2023-12-29/transnistria-new-international-reality.

CASPERSEN, Nina. 2009. Playing the Recognition Game: External Actors and De Facto States. *The International Spectator*. 1 December 2009. Vol. 44, no. 4, pp. 47–60. DOI 10.1080/03932720903351146.

CENTER FOR STRATEGIC STUDIES AND REFORMS. 2005. Transnistrian Market and its Impact on Policy and Economy of the Republic of Moldova. [Online]. July 2005. [Cited : 11 April 2026]. https://www.cisr-md.org/reports/cont-mdtrans.html.

CENUSA, Denis. 2026. Reintegration with or without EU enlargement: Can Transnistria be co-opted in Moldova's EU accession process? *Geopolitics and Security Studies Center, GSSC*. [Online]. 22 January 2026. [Cited : 10 April 2026]. https://www.gssc.lt/en/publication/reintegration-with-or-without-eu-enlargement-can-transnistria-be-co-opted-in-moldovas-eu-accession-process/.

COMAI, Giorgio and VENTURI, Bernardo. 2024. Transnistria: when buying time, make sure to use it wisely. *Osservatorio Balcani Caucaso Transeuropa*. [Online]. 19 July 2024. [Cited : 11 April 2026]. https://www.balcanicaucaso.org/cp_article/transnistria-when-buying-time-make-sure-to-use-it-wisely/.

DE LIEDEKERKE, Artur. 2015. Putin's Foot in the Door: Why Transnistria Matters. *The International Affairs Review*. [Online]. 18 March 2015. [Cited : 10 April 2026]. https://www.iar-gwu.org/blog/2015/03/19/putins-foot-in-the-door-why-transnistria-matters.

DEEN, Bob and ZWEERS, Wouter. 2022. Walking the tightrope towards the EU. Moldova's vulnerabilities amid war in Ukraine [Online]. The Hague: Netherlands Institute of International Relations 'Clingendael'. [Cited : 11 April 2026]. https://www.clingendael.org/pub/2022/walking-the-tightrope-towards-the-eu/.

DIRUN, Anatolii. 2025. Parliamentary Elections in Transnistria: Internal and External Dynamics, Including Rising Tensions with Moldova and the Influence of Russia – De facto states research unit. [Online]. 27 November 2025. [Cited : 11 April 2026]. https://defactostates.ut.ee/parliamentary-elections-in-transnistria-internal-and-external-dynamics-including-rising-tensions-with-moldova-and-the-influence-of-russia/?lang=et.

EUROPEAN COUNCIL. 2025a. Joint declaration following the first Republic of Moldova - EU Summit - Consilium. [Online]. 4 July 2025. European Council. [Cited : 10 April 2026]. https://www.consilium.europa.eu/en/press/press-releases/2025/07/04/joint-declaration-following-the-first-republic-of-moldova-eu-summit/.

EUROPEAN COUNCIL. 2025b. European Peace Facility: Council adopts two assistance measures in support of Moldovan Armed Forces. *Consilium.* [Online]. 25

April 2025. [Cited : 28 April 2026]. https://www.consilium.europa.eu/en/press/press-releases/2025/04/24/european-peace-facility-council-adopts-two-assistance-measures-in-support-of-moldovan-armed-forces/.

FOSTER, Shaun D. 2024. 'Pridnestrovie for Peace': Accounting for Transnistrian Divergence from the Russian Position vis-à-vis the Russo-Ukrainian War. *Peace Review*. 2 January 2024. Vol. 36, no. 1, pp. 115–129. DOI 10.1080/10402659.2024.2311691.

FREEDOM HOUSE. 2025. Transnistria: Freedom in the World 2025 Country Report. *Freedom House*. [Online]. 2025. [Cited : 10 April 2026]. https://freedomhouse.org/country/transnistria/freedom-world/2025.

FYLYPENKO, Artem. 2017. The 'First Hybrid': The Transnistrian Conflict in the Context of the Russian-Ukrainian Conflict. *Ukraine Analytica*. [Online]. 29 September 2017. [Cited : 10 April 2026]. https://ukraine-analytica.org/the-first-hybrid-the-transnistrian-conflict-in-the-context-of-the-russian-ukrainian-conflict/.

GORBATOVSCHI, Marina. 2025. *S-a terminat cu ferestrele deschise pe timp de iarnă și cârnațul ieftin. Din Rîbnița, la cumpărături mai ieftine în Rezina. Reportaj ZdG. 'No more windows open in winter and cheap sausage. [From Ribnita, to cheaper shopping in Rezina. ZdG Report]* [Online]. [Cited : 11 April 2026]. https://www.zdg.md/stiri/video-s-a-terminat-cu-ferestrele-deschise-pe-timp-de-iarna-si-carnatul-ieftin-din-ribnita-la-cumparaturi-mai-ieftine-in-rezina-reportaj-zdg/.

GOVERNMENT REPUBLIC OF MOLDOVA. 2024. Over 360 Thousand Residents of the Transnistrian Region Are Citizens of The Republic of Moldova. [Online]. 25 July 2024. [Cited : 11 April 2026]. https://www.gov.md/en/comunicate-de-presa-bpr/over-360-thousand-residents-transnistrian-region-are-citizens-republic.

GOVERNMENT REPUBLIC OF MOLDOVA. 2025. The European Union Remains the Main External Economic Partner of Companies from the Transnistrian Region of The Republic of Moldova. [Online]. 10 July 2025. [Cited : 11 April 2026]. https://gov.md/en/comunicate-de-presa-bpr/european-union-remains-main-external-economic-partner-companies.

GRIDINA, Marina. 2024. Serebrian: More Transnistrian citizens apply for Moldovan citizenship. *Moldova*. [Online]. 29 February 2024. [Cited : 12 April 2026]. https://moldovalive.md/serebrian-more-transnistrian-citizens-apply-for-moldovan-citizenship/.

HEDENSKOG, Jakob. 2022. *How the EU can Reduce Russia's Exploitation of Moldova's Vulnerabilities* [Online]. [Cited : 11 April 2026]. https://sceeus.se/publikationer/how-the-eu-can-reduce-russias-exploitation-of-moldovas-vulnerabilities/.

ISACHENKO, Daria. 2010. The EU border mission at work around Transdniestria: a win-win case? *Societies Politiques Comparees*. [Online]. January 2010. [Cited : 10 April 2026]. https://fasopo.org/sites/default/files/article_n21.pdf.

KEMP, Simon. 2025. Digital 2026: Transnistria [Online]. [Cited : 11 April 2026]. https://datareportal.com/reports/digital-2026-transnistria.

KIEFF, Leah. 2026. Transnistria: A Conflict Unfrozen but Not Thawed. [Online]. 18 February 2026. [Cited : 11 April 2026]. https://www.csis.org/analysis/transnistria-conflict-unfrozen-not-thawed.

KORSHAK, Stefan. 2025. Explained: Russian Troops, Pro-Russian Forces in Moldovan 'Separatist' Transnistria Region. Kyiv Post. [Online]. 25 September 2025. [Cited : 11 April 2026]. https://www.kyivpost.com/post/60871.

KOVALENKO, Nikita. 2025. On borrowed time. How Transnistria is coping without the transit of Russian gas via Ukraine. *Novaya Gazeta Europe*. [Online]. 24 December 2025. [Cited : 11 April 2026]. https://novayagazeta.eu/articles/2025/12/24/on-borrowed-time-en.

KUBICA, Lucjan. 2024. Hybrid CoE Working Paper 28: Moldova's struggle against Russia's hybrid threats: from countering the energy leverage to becoming more sovereign overall. *Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats*. [Online]. January 2024. [Cited : 11 April 2026]. https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-28-moldovas-struggle-against-russias-hybrid-threats-from-countering-the-energy-leverage-to-becoming-more-sovereign-overall/.

MACLEAN, Rory. 2019. *Pravda Ha Ha -Truth, Lies and the End of Europe*. [Online]. 1. London: Bloomsbury Publishing. [Cited : 11 April 2026]. https://www.bloomsbury.com/us/pravda-ha-ha-9781408896549/.

MIKLASOVA, Julia. 2023. Status of Transnistria Under International Law. In: *Global Encyclopedia of Territorial Rights*. ISBN 978-3-319-68846-6.

MINISTRY OF ECONOMIC DEVELOPMENT OF THE PRIDNESTROVIAN and MOLDAVIAN REPUBLIC. 2021. *Результаты внешнеэкономической деятельности. [Results of foreign economic activity].* [Online]. 19 November 2021.

Ministry of Economy and Development of the Pridnestrovian Moldavian Republic. [Cited : 11 April 2026]. https://mer.gospmr.org/search/Результаты внешнеэкономической деятельности.

NECSUTU, Madalin. 2022. Ukraine Crisis Sparks Anxiety in Moldova, Institute for War and Peace Reporting. [Online]. 1 March 2022. [Cited : 28 April 2026]. https://iwpr.net/global-voices/ukraine-crisis-sparks-anxiety-moldova.

O'LOUGHLIN, John, KOLOSSOV, Vladimir and TCHEPALYGA, Andrei. 1998. National Construction, Territorial Separatism, and Post-Soviet Geopolitics in the Transdniester Moldovan Republic*. Post-Soviet Geography and Economics*. 1 June 1998. Vol. 39, no. 6, pp. 332–358. DOI 10.1080/10889388.1998.10641081.

ONEA, Oleg. 2026. The European Union calls for an end to the Russian military occupation of Transnistria. *Cotidianul.* [Online]. 23 February 2026. [Cited : 11 April 2026]. https://cotidianul.md/en/25924/The-European-Union-calls-for-an-end-to-the-Russian-military-occupation-of-Transnistria./

OSCE. 2015. OSCE Mission to Moldova. [Online]. 10 December 2015. [Cited : 11 April 2026].
https://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede140715oscemissionmoldova_/sede140715oscemissionmoldova_en.pdf.

PARMENTIER, Florent. 2024. Transnistria, in the shadow of the war in Ukraine. *Institut Jacques Delors*. [Online]. 15 May 2024. [Cited : 11 April 2026]. https://institutdelors.eu/en/publications/transnistria-in-the-shadow-of-the-war-in-ukraine/.

PLEȘCA, Laurențiu and KINGSTON-COX, Will. 2026. Transnistria: Pain-Free Reintegration?. *German Marshall Fund of the United States*. [Online]. 11 March 2026. [Cited : 12 April 2026]. https://www.gmfus.org/news/transnistria-pain-free-reintegration.

PROCOPCIUC, Maria. 2026. Analiză: Stânga Nistrului traversează cea mai gravă criză economică și socială din ultimii 25 de ani. Analysis: The left bank of the Dniester is going through the worst economic and social crisis in the last 25 years. *IDIS.* [Online]. 6 February 2026. [Cited : 10 April 2026]. http://viitorul.org/ro/content/analiz%C4%83-st%C3%A2nga-nistrului-traverseaz%C4%83-cea-mai-grav%C4%83-criz%C4%83-economic%C4%83-%C8%99i-social%C4%83-din-ultimii-25.

RĂDULESCU, Bogdan-George. 2006. The 'Transnistria Republic' and its illegal arms export - a major security risk. In: 1 June 2006.

SHEVCHUK, Nina. 2023. Role of Russian Peacekeeping in the Pridnestrovian Settlement Process. *ResearchGate*. June 2023. Vol. 23, no. 2, pp. 228–240. DOI 10.22363/2313-0660-2023-23-2-228-240.

SMITH, David. 2025. Transnistria's Last 'Election?' [Online]. 3 October 2025. [Cited : 11 April 2026]. https://www.moldovamatters.md/p/transnistrias-last-election.

SYDORENKO, Sergiy. 2025. Moldova's quiet push for Transnistria's reintegration: a new chapter unfolds. [Online]. 10 October 2025. [Cited : 12 April 2026]. https://eualive.net/moldovas-quiet-push-for-transnistrias-reintegration-a-new-chapter-unfolds/.

TCB. 2023. Приднестровье не угроза для Молдовы и Украины. [Transnistria is not a threat to Moldova and Ukraine]. [Online]. TCB, [Cited : 11 April 2026]. https://www.youtube.com/watch?v=oqZgVKlPiKA.

UKRINFORM. 2025. Russia to retain influence over Transnistria, outcome tied to war in Ukraine — Moldovan ambassador. [Online]. 10 October 2025. [Cited : 10 April 2026]. https://www.ukrinform.net/rubric-polytics/4045952-russia-to-retain-influence-over-transnistria-outcome-tied-to-war-in-ukraine-moldovan-ambassador.html.

VIERU, Vadim. 2025. Analysis Article: 26% turnout in the Transnistrian region: how the erosion of a regime that formally never loses elections looks. *Promo-LEX*. [Online]. 8 December 2025. [Cited : 11 April 2026]. https://promolex.md/en/analysis-article-26-turnout-in-the-transnistrian-region-how-the-erosion-of-a-regime-that-formally-never-loses-elections-looks-lik/.

YEVSEIEV, Serhii, MILEVSKYI, Stanislav, MELENTI, Yevhen, VOITKO, Oleksandr, ALEKSIEIEV, Mykhailo, et al. 2025. Development of a method for assessing the society national security level based on the triple helix concept. *Eastern-European Journal of Enterprise Technologies*. 30 August 2025. Vol. 4, no. 4 (136), pp. 32–45. DOI 10.15587/1729-4061.2025.337398.

YOKO, Hirose. 2024. The Transnistria Problem and the Crisis in Ukraine: Analysis from the Perspective of the Security Dilemma Argument. *Asia-Pacific Review*. 1 March 2024. Vol. 31, no. 1, pp. 64–101. DOI 10.1080/13439006.2024.2329500. 178298011.

LTC Peter CUDERMAN: Serbia as a Strategic Hub for China–Russia Influence in the Western Balkans: Implications for NATO and EU Security Policy

Supervisor: Mr. Louis WIERENGA

Statement on the use of AI:

Copilot was used as a challenging partner to validate the cited source content with other sources to confirm data authenticity and for searching online available sources to support the structure and content of the Research Paper. ChatGPT 5.4. was used as a tool in the structure frame build and for language optimisation. AI was not used to generate text. Grammarly was used as a grammar and spelling tool. Google Translate was used to translate from source languages other than English (Serbian, Croatian, Slovene and Polish) to English.

1. Introduction

On 30 January 2024, Russian President Vladimir Putin awarded the Order of Friendship to former Director of the Serbian Security and Intelligence Agency (BIA), Aleksandar Vulin. He was honoured ‘for his significant contribution to the development and improvement of cooperation between the BIA and the Foreign Intelligence Service of Russia (SVR) in ensuring state security and defending the national interests of Serbia and Russia’ (Grković, 2024). Only six months earlier, the United States Treasury sanctioned Mr Vulin for alleged ties to narcotics trafficking networks and Russian intelligence services (US Department of the Treasury, 2023).

An episode with deliberate timing that shows how Serbia is actively managing relationships with Russia and China whilst pursuing its ambition for European Union (EU) membership. After the 1999 NATO bombing of Yugoslavia, Serbia developed a strong pro-Russian and anti-Western sentiment among its citizens. Consequently, Serbian authorities rely on Russian and Chinese support for their foreign policy, security and economic interests. In contrast, Serbia remains committed to its path to EU membership and maintains defence cooperation with Western countries.

The Western Balkans present a chronic political and security challenge to the West. Trapped in what the International Institute for Strategic Studies (IISS) describes as ‘controlled instability’, as a state where external actors and local elites maintain permanent tension to delay Euro-Atlantic Integration (MIA, 2024, p. 92). At the centre of it stands Serbia. A country that has become a strategic hub for converging Russian and Chinese interests in Europe. Successfully resisting the choice between East and West, Serbia has for years shown reluctance to integrate into Euro-Atlantic structures and is viewed as an anti-Western ‘little Russia’ in the Balkans. (Petrović, 2024, p. 7).

Such foreign policy, where the nation deliberately avoids full geopolitical alignment with any single major power, maintaining a middle path between the European Union (EU), Russia, and China, Jović-Lazić identifies as ‘Strategic Ambiguity’. She describes it as a deliberate posture designed to neutralise Western conditionality whilst preserving

optionality with Moscow and Beijing (Jović-Lazić, 2026, p. 4). In this framework, Belgrade has successfully positioned itself as indispensable to regional peace while, at the same time, remaining a source of that instability.

‘Serbia's stance has undermined EU unity and the credibility of its enlargement policy, and EU leaders are increasingly intolerant of a candidate aligning with EU foreign policy only 45% of the time’ (Jović-Lazić, 2026, p. 89).

The numbers for 2024 are staggering, since more than two-thirds of Serbian citizens express positive views of Russia. Natasya Styczyńska argues that ‘Serbo-Russian friendship’ is not an organic cultural phenomenon but a politically constructed myth that emerged in the Milošević era as a product of state-influenced media and political rhetoric, sealed in with Serbia's anti-NATO and anti-Western rhetoric, caused mainly by the 1999 NATO bombings and the activities of the Hague Tribunal (Styczyńska, 2024, p. 9). This opened the window for renewed Russian influence in the region, which Western institutions have consistently misread as authentic popular preference rather than elite driven narrative construction.

The question guiding this paper is, to what extent does Serbia's deliberate strategic ambiguity function as an enabling regional hub for Russian and Chinese influence in the Western Balkans, and what are the implications for NATO's and the EU's policy coherence? But first, how has Serbia's policy of strategic ambiguity evolved since 2014 as a mode of balancing between domestic and foreign policy related to the EU, NATO, Russia, and China? Serbia's strategic ambiguity requires infrastructure and economic dependencies, institutional arrangements and political networks that make balancing between East and West profitable. Serbia is not only a subject of Russian and Chinese influence in the Western Balkans. It serves as an enabler to Russian political and security influence, as well as to Chinese geoeconomic and technological influence across the Western Balkans.

Belgrade's strategy of deliberate strategic ambiguity, balancing EU aspirations, NATO cooperation, Russian ties, and Chinese investment, emphasises Serbia's ability to extract political, economic, and security benefits from competing powers. This ambiguity weakens Western leverage, as Russian links and Chinese technology

projects create dependencies that the EU struggles to address. The result is not only that Serbia is not being aligned with the West, but also that a coordinated EU-NATO policy is being developed to address the challenge of Serbia's role as an active strategic balancer rather than a passive arena of external influence.

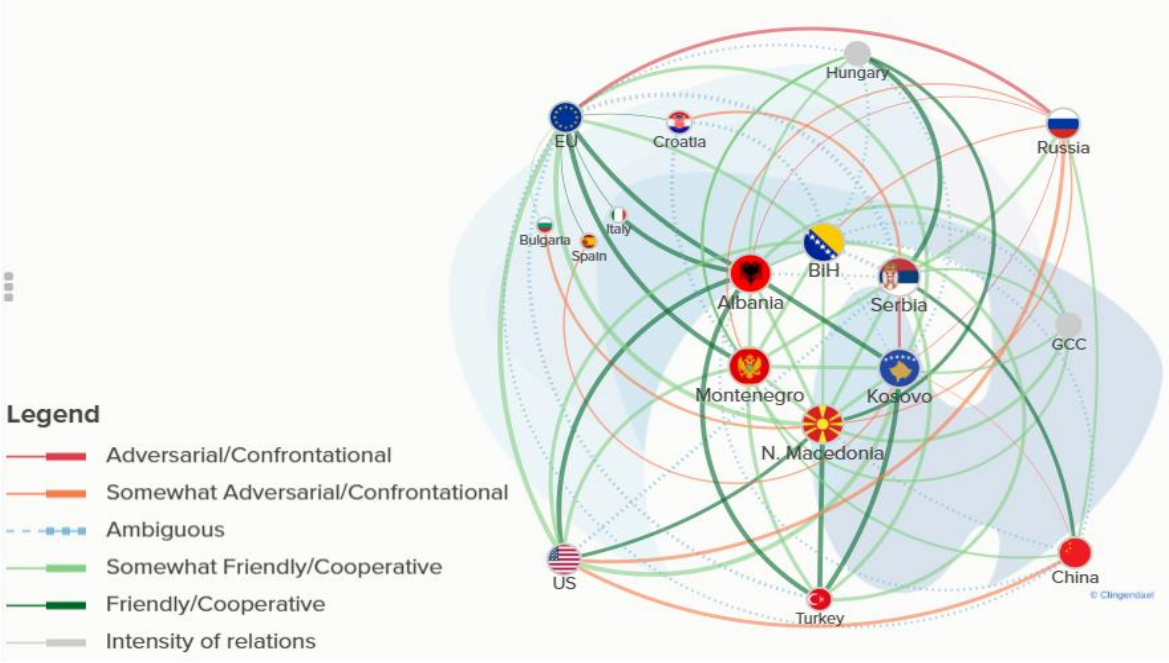

Figure 1: *A geopolitical mapping of the Western Balkans. (Zweers, W. and Kelečević, I. 2025).*

2. The Strategic Ecosystem: Serbia, Russia and China

Understanding this ecosystem requires abandoning the assumption that external influence operates primarily through direct bilateral pressure. In the case of Serbia, we can see something more sophisticated. A layered architecture where energy and technological dependencies, intelligence networks, and transnational business channels represent constraints on policy autonomy. Russian disruption and Chinese construction operate within Serbia itself, but their effects radiate outward through the strategic ecosystem, extending beyond Serbia's borders through ‘Srpski svet’ mobilisation in neighbouring states; a transmission channel that carries influence into the European Union. Serbia is not merely a recipient of external influence; it functions as a hub within a regional architecture of controlled instability.

The development of the ‘Srpski svet’ (Serbian World) project, a smaller counterpart to the ‘Russkiy mir’ (Russian World), exemplifies how Russian ideas have been adapted for local purposes. In 2021, Serbian Interior Minister Aleksandar Vulin, a veteran

politician from the Milošević era, was put in charge of promoting this new concept. The Serbian World aims to create a ‘United Serbian World’ (Ujedinjenii Srpski Svet), advocating for the unification of Serbs in the region to protect their identity, language, culture, and history, with Belgrade as the central decision-making capital (Styczyńska, 2024, p. 2). This idea serves as the ideological glue that holds the ecosystem together by framing regional integration as a matter of cultural and national survival. For example, this cultural narrative provides the necessary public support to sustain the ‘strategic ambiguity’ toward Russia and China, while simultaneously weakening the institutional role of NATO's 4,500 Kosovo Force (KFOR) troops.

2.1. The Balancing Act - Strategic balancing as an institutional practice

How has Serbia's policy of strategic ambiguity evolved since Russia annexed Crimea (2014) and after the ‘shock’ of 2022? As a means of balancing between domestic and foreign policy-related geostrategic players, Serbia's strategic ambiguity requires dependencies, arrangements, and networks that make balancing between East and West profitable. This chapter focuses on the two main subjects of the ‘Balancing Act’. The Chinese economic penetration and the Russian political influence, both representing the precondition under which Belgrade can sustain its ‘Strategic Ambiguity’.

Figure 2: President Vučić’s Strategic Balancing. Image created with ChatGPT 5.4.

The Russian invasion of Ukraine in 2022 proved a watershed moment for Serbia's foreign policy, stress-testing its strategy of strategic ambiguity. On one hand, Serbia surprised some observers by joining the UN General Assembly votes condemning Russia's violation of Ukraine's territorial integrity. This represented perhaps the maximal anti-Russian step Serbia felt it could take, a largely symbolic act, given that the UNGA resolution carried no enforcement power, which signalled to the EU that Serbia was not fully endorsing the invasion (Jović-Lazić, 2026, p.87).

Belgrade has increasingly adopted a posture of strategic ambiguity, a foreign policy of ‘not choosing sides’, as President Aleksandar Vučić himself stated when pressed about aligning with Western sanctions on Russia. This approach has seen Serbia endorse EU integration in principle while pragmatically hedging its bets: refusing to join Western sanctions on Russia, embracing Chinese investment, and declaring military neutrality even as it conducts joint drills with NATO and receives arms from Russia (Jović-Lazić, 2026, p.79).

This analysis identifies a connective tissue between Chinese investment and Serbian domestic politics, defined as ‘corrosive capital’. Such capital operates through distinctive legal and regulatory instruments also known as ‘*lex specialis’*, where corrosive practices are assessed across rule-making, rule implementation, and accountability suppression, showing how repeated elite actions have manipulated environmental assessments, media capture, and the amplification of polarising narratives (Prelec, 2025, p.34).

These are not incidental features of foreign investment. They are structural requirements for maintaining the political economy of strategic balancing. In 2025, Serbian president Aleksander Vučić discovered that domestic audiences may prove harder to balance than foreign ministries. In late 2024, a student-led protest marked one of the largest civic mobilisations that occurred in Serbia following the Novi Sad station tragedy, where the canopy of the newly renovated station collapsed and killed 16 people. Instead of responding with immediate actions and empathy toward the victims, the ruling party launched a coordinated disinformation campaign (Prelec, 2025, p. 58).

Framing the protests as a Western-backed colour revolution contributed to weakening already low public support for EU integration in Serbia. Although the European Commission later voiced support for student demands, the government worked to downplay this support and prevent it from resonating with the wider public. In aftermath, a public opinion survey, showed that many Serbs believe their country has other alternatives instead of joining the EU; 30% favour cooperation with non-EU countries, while 51 percent prefer pursuing neutrality (Prelec, 2025, p. 44). Their perception is that the US (12%) is the greatest threat to Serbia's national security, followed by

Albania (9%) and England (8%) and EU member states such as Croatia (6%) and Germany (5%) (Prelec, 2025, p. 46). Another indicative result is the Serbian disposition toward Russia, with 36 percent of the citizens identifying with common values and ideas, compared to only 18 percent of the population oriented towards EU values and ideology and only two percent feeling close to the US in terms of values and ideas (Prelec, 2025, p.58).

Serbia's geopolitical ambivalence is part of the regime's foreign policy but also deeply embedded domestically. Since Vučić came to power, the government-controlled media have deliberately promoted an anti-Western narrative, with Russia and China appearing in an overwhelmingly positive light. At the same time, the tabloid media often points fingers at neighbouring states and the West as potential threats.

Serbia's selective compliance is not random. It reflects a calculated assessment of which EU positions can be endorsed without jeopardising Chinese economic relationships or Russian political support. Strategic ambiguity is often seen as a short-term adjustment by smaller states facing great-power rivalry. In Serbia, however, it has evolved into a stable governing strategy within the framework of European Union accession (Jović-Lazić, 2026, p.79).

2.2. China: The economic anchor and ‘corrosive capital’

How is China using its geoeconomic and technological influence in Serbia, and how does this differ from Russian influence? Serbia's development model is heavily reliant on foreign direct investment (FDI), which hit $6.6 billion in 2024. Serbia continues to declare its commitment to European Integration, yet its growing dependency on Chinese capital suggests an alternative path, one less anchored in institutional reform and democratic norms (Vladisavljev, 2025, p. 6).

Macroeconomically, a valid question would be, how much money has China actually given to Serbia? In her 2025 article for the Serbian Monitor titled How much does Serbia owe China, Rakić (2025) used data from the Serbian Chamber of Commerce and stated that Chinese investment in Serbia has reached approximately 10,3 billion euros, representing 22% of national GDP. This figure alone shows the strategic

significance of Chinese capital in extractive industries, heavy manufacturing, and critical infrastructure, creating Serbian dependence. When a single foreign actor controls such a substantial portion of copper production, steel manufacturing, and railway construction, the relationship transcends commerce. It becomes structural and strategic (Rakić, 2025, p. 5). Until 2022, China was Serbia's second largest development partner. Between 2000 and 2022, China's official sector lenders and donors provided grant and loan commitments worth $7.7 billion across 121 projects and activities in Serbia. As shown in Figure 1, Serbia's portfolio is overwhelmingly dominated by non-concessional loan commitments, with very little aid such as grants, concessional loans, or in-kind donations committed from China over this period (Sickell, 2025, p.5).

In 2018, Zijin Mining acquired a majority stake (63%) in the RTB Bor copper complex, while Shandong Linglong invested approximately $1 billion in a new tyre manufacturing plant in Zrenjanin. Through the '*lex specialis*' legislation, Zijin operations are exempt from standard environmental impact assessments and local planning approvals. Copper exports, largely driven by the activities of the Bor and Majdanpek complexes, account for more than half of Serbia's exports to China, pointing to a dependency in which Serbian exports are tied to Chinese invested assets in Serbia. (Vladisavljev, 2025, p.10). The consequences for local communities have been severe. Environmental protests in Bor and surrounding villages documented elevated pollution levels, water contamination, and respiratory health impacts, but with little media or political attention. The Hesteel acquisition of Smederevo steelworks follows a similar pattern. The 2016 purchase was framed as saving 5,000 jobs in a politically sensitive region. The regulatory arrangements accompanying the deal, however, established precedents that subsequent Chinese investments would exploit. (Vladisavljev, 2025, p.8).

In 2023, Serbia exported goods worth roughly $1.1 billion to China, while imports from China reached nearly $5 billion. Industrial machinery, electronics, telecommunications equipment, motor vehicles, and consumer goods dominate exports to Serbia. Conversely, Serbia's exports to China are primarily copper and related mineral products, agricultural goods such as frozen fruits and cereals, and, to a lesser extent, timber (Vladisavljev, 2025, p. 10).

‘Corrosive capital’ does not merely weaken institutions; it restructures local political economies to make opposition costly and compliance rewarding. In the case of Zijin Mining operating in Serbia, a single employer dominates the local labour market and operates under Serbian political protection. The result is a community unable to resist the economic hegemon. The Serbian ‘corrosive capital’ model can also be seen in other Chinese investments in Serbia, such as the Belgrade-Budapest railway. A practice that contradicts EU norms, influencing Serbia's process of joining the EU, particularly by closing Chapter 23 on Judiciary and Fundamental Rights and Chapter 24 on Justice, Freedom, and Security. The EU accession process requires candidate countries to demonstrate commitment to the Copenhagen Criteria, which emphasise democratic governance, transparency, and the rule of law. Serbia's deepening relations with China, particularly in infrastructure projects financed through ‘corrosive capital’, raise questions about Serbia's economic transparency, rule of law, and corruption levels (Vladisavljev, 2025, p. 15).

Serbia is maintaining a strong Yugoslav defence industry complex. This complex enables the Serbian Armed Forces to continue to operate former Yugoslav National Army-inherited legacy weapons systems and also supports the Serbian Military's transition to Western Military standards. In the last five years, we have witnessed the Serbian MoD defence procurement focusing on the technological dimension, bolstering its precision-strike capacities, drones, air defence systems and sensor technology. In 2022-2023, Serbia took delivery of the FK-3 surface-to-air missile system and acquired the HQ 17AE Air defence missile system, designed for medium to short-range engagement (Vladisavljev, 2025, p.18). CH-92A unmanned combat aerial vehicles (UCAV) add a further layer of complexity. These systems provide Serbia with strike capabilities previously absent from its inventory. Their deployment near Kosovo creates surveillance and potential strike options that KFOR planning must now accommodate. These are not neutral purchases. These procurements have created a technological dependency, where NATO interoperability seems structurally impossible, with core systems operating on Chinese technical standards, requiring Chinese maintenance support and dependent on Chinese supply chains for spare parts and upgrades. This is how the Chinese military creates an interoperability issue with NATO. The choice is not accidental. Seeking technological modernisation for

Serbian defence and security, Serbia-China cooperation has expanded to include arms sales, defence training, strategic agreements, and the adoption of Chinese surveillance technology in Serbian cities (Vladisavljev, 2025, p.17).

Another major dimension of Serbia–China security cooperation is the deployment of Chinese surveillance and ‘Smart-City’ technology in Serbia. Through the ‘Smart-City’ surveillance project, Chinese companies are deeply involved in Serbia's telecommunications and digital infrastructure, which presents both opportunities and cybersecurity risks. Telekom Srbija relies on Huawei equipment for Serbia's 3G/4G mobile network hardware and is integral to Serbia's fibre optic broadband network. This extensive Chinese role in digital infrastructure means that a significant portion of Serbia's communications backbone is running on Chinese technology. From cellular networks to surveillance systems to data centres, Chinese tech is deeply integrated into Serbia's digital ecosystem, serving as a testament to the Digital Silk Road component (Vladisavljev, 2025, p. 19). Huawei systems utilise proprietary protocols for data transmission and storage. This creates potential intelligence collection possibilities that extend well beyond stated public safety objectives. The integration of facial recognition, vehicle tracking, and communications monitoring, represent capabilities that authoritarian governance finds useful and acceptable, democratic governments, on the other hand, find them challenging. When such systems are provided by a state, that explicitly rejects Western conceptions of privacy and civil liberties. Concerns regarding this topic were raised not only in Serbia but also in the EU. Since Serbia is a candidate for accession to the EU, the ‘Safe City’ project raised national security concerns in the European Parliament about ‘China's penetration into Europe’, in a project where Huawei actively participates in more than 120 cities and more than 40 countries in the process of developing ‘Smart Cities’. Although Huawei is a private company, the Chinese Communist Party has selected it as a national champion for developing homegrown telecom equipment. The US government has blocklisted the company over its ties to the Chinese military and concerns that its equipment could be used for espionage (Tal, 2025, p. 74).

Belt and Road Initiative projects in the infrastructure and technology sectors reinforce Serbia’s dependence through financial mechanisms. The Budapest-Belgrade railway exemplifies a debt trap dynamic. This is reflected in the approach of loan conditionality

favouring Chinese contractors, limiting transparency regarding terms, and imposing long repayment periods. The absence of European standard conditionality makes Chinese capital attractive to Serbian elites. Corrosive capital flows precisely because it corrodes the institutional requirements that democratic governance demands.

2.3. Russia: Political destabilisation

To answer the question of how Russia is exercising its political and security influence in and through Serbia, we need to understand that Russia's strategic objective in the Western Balkans is not territorial acquisition. Russia pursues its objectives through energy dependency, intelligence penetration, and the mobilisation of the Serbian diaspora across the region.

Energy dependency and strategic capture are Russia's primary structural leverage, and it has no issue weaponising them to ensure Serbia's strategic loyalty. The relationship based on energy sources constitutes Russia's strongest strategic influence. The 2008 sale of Naftna Industrija Srbije (NIS) to Gazprom Neft established a dependency relationship through a 56.15% majority stake, which controls the country's only oil refinery. On 19 January 2026, the Hungarian Oil Company MOL announced that it had signed a binding Heads of Agreement to acquire Gazprom Neft's 56.15% stake, but the transaction remained subject to regulatory and sanctions-related approvals. This reduction of Russia's direct leverage raises a new question: to what extent will Hungarian commercial interests substitute for Russian political ones?

Serbia's political landscape is notably marked by the enduring allegiance towards Russia, spearheaded by the nation's President Aleksandar Vučić. The depth of this political camaraderie can be seen in the case of the former pro-Russian head of the Serbian Security and Intelligence Agency, BIA (Bezbednosno informativna agencija), Mr Aleksandar Vulin.

Vulin: '*Unification of Serbs is the Path to Peace in the Balkans'*
(Petrović, 2024, p.14)

The Serbian World is a concept that has been present among political and cultural elites, as well as nationalist circles, in Serbia since the mid–19th century. However, this term only began to attract attention from the domestic and regional public in 2020 when Aleksandar Vulin, the then Minister of Defence, began using it regularly during public appearances.

In recognition of his significant personal contribution to strengthening cooperation between BIA and Russian security intelligence services in protecting the national interests of Serbia and Russia, Vulin was awarded honours by both the FSB and SVR. The second honour, the Order of Friendship, was presented to Vulin by President Putin himself (Petrović, 2024, p.25).

From 24 February 2022, ‘Serbia has become a fertile ground for the Russian state presence and the spread of the Russian war propaganda. Serbia's refusal to join the EU sanctions against Russia enabled it to remain a safe destination for Russian diplomats expelled or blacklisted by EU member states for espionage’ (Cvijić, 2025, p. 11). By the end of December 2024, the Serbian Foreigners Administration, the primary authority for legalising stay and processing formal applications, had received 73,197 applications for temporary residency from Russian immigrants, of which 67,236 were granted (Cvijić, 2025, p. 13).

Russian influence in Serbia operates through channels designed not to build but to disrupt, not to integrate but to fragment. The Orthodox Church serves as one such channel; the other is the Serbian diaspora throughout Europe. Russia's relationship with Serbia provides the Kremlin with an instrument of regional strategic influence through the Serbian diaspora communities distributed across the Western Balkans, which Moscow can mobilise to destabilise Kosovo, Bosnia and Herzegovina, Montenegro, as well as countries in the EU and NATO with significant Serbian populations. This influence is most operationally obvious in Russia's relationship with Republika Srpska in Bosnia and Herzegovina. Bosnian Serb leader Željka Cvijanović and, previously, Milorad Dodik, have systematically obstructed state institutions and the authorities set by the framework agreement for peace in Bosnia and Herzegovina, signed in Dayton, Ohio (Dayton Accords). Threatening secession and refusing implementation of Constitutional Court decisions are just a few actions that serve

Russian interests. The September 2023 Banjska incident could have led to a larger armed conflict between Serbia and Kosovo. At that time, around 30 armed and uniformed Serbs from northern Kosovo set up barricades to launch an armed uprising. A conflict soon ensued between the group and the Kosovo police, resulting in the death of one Kosovar police officer and three Serbs. Kosovo authorities claimed that this was an attempt by Serbia, backed by Russia, to destabilise the region by trying to annex North Kosovo, like Russia's actions in Crimea. (Petrović, 2024, p.11).

The ‘Srpski svet’ (Serbian World) concept illustrates its disruptive potential. Vučić has instrumentalised this ethno-nationalist framework to justify interference in Montenegro and Bosnia-Herzegovina, framing Serbian minorities abroad as populations requiring Belgrade's protection (Styczyńska, 2024, p. 18). The parallels with Russian ‘compatriot’ policies are not coincidental. They represent ideological alignment that serves Moscow's broader objective of fragmenting Western Balkan cohesion. When Serbian nationalist mobilisation destabilises neighbouring contexts through ethnic mobilisation, it accomplishes Russian strategic goals without requiring direct Russian intervention. The Serbian government employs this narrative for two main purposes. First, they impose certain values through the school curriculum, promote special relations in culture and sports, and foster a clerical society that views the Orthodox churches in Belgrade and Moscow as the only ‘pure’ institutions. This strategy promotes ‘traditional values and culture’ aligned with Putin's Russia while condemning the liberal West (Styczyńska, 2024, p.6). This is influence laundered through spirituality, rendered resistant to counter messaging precisely because it operates in affective rather than cognitive registers.

Figure 3: The ideological map representing the territory covering the idea of “Srpski Svet”. https://www.koreni.rs/srbska-zemlja-ili-srpski-svet/

3. EU and NATO - Security, technology and the limits of Integration

This chapter examines the security and technological dimension, focusing on the intersection of intelligence networks, Russian and Chinese military systems, and surveillance infrastructure.

The EU is Serbia's primary trading partner, accounting for 54% of Serbia's overall trade in 2022 and remaining stable over the years. Serbia's exports to the EU grew from EUR 3.2 billion in 2009 to almost EUR 18 billion in 2022. In comparison, total trade with China, Russia, and the United States in 2022 amounted to EUR 5.8 billion (imports: 4.7 billion, exports: 1.1 billion), EUR 4.03 billion (imports: 2.9 billion, exports: 1.13 billion), and EUR 1.19 billion (imports: 0.68 billion, exports: 0.51 billion), respectively. Between 2010 and 2022, over 59% of Serbia's foreign direct investment (FDI) originated in the EU, totalling EUR 20.3 billion. By contrast, China, Russia, and the United States accounted for 9 % (EUR 3.1 billion), 7 % (EUR 2.6 billion), and 2 % (EUR 0.84 billion) of FDI. (Weissmann, 2023, p. 19).

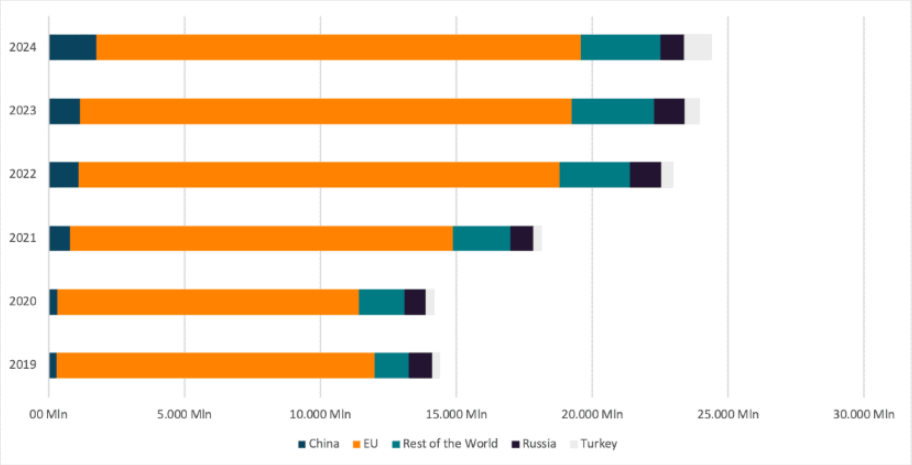

Figure 4: *STRÖHM, 2025:* Exports of goods, Serbia (2019-2024, in EUR million)

Despite the high level of economic cooperation and the EU's messaging on the region's future, the situation is not as positive as it is often depicted. To quote Dr Tzifakis, 'Russia and China largely outpace the EU across almost all indicators of influence and appreciation. Worryingly, Serbia has attempted to extend its influence through most of the region and with it, there is a risk that external orientation towards China and Russia, coupled with its critical views of EU policies, may present a paradigm for other Western Balkan countries' (Tzifakis, 2021, p.3).

The reliance on Chinese weaponry, such as the FK-3 and HQ-17AE systems, complicates NATO interoperability objectives that NATO seeks to promote through the Partnership for Peace program. Serbia considers the RS entity in BiH as a bargaining chip in its relations with Kosovo and external powers. That is, if Kosovo could secede

from Serbia, Serbia would *ipso facto* consider BiH's territorial arrangements a reopened question despite Belgrade having signed the Dayton Peace Accord (Jusić, 2024, p. 7).

Vulin's trajectory through Serbian institutions reveals the pattern. The ecosystem extends beyond individual actors. Russia is approached as being a 'network state', in which the duality of weak formal and powerful informal institutions coexist and where the borders between what is public and what is private are blurred (Secrieru, 2019, p.5). The concept of the 'network state' captures how Russian influence operates through distributed nodes rather than hierarchical command structures. In Serbia, these nodes include the Orthodox Church, the energy sector management within NIS, media outlets dependent on state advertising, and parliamentary groupings maintaining informal channels with Moscow.

Figure 5: *NATO and EU peacekeepers in the Western Balkans. (MIA, 2024. P.91) The Western Balkans Controlled Inst*

3.1. Stabilitocracy and the absence of the EU

Based on the use of the term in earlier BiEPAG studies describing semi-authoritarian regimes in the Western Balkans that receive external support from EU member states, for the sake of the (false) promise of stability. Stabilitocracy is a regime that suffers from significant shortcomings in democratic governance and derives external legitimacy from offering a supposed sense of stability (Bieber, 2017).

Stabilitocracy in the Western Balkans describes the current state of democracy in the region. Its distinctive features include strong leadership and external legitimisation (primarily from the EU). Serbia saw the emergence of stabilitocracy with the rise to power of Aleksandar Vučić and his Serbian Progressive Party in 2012. The term distinguishes the pattern in the Western Balkans from similar yet distinct forms of illiberal democracies inside the EU (Hungary and Poland, for instance), as well as authoritarianism in countries like Turkey and Russia. (Bieber, 2017).

While focused on economic dimensions, Brussels has shown tolerance for democratic backsliding in exchange for superficial cooperation on migration and regional stability. The cost of this bargain becomes apparent in the gap between EU rhetoric on values and EU practice on conditionality.

The 2023 and 2024 European Parliament reports acknowledge Serbia's good progress in macroeconomic stability and fiscal discipline, but voice concern that there has been limited or no overall progress in meeting the benchmarks for EU membership across the negotiating chapters. Shortcomings identified included the rule of law, media freedom, public administration reform, and alignment with EU policies, particularly the EU's foreign policy (European Parliament, 2025, p. 5).

In the spirit of stabilitocracy, short-term stability over structural transformation, the EU permits a sophisticated embedding of Russian and Chinese influence within Serbian institutions. With each year without action from the EU, the potential for influence becomes increasingly ineffective.

4. Strategic Implications and Recommendations

4.1. The Erosion of Euro-Atlantic Unity

Belgrade's balancing act has not merely delayed integration; it has also undermined it. It has created institutional architectures that actively impede future alignment, even if a strong political will were to emerge. The intelligence networks, technological dependencies and financial flows all have implications for Serbia's Euro-Atlantic ambition. Limited cooperation with NATO and persistent media and public scepticism toward the Alliance erode NATO's strategic role in the Western Balkans. This ambiguity creates structural openings that both Russia and China actively exploit. Russia leverages historical, energy, and security ties to maintain political influence and disrupt Western alignment. On the other hand, China expands its footprint through infrastructure investment and economic diplomacy, reinforcing Serbia's strategic autonomy from Western institutions.

Serbia's military neutrality, strategic posture, and multidirectional diplomacy illustrate its function as a conduit for external influence that challenges Euro-Atlantic cohesion. Though clearly condemning the Russian aggression against Ukraine and voting alongside the EU in the UN, Serbia has not imposed sanctions against Russia. ‘Serbia has mostly continued its alignment patterns with the Common Foreign and Security Policy (CFSP) in 2024, similar to 2022 and 2023, when Serbia had alignment rates of 48 percent and 54 percent, respectively. In 2024, Serbia’s alignment rate reached 59 percent, what represents an improvement. However, its rate remains to be the lowest among EU candidate countries from the Western Balkans’ (Novaković, 2025, p. 1). The implications for EU and NATO policy are significant. Serbia's position weakens the credibility of EU enlargement conditionality and complicates NATO's efforts to consolidate regional security. Addressing this requires a recalibrated strategy that strengthens conditional engagement. Serbia's trajectory indicates a risk of accelerated strategic ambiguity and a fragmentation of Euro-Atlantic unity over member state policies toward the Western Balkans.

4.2. Differentiated policy recommendations

An effective Western response requires recognising that Serbia is not simply a passive recipient of external influence, but an active strategic actor leveraging competing powers. Whatever the EU and NATO policy response will be, it must be coordinated and targeted across security, economic, and political elements of power.

4.2.1. Security services

NATO should enhance its intelligence posture in the Western Balkans by establishing a dedicated coordination mechanism focused specifically on hybrid influence networks operating through Serbia. This could be achieved within existing structures, such as expanding the role of the NATO Intelligence Fusion Centre (NIFC). The priority should be the systematic mapping of influence networks linked to Serbian actors operating across the region.

4.2.2. EU integration and diplomacy strategy

The EU must recalibrate its enlargement strategy by moving from declaratory conditionality to enforceable benchmarks, more precisely, Chapters 23 (Judiciary) and 31 (Foreign Policy). They should be treated as core political criteria rather than technical negotiation chapters. Progress in other areas should be explicitly conditioned on measurable improvements in the rule of law and foreign policy alignment.

To restore credibility, the EU should introduce automatic consequences for sustained non-alignment with CFSP positions. The EU should also clearly communicate that integration into European security structures is incompatible with long-term reliance on non-interoperable military systems, regardless of the individual benefits. This approach would shift the calculation of strategic ambiguity to responsible Serbian decision-making in line with EU policies.

5. Conclusion

To what extent does Serbia's deliberate strategic ambiguity function as an enabling regional hub for Russian and Chinese influence in the Western Balkans, and what are the implications for NATO and EU policy coherence? The analysis demonstrates that Serbia's position as a strategic hub for Chinese and Russian influence in the Western

Balkans is a deliberate choice by a government that has identified strategic ambiguity as a governing strategy. Serbia's balancing between the EU, NATO, Russia, and China enables it to extract political and economic benefits while simultaneously facilitating the projection of Russian and Chinese influence across the region.

The implications for NATO and the EU are significant. Serbia's position undermines the credibility of EU enlargement and complicates NATO's efforts to ensure interoperability and regional stability. Serbia's role as a transponder of influence into neighbouring countries amplifies the strategic impact beyond its national borders, affecting the broader Western Balkans and, indirectly, the European security environment. EU's prioritisation of short-term stability over democratic reform, combined with inconsistent conditionality, has enabled the consolidation of ‘stabilitocratic’ governance structures. Reversing this trajectory will require stronger policies and a coherent strategic approach that recognises Serbia's agency and the systemic nature of the challenge.

The window for effective policy intervention is narrowing. Chinese infrastructural and technological dependencies continue to deepen, while Russian political and intelligence networks remain embedded within Serbian institutions and regional linkages. Ultimately, the success of Euro-Atlantic policy in the Western Balkans will depend on restoring credibility. This requires demonstrating that alignment with EU and NATO structures delivers tangible political, economic, and security benefits, while also making clear that strategic ambiguity carries measurable costs.

Bibliography

BECHEV, Dimitar. 2024. *Between the EU and Moscow: How Russia Exploits Divisions in Bosnia*. Carnegie Endowment for International Peace [online]. 27 June 2024. https://carnegieendowment.org/research/2024/07/bosnia-between-russia-eu

BIEBER, Florian. 2017. *What is a Stabilitocracy?* Balkans in Europe Policy Advisory Group (BiEPAG) [online]. 05 May 2017. https://www.biepag.eu/blog/what-is-a-stabilitocracy.

BIEBER, Florian. 2017. *The Rise (and Fall) of Balkan Stabilitocracies.* Centre for International relations and sustainable development (CIRSD) [online]. 20 April 2026. https://cirsd.org/horizon-article/the-rise-and-fall-of-balkan-stabilitocracies/

CVIJIĆ, Srdjan; NIKOLIĆ, Kristina. 2025. *What does the Russian community in Serbia think and do?* Belgrade Centre for Security Policy.

CIPAN, Vibor; KIRICHENKO, David. 2024. *Russian Influence and Disinformation Operations in the Balkans*. *Georgetown Security Studies Review*, 11(2), 65–85.

DUFALLA, Jacqueline; METODIEVA, Asya. 2024. *From affect to strategy: Serbia's diplomatic balance during the Russia-Ukraine War.* Routledge, Taylor and Francis Group.

EUROPEAN PARLIAMENT. 2025. *European Parliament resolution of 7 May 2025 on the 2023 and 2024 Commission reports on Serbia (2025/2022(INI)).* P10_TA(2025)0093.

GRKOVIĆ, Branislav. 2024. *Vulin received another Russian order, now personally from Putin*. Vreme: [online]. 24 January 2024. https://vreme.com/en/vesti/vulin-dobio-jos-jedan-ruski-orden-sada-licno-od-putina/#:~:text=According%20to%20the%20Movement%20of,from%20the%20FPN%20told%20N1.

JOVIĆ-LAZIĆ, Ana. 2026. *Serbia's Strategic Ambiguity as a Governing Strategy: EU Accession, Russia, and China*. *Journal of Liberty and International Affairs*, Volume 12, Number 1, eISSN 1857-9760.

JUSIĆ, Asim. 2024. *The (Uncertain) Future of Kosovo's Community of Serb Municipalities: Another Republika Srpska?* Atlantic Initiative – Centre for Security and Justice Research.

MIA, Irene. 2024. *The Western Balkans: Controlled Instability?* In *Armed Conflict Survey 2024*. International Institute for Strategic Studies (IISS).

NOVAKOVIĆ, Igor; STOJANOVIĆ, Nataša; PLAVŠIĆ, Tanja. 2024. *An Analysis of Serbia's Alignment with the European Union's Foreign Policy Declarations and measures: Annual review for 2024*. CFSP and Serbia's Accession to the EU. Belgrade: ISAC Fund.

PETROVIĆ, Predrag. 2024. *Strategic (Dis)orientation of Vučić's Serbia: Reluctantly Moving West, Willingly Embracing the East*. Atlantic Initiative – Centre for Security and Justice Research.

PRELEC, Tena; STOJANOVIĆ-GAJIĆ, Sonja; KRIVOKAPIĆ, Đorđe; PALLOSHI-DISHA, Edlira. 2025. *Foreign Influence Challenges: Corrosive Capital and Disinformation in the Western Balkans and Associated Trio*. GEO-POWER-EU. November 2025. DOI 10.5281/zenodo.17787804.

RAKIĆ, Snežana. 2025. How Much Does Serbia Owe China? Serbian Monitor [online]. 25 November 2025. https://www.serbianmonitor.com/en/how-much-does-serbia-owe-china

SECRIERU, Stanislav. 2019. *Russia in the Western Balkans: Tactical Wins, Strategic Setbacks*. Brief No. 8. Paris: European Union Institute for Security Studies.

SICKELL, Julieann; ESCOBAR, Brooke. 2025. *Serbia: The Scale, Scope, and Composition of Chinese Development Finance*. Williamsburg, VA: AidData at William & Mary.

STANICEK, Branislav; CAPRILE, Anna. 2023. *Russia and the Western Balkans: Geopolitical Confrontation, Economic Influence and Political Interference*. Brussels: European Parliamentary Research Service.

STRÖHM, Bernd Christoph; LAMPRECHT, Philipp. 2025. *Unlocking the Western Balkans: Why Serbia Holds the Geopolitical Key*. ECIPE Insights [online]. July 2025. https://ecipe.org/insights/unlocking-the-western-balkans-serbia

STYCZYŃSKA, Natasza. 2024. *The Myth of the Serbian-Russian Friendship*. *New Eastern Europe*.

TAL, Pavel. 2025. *State Surveillance in Serbia: Examining the Role of Chinese Supplied Surveillance Cameras.* DOT.PL, no. 1/ 2025, 10.60097/DOTPL/ 214711

TZIFAKIS, Nikolaos. 2021. *Geopolitically irrelevant in its 'inner courtyard'?: The EU amidst third actors in the Western Balkans.* BiEPAG

US DEPARTMENT OF THE TREASURY. 2023. *Treasury Sanctions Official Linked to Corruption in Serbia*. Press release [online], 11 July 2023. https://home.treasury.gov/news/press-releases/jy1606.

US DEPARTMENT OF THE TREASURY. 2025. *Treasury Intensifies Sanctions Against Russia by Targeting Russia's Oil Production and Exports*. Press release [online], 10 January 2025. https://home.treasury.gov/news/press-releases/jy2777.

VLADISAVLJEV, Stefan; DIZDAREVIĆ, Damir; ĐORĐEVIĆ, Mirjana. 2025. *Analysing China's Influence in Serbia and Its Implications for Transatlantic and European Security*. Belgrade: Foundation BFPE for a Responsible Society.

WEISSMANN, Mikael. 2023. *Chinese and Other Foreign Influence in Serbia and the Western Balkans: A Tale of Cooperation, Competition, and Distrust*? Connections: The Quarterly Journal.

ZWEERS, Wouter; Kelečević, Ivan. 2025. *Geopolitically Mapping in the Western Balkans*. The Hague: Clingendael Institute.

LTC Kuido PETTAI: What Factors Limit Joint Procurement in NATO, and how could an Improved Joint Procurement Process Enhance Member States' Defence Capabilities?

Supervisor: COL (ret.) Dr. Çlirim TOCI

Statement on the Use of AI Tools:

This research paper was prepared by me using AI collaboration to ensure it meets higher academic standards.

Tools: Microsoft Copilot, Grammarly

Purpose: Structural development, content refinement, additional argumentation and bibliography editing

Process: Initial structure developed through iterative dialogue with Copilot and Perplexity over 3 sessions (January-April 2026). I provided the core concepts and ideas for a research paper regarding AI adoption challenges within NATO. I provided sources and intended outcomes. Copilot and Perplexity assisted with organising content flow, section structure and additional arguments for my revision. The Grammarly app helped resolve grammatical issues and mistakes in the paper version. Zotero assisted with correcting the initial bibliography (in addition to ISO 690).

Ownership: All conceptual frameworks originated from my research and academic publications and primary sources. Academic argumentation and conclusions are my intellectual contributions. I reviewed and revised all supplementary AI-generated text for accuracy. Final content decisions and research logic were mine.

Introduction

We cannot solve our problems with the same thinking we used when we created them. –
Albert Einstein

There is only one thing worse than fighting with allies, and that is fighting without them. –
Winston Churchill

NATO has a key role in supporting Allies as they build and modernise their military capabilities, including the acquisition of new weapon systems, vehicles and other major equipment. While capability development remains the responsibility of individual NATO member states, NATO coordination helps them identify, prioritise and procure the capabilities required to defend both themselves and the Alliance. This cooperation can also create economies of scale and improve cost-effectiveness. In addition, NATO helps ensure that national systems are interoperable and can operate together effectively when required. Close cooperation with the defence industry is essential to achieve these objectives (*NATO's role in defence industry production*, 2025a).

Despite a strong message from the NATO political level to strengthen defence capability development through joint procurement (*Washington Summit Declaration*, 2024), Allies commit to allocating 5% of GDP each year by 2035 to core defence needs, as well as broader defence- and security-related expenditure, to meet both national and collective obligations (NATO, 2025c). There is still no defined procedure, centralised procurement authority, or official NATO definition for the extensive multinational joint procurement process for member states' military equipment. Therefore, the joint procurement process is fragmented, which can create the risk of slowing down capability delivery, hamper interoperability and call into question NATO's credibility in responding to threats. At the same time, NATO defines the capabilities for NATO member states through the NATO Defence Planning Process (NDPP).

Therefore, this research paper addresses problematic areas of the joint procurement process, provides a definition of the joint procurement process and examines how an enhanced joint procurement process affects future capability development.

Moreover, fragmented decision-making and divergent national interests hinder NATO joint procurement and a more coherent, centralised approach is needed to accelerate capability development.

The research paper is divided into three chapters. The first chapter maps and analyses NATO, as an organisation and its member states, procurement organisations and the factors and limitations that will impact the joint procurement process. The second chapter analyses how an enhanced joint procurement process can improve member states' defence capability development. Recommendations for future solution options are offered in the third chapter. The author provides conclusions at the end of the research paper.

2. Factor analysis of actors and joint procurement limitations in NATO

First of all, what is the NATO joint procurement process? There is no proper definition for that process. Therefore, the proposed definition will be as follows: NATO Joint Procurement is the consolidation of requirements from multiple member states to acquire equipment, systems or services through a single multinational procurement process to achieve economies of scale, cost-efficiency, interoperability, innovation and improved supply chain and delivery times. Moreover, in cooperation with partners and established international institutions and in support of existing NATO and EU initiatives, the mechanism should aim to reinforce collective deterrence, enlarge defence-industrial capacity and improve defence capabilities through joint procurement. (Reeves, 2026).

2.1. NATO Procurement organisations

NAC approved a new 2025 NATO procurement policy, whose purpose is to make the procurement mechanism of NATO common-funded goods and services faster and

more flexible, but within the scope of NATO-owned or NATO-managed capabilities (*procurement-policy_en.pdf*, no date).

NATO procurement is carried out by several different bodies, including NATO agencies, acting on the Alliance's behalf. However, there is no single central organisation responsible for all NATO procurement activity. Funding also comes from various NATO sources, depending on the type of project. However, most capital investment projects delivered by NATO are financed through the NATO Security Investment Programme (NSIP) (GOV.UK, 2026). Procurement is a hybrid system that combines national independent procurement decisions with shared NATO mechanisms.

2.1.1. NATO Support and Procurement Agency

The NATO Support and Procurement Agency (NSPA) combine acquisition, logistics, medical support, infrastructure, operational support, systems support and related services within one organisation. It provides these services to NATO member states, NATO Military Authorities and partner nations. As NATO's main support and procurement enabler, NSPA's role is to deliver effective, cost-efficient multinational solutions for the Alliance, its 32 member states and partners.

NSPA operates on a 'no profit, no loss' basis. As one of NATO's three agencies, it functions under charters approved by the North Atlantic Council (NAC). The Agency serves as the executive body of the NATO Support and Procurement Organisation (NSPO), which comprises all 32 NATO nations. Strategic direction, guidance, oversight and performance monitoring are provided by the NSPO Agency Supervisory Board, whose members are represented by the member nations (NSPA, 2026a).

This support covers a wide spectrum of activities, from multinational procurement of advanced platforms such as aircraft, helicopters and unmanned systems, to the delivery of essential supplies including fuel, spare parts and ammunition, as well as services such as air-defence radar maintenance, deployable infrastructure, transport, medical support and catering. Cooperation with industry is one of NSPA's key

strengths, allowing the Alliance to develop cutting-edge solutions and access the newest technologies. To provide NATO and Partner Nations with both current and future capabilities and to keep pace with the latest innovations, NSPA works with industry across the acquisition and sustainment processes. Its goal is to secure the best possible services or equipment at the most favourable price for customers by combining requirements from multiple nations and delivering them efficiently through its turnkey multinational acquisition framework. (NSPA, 2026b).

The NSPO Support Partnership (SP) is a multinational cooperation arrangement created when two or more NATO nations decide to organise shared support and service activities. This model is one of NSPA's distinctive features. Participating nations provide governance and strategic guidance, while NSPA develops the necessary capabilities and manages national requirements.

By consolidating requirements, the Support Partnership model creates economies of scale, lowers costs and reduces the logistics footprint. Its legal framework also provides a common and efficient basis for delivering support. In addition, the format encourages participating nations to discuss their logistics challenges together, helping them identify and address both shared and national requirements (NSPA, 2026c).

2.1.2. NATO member states procurement organisations

Russia's full-scale invasion of Ukraine in February 2022 and its continuing war of aggression have severely destabilised European peace and underscored the importance of NATO maintaining a robust and credible deterrence and defence stance. In response, Allied countries have increased investment in defence production to strengthen their own military capabilities and restore stockpiles reduced by assistance provided to Ukraine. (*NATO's role in defence industry production*, 2025b).

The 32 NATO member states have organised their procurement systems in accordance with nationally agreed-upon arrangements: major powers (the U.S., France, Germany, the U.K. and Italy) operate highly institutionalised defence procurement agencies, while smaller countries often handle procurement within their respective Ministries of Defence.

For example, in Estonia, the Estonian Centre for Defence Investments (ECDI) provides centralised procurement management services for organisations operating under the Ministry of Defence. Its role includes organising centralised procurements to secure the goods and services required across the Ministry's area of responsibility. The ECDI also conducts joint procurements with other countries and organisations to combine requirements and achieve cost savings (RKIK, 2026).

2.2. Political and legal constraints

Defence remains primarily a national responsibility and most defence acquisitions are therefore conducted by governments to meet the needs of their own armed forces. There are several reasons why procurement is often carried out nationally. Equipment requirements are shaped by factors such as geography, strategic culture, military doctrine, domestic defence-industrial policy, international security commitments and available budgets. In some countries, legal restrictions also limit participation in international armaments cooperation (Friton, Wolters, Andree, 2020).

Defence acquisition is the process of defining needs, securing military equipment and ensuring its delivery on schedule, within budget and in line with agreed requirements. While the terms defence acquisition and defence procurement are frequently used as if they mean the same thing, including in policy documents, it is helpful to separate them for analytical purposes. Acquisition is the broader concept, covering decisions about what to buy, how to buy and how to support systems and platforms throughout their lifecycle. Procurement, by contrast, refers more specifically to the negotiation and management of contracts. (Andersson, 2023).

As agreed at the Hague Summit, the 5% target is primarily a political signal. Its purpose is to show Allied determination, unity, and a common willingness to bear the burden of defence and security, especially as a deterrent message to NATO's adversaries, with Russia as the principal concern (Tian, Scarazzato, Guiberteau Ricard, 2025).

Previously, at the London Summit 2019, it was agreed through the Defence Investment Pledge that NATO will increase member states' defence investment, in line with the

20% guidelines, investing in new capabilities and contributing more forces to missions and operations (NATO, 2019).

Each NATO member's political leadership is responsible for defining the state's strategic goals in accordance with a threat assessment (Retter et al., 2021). Procurement decisions will be influenced by independent decision-making policy, the domestic defence industrial base and domestic legal regulations (Hurt, Vargulis, Zdanavičius, Jermalavičius, 2023). This is a matter of policy and will, compounded by a gap between verbal ambition, actual investment interest, risk appetite and an understanding of the risks, both in terms of financial resources and procurement processes (Barry, 2025). Every ally wants jobs, supply security, and full control over the product lifecycle, resulting in highly inefficient resource use. Therefore, there is a need to decide which procurement processes truly require autonomy, which can be handled jointly, and which can be purchased on the market—only the latter two can generate scale and momentum. It is even noticed at highest level of NATO, by Tarja Jaakola, NATO's assistant secretary general for defence industry, innovation, and armaments, but not as positive notes: '[…] *NATO members aren't regularly buying weapons together, limiting how quickly and cheaply they can build up stockpiles* […] *that allies can acquire weaponry most cost-effectively by jointly purchasing it* [...]. *Having multiple countries trying to independently develop similar weaponry means fewer resources per program and higher per-unit costs than working together* [...]' (Baker, 2026).

On the other side, each NATO country has independent decision-making power over its defence spending:

1. Countries decide for themselves the size of their budgets and how much of those budgets is allocated to the procurement of defence and non-defence equipment.
2. The equipment needed to be procured is determined by the armed forces of the member states, using the principle of minimum military requirements (MMR).
3. Contracts are signed by the ministries of the member states or by the bodies responsible for the procurement process.

But at the same time, NATO member states' procurement processes are slow and bureaucratic, which is leading NATO to develop yesterday's defence capabilities (Barry, 2025). Their defence institutions (Ministries of Defence, Defence Forces) must improve, adapt, turn lessons learned into practical lessons, and implement them as tangible progress.

Moreover, failure to follow the standardisation process through STANAG can lead to the procurement of non-interoperable equipment and systems. The Unmanned Aerial Systems (UAS)/Counter-UAS (C-UAS) capability development identified a shortfall in the legal domain, requiring the implementation of a new legal process. Participating in the joint procurement process requires consensus-based decision-making, which can slow down or block the joint approach. Moreover, some nations will avoid the joint procurement process when there are indications that it could conflict with political ambitions, national security strategy, or the domestic defence industrial base.

On 30 September 2025, European Commission President Ursula von der Leyen made a statement to NATO Secretary General Mark Rutte, '[…] *we have a single set of forces, assigned to different missions – NATO, EU, UN or Coalitions of the Willing. Therefore, in close cooperation with NATO, we need capabilities that are interoperable. To achieve this, we need more joint procurement* […]' (von der Leyen, 2025).

Despite supportive political language and formal commitments to EU–NATO complementarity, tangible progress in strengthening coherence and reducing duplication has been minimal. Implementing effective EU-NATO cooperation remains difficult, partly because tensions involving states that belong to one organisation but not the other restrict meaningful information sharing and joint planning (Retter et al., 2021). Moreover, EU defence spending reached €381 billion in 2025; a proportional rise has not kept pace with this increase in joint acquisitions. EU institutions still point to persistent duplication, capability shortfalls and dependence on suppliers from outside the EU. In response, the EU has broadened its financial and regulatory tools. EDIRPA, EDIP and SAFE offer grants and loans designed to encourage joint procurement, while the Defence Readiness Roadmap 2030 sets a target of 40% joint procurement by 2027. Proposed changes to the Defence Procurement Directive are intended to reduce administrative obstacles and make multinational contracting easier

(Tothova, Clapp, 2026). There is no conflict between NATO and the EU; rather, the opposite is true—NATO needs capabilities and the EU helps member states achieve them. There is a need to work more closely together to achieve goals that are currently out of reach, to assess whether all existing weapon systems are necessary and to optimise them where possible. On the other hand, it is necessary to enhance the military mobility project, which is a key area of EU-NATO cooperation: the EU has the budget to help make the movement of troops in Europe—both in terms of infrastructure and processes—as swift as possible and in line with NATO's requirements.

The main problem is structural, not accidental. The goal of NATO's joint procurement model is to coordinate sovereign countries, not to force them. All mechanisms — from the Defence Production Plan to NSPA framework agreements — ultimately depend on each country's voluntary participation decisions at each point of decision-making. This means that at any moment when the domestic industrial interests, electoral considerations, or strategic culture of a member state differ from the collective, the process comes to a halt. The result is a systemic gap between political declarations of solidarity and contractual obligations that would actually move the production line.

Of the multiple constraints identified above, the binding constraint is political sovereignty: the voluntary nature of all NATO joint procurement mechanisms means that every single member state can opt out at any decision point based on domestic political, industrial or electoral considerations. Legal constraints, divergent threat perception and industrial base weaknesses are serious secondary factors, but they are ultimately resolvable through treaty revision, interoperability standards and investment. Sovereignty-driven fragmentation, by contrast, can’t be engineered away – it requires political will and trust building over time. This is why information asymmetry matters so much: if member states can’t see what their allies are procuring, when and at what cost, they have no rational basis for choosing joint over national procurement. Reducing information asymmetry is, therefore, the most actionable near-term lever for incrementally building the political confidence that joint procurement can work.

2.3. Strategic military leadership priorities

Strategic military leadership priorities regarding capability caps are defined by nations through their national defence planning processes. At the same time, the NATO defence planning process identifies the capabilities listed in the NATO capability targets document (Tian et al., 2025). These two processes are linked to nations' defence budgets and the availability of funds for a specific planning timeframe. Most of the time, capability development, delivery, and budget allocations are not aligned with those of NATO member nations. The reason is quite simple: NATO member states have different threat perceptions and capability requirements, which underpin NATO's trustworthiness and resilience.

Today, based on Ukraine's experience, the battlefield adaptation cycle lasts 2–6 weeks; in other words, adaptation is not merely about developing new and innovative equipment, but also about using existing technology in new ways. Overall, this is a strategic decision by the defence leadership—reframing objectives, allowing for room for error and bringing the right parties together (end-users and procurers, government and industry).

A decision must be made on how to reduce the gap between technology development and deployment, align the armed forces' interests with the technology itself rather than overall capability and share the risks between the private and public sectors. A prerequisite for this planning cycle is that the process culminates in a successful procurement, which should serve as a motivator, encouraging member states to jointly develop capabilities. Today's NATO capability planning process dictates that problems must be solved with current or past capabilities, which, in turn, creates an innovation problem—that is, planning should be adjusted to be forward-looking through an innovation matrix rather than repeating old mistakes. This would reduce bureaucracy and allow investment in more innovative, albeit higher-risk, technologies that support faster modernisation of overall defence capabilities.

We must take into account the needs arising from our plans and the developments that will occur between now and 2035—that is, address today’s capability gaps while ensuring we remain up to the task in the future (in terms of innovative technological

development and advantages, as well as human resources). Capability planning must be realigned with operational needs, which will be very difficult to implement. Another problematic issue is the cost-effective use of the defence budget to develop the capabilities outlined in the Capability Targets 2025 document. A positive trend has been established with the decision adopted at the Hague Summit to allocate 5% of GDP to defence capabilities, as anything less would be insufficient to meet both operational and capability-planning needs.

Rapid development of innovative technology - the UAS/C-UAS capability required by NATO requires new tactics, techniques and procedures (TTP) and technology (radars, acoustic detectors, Electronic Warfare, Artificial Intelligence), which changed the modern warfare dynamic.

2.4. The defence industrial base

Risk assessment is a combination of factors that have a critical impact on the NATO Capability delivery and interoperability. The defence industrial base was under-resourced for decades, and investment was insufficient. It led NATO to low production capacity and supply chain bottlenecks. The conflict in Ukraine exposed a severe shortfall of critical stockpiles (ammunition, aid, defence and ISR systems) among the NATO member states.

Historically, sharp rises in military spending have carried notable risks, including inefficient procurement, inflated prices, misuse of funds and the weakening or avoidance of oversight procedures. In addition, it remains unclear whether the defence industrial base can absorb large, sudden increases in expenditure. Since 2022, the industry, particularly in Europe, has faced difficulties expanding production quickly enough to meet growing demand (Eurasia, 2026).

Defence-sector inflation, commonly known as ‘defence cost inflation’, often increases more rapidly than overall inflation. Consequently, even substantial nominal growth in defence budgets may translate into only modest real gains in military capability. Under such conditions, the added benefit from each new investment can diminish quickly, increasing the risk of inefficient or wasteful spending. Defence inflation can stem from

demand-pull pressures, where demand outstrips available supply, as well as cost-push pressures, as successive generations of equipment become more technologically advanced, complex and costly. Limited competition and inadequate economies of scale can also restrict market flexibility and push production costs and prices higher (Tian et al., 2025).

The talent gap – a hidden obstacle to increasing production capacity in the defence industry, as production lines must be staffed in both peacetime and wartime, but the labour market currently suffers from a chronic shortage of critical skills, making it impossible to recruit them into the defence industry or armed forces when competing with technology companies. A fundamentally different approach is needed to find, develop and retain talent. For the past 20–30 years, the defence industry has not required the skills needed today in the necessary quantities; maintaining their quantity and quality is expensive and redeveloping them is even more so, given the lack of recruits. A new kind of integrated force is needed—distributing talent between the defence industry and the battlefield and making innovative use of reservists.

3. How the improved joint procurement process will enhance defence capabilities

In planning and developing forces and military capabilities suitable for fulfilling military defence objectives (e.g., defining the roles of service branches and developing specific capabilities), the primary focus is on the essential capabilities required for independent defence operations (including the needs of comprehensive national defence). Existing and future military capabilities form the basis for a successful independent defence, an integral part of which is participation in collective defence. Specific capabilities will not be developed if their full potential depends directly on other participants in collective defence or is related solely to collective defence needs.

NATO must expand the capacity of its defence industrial base (DIB) while developing an acquisition strategy to meet the rising demand for weapons and ammunition. At the same time, these efforts need to be managed carefully in light of political sensitivities (Marcinek, 2024). Through joint procurement, all involved parties win – nations get capabilities more cheaply or, with the same amount of funds, more capabilities.

Innovation procurements contribute significantly to increasing NATO member nations' defence capabilities by developing new technologies for the defence forces and to local economic growth and competitiveness. Innovation procurement results in new, high-quality and efficient solutions (e.g., better, faster, cheaper, more sustainable). This makes it possible to find innovative solutions to problems for which there is currently no suitable solution on the market. Through innovation procurement, NATO member states can learn about new approaches and solutions and contribute to innovation. This enables NATO member states and the defence industry to collaborate on developing and testing innovative products or services to address capability gaps.

NATO's enhanced joint procurement approach allows multiple allied countries to combine needs, funding and demand with NATO member states' military strategic leadership directions and guidance, while relying on centralised institutions, standards and digital platforms to manage information, offers, contracts and lifecycle support. At the core of this system is NSPA, supported by tools such as the NSPA portal, CAPCAT (Capabilities Catalogue), NATO Codification System (NCS) and notifications of upcoming business opportunities.

Improved joint procurement enhances defence capability development through four connected mechanisms through the High Visibility Projects (HVP). First, it accelerates capability delivery by aggregating national demand into larger and more predictable orders, which can help the industry plan production capacity and reduce duplication. NATO’s Land Battle Decisive Munitions (LBDM) project, involving 24 countries and first deliveries in January 2019, illustrates how joint procurement of munitions can translate shared requirements into actual military capability (*Multinational capability cooperation*, 2026). Second, it improves interoperability by aligning equipment, training, logistics and sustainment from the start to the end. The Multi-Role Tanker Transport Capability (MRTT-C) project shows this mechanism in practice: 6 NATO member nations jointly acquired a multinationally owned and operated Airbus A330 tanker fleet, reached initial operational capability (IOC) in March 2023 and are scheduled to operate ten aircraft after final delivery in 2026 (*Multinational capability cooperation*, 2026). Third, joint procurement strengthens readiness by providing Allies assured access to capabilities that would be costly to maintain through national capacity; the Strategic Airlift Capability (SAC) jointly acquired three C-17 aircraft for 12

participating countries and shared costs, flight hours and sustainment through NSPA (SAC, 2026). Fourth, it strengthens deterrence by providing that political commitments can become usable stockpiles and air-defence capacity, as shown by NSPA – supported contracts for up to 1000 Patrion missiles (NATO, 2024b) and around 220,000 rounds of 155mm artillery ammunition (NATO, 2024a). However, joint procurement is not automatically a success story: the A400M programme suffered delays and cost overruns, showing that pooled procurement requires unified, agreed requirements, disciplined governance, a project lead, realistic timelines and a balanced industrial workshare (Tothova, Clapp, 2026).

It is important to acknowledge the strongest counterarguments to joint procurement, as they represent legitimate policy positions held by several NATO member states. First, joint procurement reduces national flexibility – a country that has pooled requirements with allies may find itself unable to accelerate, cancel or redirect a procurement in response to its own threat assessment without incurring political and financial costs. Second, for larger NATO members with established domestic defence industries – notably France, Germany and the United Kingdom – joint procurement risks undermining domestic industrial capacity, employment and sovereign technology development. These states have used national procurement as an industrial policy instrument for years and a shift toward multinational pooling requires compensating mechanisms to maintain political feasibility. Third, excessive centralisation of procurement creates single points of failure in the supply chain – if a joint procurement process is disrupted, all participating nations are simultaneously affected. These counterarguments do not invalidate the case for improved joint procurement. Still, they establish that any reform or change must preserve meaningful national opt-out rights, ensure equitable industrial participation and maintain supply chain redundancy. The Centralised Information Hub proposed in the recommendation chapter is designed precisely to enable informed, voluntary participation rather than compulsory pooling, which addresses the first and most fundamental of these objections.

These mechanisms depend on earlier visibility of national procurement intentions, which is why the next section proposes a Single Centralised Information Hub as the practical enabler of voluntary procurement.

4. Recommendation - Single Centralised Information Hub

The Single Centralised Information Hub under NSPA – the eProcurement portal (NSPA, 2026d) - addresses the information asymmetry problem but, in itself, doesn't resolve the deeper political and legal constraints on joint procurement. To make the reform or change actionable, three complementary measures are proposed alongside the hub. First, NSPA's mandate should be formally expanded, through a North Atlantic Council decision to include an early warning function: NATO member states would submit initial procurement intention notices (covering capability type, approximate timeline and budget range) at the capability planning stage, before national approval. This preserves sovereign decision-making while enabling other nations to express interest in joining before national positions harden. Second, the NDPP should be adjusted to include a joint procurement compatibility check. When a NATO member state's Capability Target can be met through an existing NSPA framework agreement or an active HVP, the NDPP staff should flag this formally in the capability review cycle, creating a structured decision point for joint procurement rather than national procurement. Third, the EU's EDIRPA, EDIP and SAFE financial instruments could formally link to NATO's NDPP capability targets through a jointly agreed mapping exercise, so that EU co-financing incentives reinforce NATO capability priorities rather than operating in parallel. These three measures together – the hub, NDPP compatibility check and the EU-NATO instrument alignment – constitute a reform package that addresses the information, process and financial dimensions of the joint procurement problem without requiring changes to national sovereignty over ultimate procurement decisions.

5. Conclusions

This research paper has argued that fragmented decision-making and divergent national interests are the primary structural constraints on NATO joint procurement and that a more coherent, centralised approach – built on voluntary participation, better information sharing and process alignment – is both necessary and achievable. The research paper is confirmed by the evidence reviewed – despite strong political declarations at the London (2019), Washington (2024) and The Hague (2025) Summits, the absence of a defined joint procurement procedure continues to produce

capability delivery delays, interoperability shortfalls and cost inefficiencies that directly affect NATO's deterrence credibility (Lawrence, 2023). The structural nature of this problem means it will not be resolved by political rhetoric alone; it requires institutional reform or change at the NSPA level, process adjustments in the NDPP and alignment of financial incentives between NATO and EU instruments.

The implications extend beyond procurement efficiency. NATO's credibility as a collective defence organisation rests in part on its ability to field interoperable capabilities at scale and speed. If NATO member states continue to procure independently, they will inevitably produce non-interoperable equipment sets, duplicate development costs and undermine the very collective defence logic that justifies the Alliance's existence. The positive examples reviewed, including MRTT-C, LBDM, SAC and NSPA-supported ammunition and air-defence contracts, demonstrate that joint procurement works when political will, clear requirements and an enabling legal framework align. The A400M case, however, shows that multinational procurement can also lead to delays and cost overruns when requirements, governance and industrial workshare are not sufficiently disciplined. The task for NATO leadership is to make the alignment the rule rather than the exception. The EU, through EDIP, EDIRPA and SAFE, provides financial instruments that can accelerate this shift, provided NATO and the EU develop the institutional coordination needed to ensure their respective procurement incentives point in the same direction.

Looking forward, the defence investment commitment agreed at the Hague Summit creates an unprecedented fiscal opportunity: 5% of GDP allocated to defence spending generates real collective capability only if it is spent efficiently and in ways that avoid duplication. Joint procurement is the most powerful tool available to convert that resource into credible deterrence.

The recommendations in this research paper – a centralised information hub under NSPA, an NDPP joint procurement check and EU-NATO instrument alignment – are designed to be implementable within the current political and legal architecture of the Alliance, without requiring treaty revision or the creation of a new central procurement authority. They represent a pragmatic first step toward the more coherent joint procurement posture that the NATO security environment now demands.

Bibliography

ANDERSSON, Jan Joel. 2023. Buying weapons together (or not). *European Union Institute for Security Studies*. [Online]. 3 April 2023. [Cited : 25 April 2026]. https://www.iss.europa.eu/publications/briefs/buying-weapons-together-or-not.

BAKER, Sinéad. 2026. NATO official says members often aren't buying weapons together, and it's a mistake. *Business Insider*. [Online]. 2026. [Cited : 22 April 2026]. https://www.businessinsider.com/nato-allies-arent-buying-enough-weaponry-together-official-2026-3.

BARRY, Ben. 2025. Defending Europe Without the United States: Costs and Consequences. *IISS*. [Online]. 15 May 2025. [Cited : 18 April 2026]. https://www.iiss.org/research-paper/2025/05/defending-europe-without--the-united-states-costs-and-consequences/.

FRITON, Pascal, WOLTERS, Christopher and ANDREE, Niklas. 2020. Cooperation in Defence and Security Procurement among EU Member States. *European Procurement & Public Private Partnership Law Review*. 2020. Vol. 15, no. 1, pp. 24–41. DOI 10.21552/epppl/2020/1/6.

HURT, Martin, VARGULIS, Mārtiņš, ZDANAVIČIUS, Liudas and JERMALAVIČIUS, Tomas. Baltic Defence Development. *ICDS*. [Online] 2023. [Cited : 10 June 2026.] https://icds.ee/static/icds_analysis_baltic_defence_development_hurt_vargulis_zdanavicius_jermalavicius_march_2023.pdf.

LAWRENCE, Tony. 2023. Kuidas kiirendada Balti riikide kaitsevõime kasvu [How to Accelerate the Growth of the Baltic States' Defence Capabilities]. *Diplomaatia*. [Online]. 9 June 2023. [Cited : 15 April 2026]. https://diplomaatia.ee/tony-lawrence-kuidas-kiirendada-balti-riikide-kaitsevoime-kasvu/.

MARCINEK, Krystyna. 2024. NATO and Its Defense Industrial Base. *RAND*. [Online]. [Cited : 19 April 2026]. https://www.rand.org/pubs/commentary/2024/10/nato-and-its-defense-industrial-base.html.

NATO. 2019. London Declaration. *NATO*. [Online]. [Cited : 22 April 2026]. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2019/12/04/london-declaration.

NATO. 2024a. NATO concludes contracts for another $1.2 billion in artillery ammunition, 2024. *NATO, News and Events*. [Online]. [Cited : 26 April 2026].

https://www.nato.int/en/news-and-events/articles/news/2024/01/23/nato-concludes-contracts-for-another-3612-billion-in-artillery-ammunition.

NATO. 2024. NATO to buy 1,000 Patriot missiles to enhance Allies' air defences, 2024. *NATO, News and Events*. [Online]. [Cited : 26 April 2026]. https://www.nato.int/en/news-and-events/articles/news/2024/01/03/nato-to-buy-1000-patriot-missiles-to-enhance-allies-air-defences.

NATO. 2025a. NATO's role in defence industry production, 2025a. *NATO*, What we do. [Online]. [Cited : 18 April 2026]. https://www.nato.int/en/what-we-do/deterrence-and-defence/natos-role-in-defence-industry-production.

NATO. 2025b. NATO's role in defence industry production, 2025b. *NATO, What we do*. [Online]. [Cited : 13 April 2026]. https://www.nato.int/en/what-we-do/deterrence-and-defence/natos-role-in-defence-industry-production.

NATO 2025c. The Hague Summit Declaration. *NATO*. [Online]. [Cited : 14 April 2026]. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration.

NATO. 2026. Multinational capability cooperation. *NATO*. [Online]. [Cited : 22 April 2026]. https://www.nato.int/en/what-we-do/deterrence-and-defence/multinational-capability-cooperation.

Eurasia. 2026. NATO's New Spending Target: Challenges and Risks Associated with A Political Signal – Analysis. *Eurasia*. [Online]. [Cited : 27 April 2026]. https://www.eurasia.ro/2025/07/02/natos-new-spending-target-challenges-and-risks-associated-with-a-political-signal-analysis/.

GOV.UK. 2026. Navigating NATO procurement, 2026. GOV.UK. [Online]. [Cited : 9 April 2026]. https://www.gov.uk/government/publications/navigating-nato-procurement/navigating-nato-procurement.

NSPA. 2026a. About Us*. NSPA, NATO.* [Online]. [Cited : 9 April 2026]. https://www.nspa.nato.int/about.

NSPA. 2026b. NATO Support and Procurement Agency (NSPA), *NSPA, NATO.* 2026. [Online]. [Cited : 9 April 2026]. https://www.nspa.nato.int/about/nspa.

NSPA. 2026c. Support Partnerships. *NSPA, NATO.* [Online]. [Cited : 9 April 2026]. https://www.nspa.nato.int/business/support-partnerships.

NSPA. 2026d. Vendor Registration. *NSPA, NATO.* [Online]. [Cited : 18 April 2026]. https://www.nspa.nato.int/business/procurement/vendor.

RKIK. 2026. Organisation. *Riigi Kaitseinvesteeringute Keskus.* [Online]. [Cited : 28 April 2026]. https://www.kaitseinvesteeringud.ee/en/organisation/.

procurement-policy_en.pdf, no date. [Online]. [Cited : 6 April 2026]. https://www.nato.int/content/dam/nato/webready/documents/finance/procurement-policy_en.pdf.

REEVES, Rachel. 2026. Joint statement from Finland, the Netherlands, and the United Kingdom on joint defence financing and procurement. *GOV.UK*. [Online]. 17 March 2026. [Cited : 14 April 2026]. https://www.gov.uk/government/news/joint-statement-from-finland-the-netherlands-and-the-united-kingdom-on-joint-defence-financing-and-procurement.

RETTER, Lucia, PEZARD, Stephanie, FLANAGAN, Stephen J., GERMANOVICH, Gene, GRAND-CLEMENT, Sarah, et al. 2021. European Strategic Autonomy in Defence: Transatlantic visions and implications for NATO, US and EU relations. *RAND.* [Online]. [Cited : 18 April 2026]. https://www.rand.org/pubs/research_reports/RRA1319-1.html.

SAC. 2026. Strategic Airlift Capability. *sacprogram.org*. [Online]. 2026. [Cited : 26 April 2026]. https://sacprogram.org/default.aspx.

TIAN, Nan, SCARAZZATO, Lorenzo and GUIBERTEAU RICARD, Jade. 2025. NATO's new spending target: challenges and risks associated with a political signal. *SIPRI*. [Online]. 27 June 2025. [Cited : 18 April 2026]. https://www.sipri.org/commentary/essay/2025/natos-new-spending-target-challenges-and-risks-associated-political-signal.

TOTHOVA, Linda and CLAPP, Sebastian. 2026. EU joint defence procurement. [Online]. 2026. https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/785665/EPRS_BRI(2026)785665_EN.pdf.

VON DER LEYEN, Ursula. 2025. Statement by President von der Leyen with NATO Secretary-General Mark Rutte. [Online]. 30 September 2025. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/statement_25_2254/STATEMENT_25_2254_EN.pdf.

Washington Summit Declaration. 2024. Official texts and resources | NATO. [Online]. [Cited : 13 April 2026]. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/washington-summit-declaration.

COL Radek PILAR*:* Strategic Communication and the Czech Defence Consensus. Assessing the Vulnerability of Public Support for Military Investment and NATO Commitments to Hostile Narrative Pressure.

Supervisor*:* Dr. Dumitru MINZARARI

Statement on the Use of AI Tools

The research question, thesis, analytical approach, source selection, evidence interpretation, argumentation, recommendations, and conclusions in this Research Paper are the author's own. ChatGPT (OpenAI) and Claude (Anthropic) were used as critical-review tools to stress-test the analytical logic, identify weak claims and unsupported assertions, and check structural coherence against BALTDEFCOL principles of focus, accuracy, credibility, structure, cohesion, and fair treatment of sources. They were not used to generate analytical claims, conclusions, or produce the argumentative core of the paper.

The process was iterative. The author provided the research question, the thesis statement, the chapter structure, the draft text, the source material, and specific revision instructions. AI outputs were used as critiques and as prompts for the author's reconsideration. Where AI proposed wording or identified potential weaknesses, the author reviewed each suggestion critically and decided whether to accept, amend, or reject it. Factual claims, statistics, source references, and bibliography entries were checked against the underlying sources before final inclusion.

Grammarly was used for spelling, grammar, and language-level proofreading.

The author takes full responsibility for the content of this Research Paper, including its arguments, use of evidence, citations, bibliography, language, and conclusions.

Chapter 1 — Introduction

The Czech Republic occupies an important position in NATO's logistical and industrial architecture in Central Europe (Ministry of Defence of the Czech Republic, 2023). Its ability to sustain military investment, meet Host Nation Support (HNS) requirements, and contribute credibly to Allied force posture depends not only on military capability but also on durable public consent for those commitments. That consent is under pressure from two directions. First, hostile Russian information operations target public support for defence and Alliance solidarity. Second, domestic scepticism that, regardless of intent, can weaken support for the same commitments. The 2023 Czech Defence Strategy recognises this challenge by adopting a whole-of-government and whole-of-society approach to societal resilience (Ministry of Defence of the Czech Republic, 2023). The question is whether the Czech Republic's strategic communication (STRATCOM) architecture is adequate for that task.

This paper asks why Czech public consent for military investment and NATO commitments is vulnerable to hostile narrative pressure, and to what extent STRATCOM can mitigate that vulnerability. In this paper, public consent refers to sustained public support for three politically consequential commitments: (1) military investment, (2) NATO-centred defence policy including HNS, and (3) acceptance of the costs these commitments impose.

The paper argues that the Czech Republic's STRATCOM framework is not configured to protect the public consent that military investment and NATO commitments require to remain politically sustainable.

Three mutually reinforcing weaknesses create a vulnerability that targeted STRATCOM reform can reduce: (1) a gap between elite and public threat perception, (2) insufficient proactive defence communication, and (3) the functional convergence of Russian and domestic sceptic narratives. However, it cannot substitute for broader political leadership.

For the purposes of this analysis, STRATCOM is defined as the institutional capacity to build and protect public consent for national defence. This concept extends beyond counter-disinformation. Its core purpose is to sustain the political foundation on which military investment and Alliance commitments depend. This definition aligns with the evolving understanding of STRATCOM within NATO and Allied states as a defence-enabling capability rather than a narrow messaging function (NATO, 2023a; Aday et al., 2019).

The paper uses a four-step policy-oriented diagnostic analysis. First, it tests whether a defence-consent gap exists by cross-validating public opinion and expenditure data, primarily from the Public Opinion Research Centre (CVVM), the Institute for Empirical Research (STEM), and NATO data, on threat perception, defence spending, and NATO-related commitments. Second, it maps documented hostile narrative lines using open-source reporting from the Security Information Service (BIS), Centre Against Terrorism and Hybrid Threats (CTHH), the European External Action Service (EEAS), the European Values Center for Security Policy, and the Czech authorities' response to the Voice of Europe case, and assesses whether these narratives target the identified areas of consent fragility. Third, it evaluates the Czech STRATCOM institutional architecture against the vulnerabilities identified in the first two steps. Fourth, it distinguishes between vulnerabilities that STRATCOM reform can address and those requiring broader political action. Finland is used as a bounded benchmark: not as a transferable template, but as a democratic state with a mature whole-of-society defence communication model sustained across decades and across changes of Government.

The analysis is confined to the Czech Republic, to STRATCOM as a specific instrument, and to defence-consent vulnerability in particular. It does not attempt a comprehensive study of Russian information warfare, a comparative analysis of multiple NATO states, or a theory of populism. The institutional assessment relies on open-source indicators. Classified information on Czech STRATCOM capabilities is outside the scope of this paper. Electoral and opinion trends are treated as indicators of societal attitudes, not as objects of partisan evaluation.

The paper proceeds as follows. Chapter 2 diagnoses the structural roots of Czech defence-consent fragility through historical analysis and polling data. Chapter 3 maps documented hostile narrative lines and their convergence with domestic sceptic messaging. Chapter 4 assesses Czech STRATCOM capability against the identified vulnerability and threat, benchmarked against the Finnish model. Chapter 5 proposes targeted reforms linked to specific gaps while specifying the limits of what STRATCOM alone can achieve. Chapter 6 restates the findings and their implications for Czech defence policy.

Chapter 2 — Why Public Consent Is Vulnerable: The Czech Defence Consensus Gap

Czech public consent for defence commitments has not collapsed. The problem is that this consent appears broad in principle but shallow when translated into material costs, operational risk, and Alliance obligations. This chapter argues that the vulnerability has cumulative historical roots and remains politically relevant today. The claim is not that historical experience mechanically determines annual defence budgets or contemporary voting behaviour. Rather, earlier experiences helped shape an interpretive repertoire in which defence is symbolically endorsed but less consistently internalised as an obligation requiring sustained sacrifice and risk-sharing.

Structural roots of Czech defence-consent fragility

The first historical layer is the legacy of the 1938 Munich Agreement. The Franco-British decision to cede the Sudetenland without Czechoslovak participation created a durable narrative that alliances betray small states at moments of greatest need. Zimmermanová and Kříž (2019) traced this narrative through Czech textbooks from 1945 to 2015 and found that its core message, the message of Czech smallness, endured across seventy years and successive political regimes. This does not prove that present-day attitudes are determined by one historical memory. It suggests that doubts about the reliability of alliances and the limited agency of small states remain a culturally available frame when questions of external guarantees and national defence arise.

The second layer is the legacy of the 1968 Warsaw Pact invasion and the period of normalisation that followed. Gabal, Helšusová and Szayna (2002, p. 29) found that the post-1968 era left the Czech public particularly sensitive to the presence of foreign troops on national territory. The same study argues that unlike in Poland or Hungary, the hard orthodoxy that followed 1968 in Czechoslovakia prevented the development of even a minimal community of independent civilian security experts capable of preparing society for alliance membership after 1989 (Gabal, Helšusová and Szayna, 2002, p. 3). As a result, the Czech Republic entered the 1990s with limited civilian capacity to explain defence policy, Alliance obligations, and military reform to a wider public.

The third layer concerns the way NATO accession was domestically framed. Czech political elites presented NATO membership often in civilisational rather than military terms, keeping public debate closer to financial cost-benefit arguments rather than to the obligations membership entailed (Gabal, Helšusová and Szayna, 2002, p. 3). Then-Prime Minister Václav Klaus exemplified this framing when he told an American audience in 1997 that ‘NATO is about ideas, not about enemies’, defining it primarily as an alliance of democratic values (Klaus, 1997). The accession decision was taken without a referendum, despite 71% of respondents in a subsequent survey believing one should have been held (Gabal, Helšusová and Szayna, 2002, p. 23). The result was that many Czech citizens understood NATO membership more as a geopolitical shift toward the West than as accession to an organisation of collective military defence (Gabal, Helšusová and Szayna, 2002, p. 9).

The measurable present condition

These historical roots matter only if they remain visible in current attitudes. The March 2025 survey by CVVM indicates that they do. The survey found that 89% of respondents agreed that state sovereignty must be defended at all costs (CVVM, 2025). Yet 47% also agreed that defending the Czech Republic was not essential because it is a small country whose fate lies in the hands of superpowers (CVVM, 2025), a finding that clearly echoes the ‘message of Czech smallness’ identified by Zimmermanová and Kříž. In the same survey, 39% regarded defence spending as an

unnecessary burden on the budget, and 63% doubted the country's ability to defend itself if something were to happen (CVVM, 2025).

At the same time, support for NATO membership remained comparatively high (CVVM, 2025). CVVM found that 39% were definitely satisfied and a further 37% somewhat satisfied with Czech membership, while 65% judged NATO's existence and actions to have a positive effect on the security of its members (CVVM, 2025). The key issue is therefore not that Czech society categorically rejects NATO or defence. It is that endorsement is uneven. Support is strong at the level of abstract principle, sovereignty, membership, and general security, but weaker when translated into spending, agency, and confidence in national defence capacity. This gap between symbolic approval and practical commitment is the chapter's central indicator of fragility.

Why is the fragility politically relevant

The political relevance of this fragility is visible first in the budgetary record. NATO data show that Czech defence spending, measured as a share of GDP at constant 2021 prices, remained between 0.94% and 1.35% throughout 2014–2023 (NATO, 2025). The 2024 and 2025 figures in the same source are NATO estimates and are therefore not used here. The point is not that the Czech Republic was uniquely low within NATO, but that defence was not treated as a consistently protected political priority over a prolonged period. For a small Allied state whose defence ultimately depends on credibility within a collective system, this pattern is politically significant even if it does not explain any single annual budget decision.

That under-prioritisation coincided with capability deficiencies acknowledged in official Czech defence planning documents. The Czech Armed Forces Development Concept 2030 identifies incomplete modernisation, equipment obsolescence, low manning levels, and insufficient materiel and ammunition stocks as persistent shortcomings (Ministry of Defence of the Czech Republic, 2019). Independent analysis estimates the Czech Republic's defence-related internal debt at between CZK 265 billion and CZK 562 billion (Bahenský et al., 2025, p. 11), while former Defence Minister Jana Černochová has cited estimates ranging from CZK 600 billion to CZK 1 trillion when inflation is accounted for (Chamber of Deputies of the Parliament of the Czech

Republic, 2025). The precise figure is contestable, but the broader conclusion is harder to dispute: long-term underinvestment left a substantial backlog in armament, equipment, materials, and infrastructure. This does not show that public attitudes directly determined budget outcomes. Coalition politics, fiscal choices, and procurement cycles also mattered. This pattern may have reduced the political pressure for sustained defence prioritisation.

Conditional solidarity towards Allies points in the same direction. STEM found that 82% of respondents would support sending Czech troops to help neighbouring Poland if attacked, but only 65% would support doing so for the Baltic states (STEM, 2024).

These data indicate that Alliance solidarity is not absent in principle, but that its stability appears conditioned by proximity and relevance. Support is stronger where obligations feel immediate and intuitively connected to Czech security, and weaker where they appear more distant or abstract.

The argument of this chapter is therefore limited but important. Historical legacies are not presented here as a one-sided explanation for any single policy. Rather, they help explain why present-day Czech defence consent remains vulnerable. Support for defence and NATO exists, but it is more robust in principle than in sustained spending, risk-sharing, and distant Alliance obligations.

That condition does not, by itself, produce hostile-narrative success, but it creates conditions in which such narratives can work more effectively. Chapter 3 turns directly to that mechanism.

Chapter 3 — How Hostile Narratives Exploit the Vulnerability

Documented Russian narratives targeting the Czech defence consent

BIS assessed 2024 as one of the most demanding recent years for Czech security, describing a Russian information environment that relied less on open propaganda and more on manipulation channelled through local intermediaries and domestically understandable themes (BIS, 2025). This shift matters analytically because the most

effective hostile messages are not necessarily presented as foreign messages. They are embedded in claims that can circulate as ordinary domestic arguments.

Open-source monitoring points to three recurring narrative lines relevant to Czech defence consent. BIS documents Russian use of local proxies and anti-NATO or anti-Western narratives in the Czech information environment (BIS, 2024; BIS, 2025). EEAS reporting identifies Russian Foreign Information Manipulation and Interference (FIMI) themes aimed at Alliance division, war fatigue, and reduced support for Ukraine (European External Action Service, 2024). European Values Center for Security Policy monitoring shows similar themes circulating in Czech-language disinformation ecosystems (European Values Center for Security Policy, 2023). The first line frames NATO and the wider West as escalatory actors whose policies increase rather than reduce the risk of conflict. The second presents defence spending and military support for Ukraine as wasteful burdens that divert resources from domestic social needs. The third portrays neutrality, restraint, or distance from Alliance commitments as safer than sustained military and political engagement. The pressure mechanism is therefore threefold: (1) anti-NATO narratives target Alliance trust, (2) cost narratives target support for military investment, and (3) neutrality narratives target willingness to accept risk-sharing obligations.

The most concrete attributable case is the Voice of Europe network, a Prague-based Russian influence operation exposed by Czech authorities in 2024. BIS linked the network to Russian influence activity, and the Ministry of Foreign Affairs subsequently announced that the European Union had placed Voice of Europe, Viktor Medvedchuk, and Artem Marchevskyi on the sanctions list following a Czech proposal (BIS, 2024; Ministry of Foreign Affairs of the Czech Republic, 2024). The case supports three points relevant to this analysis. First, Russian information operations in the Czech Republic are operational and attributable. Second, they are designed to work through localised, politically resonant messaging rather than easily identifiable foreign propaganda. Third, the Czech state itself has formally identified and acted against them, making the threat assessment presented here consistent with official Czech findings rather than external speculation.

Functional convergence with domestic sceptic messaging

The analytically decisive point is not whether Russian operations directly control domestic political messaging. Such a claim cannot be methodologically proven from open sources and is not made here. The point is that narratives consistent with documented Russian information objectives can receive domestic support through channels that operate independently. The relevant framework is the convergence of effect, not the attribution of intent. The argument is not that domestic scepticism is illegitimate or externally directed; it is that analytically similar claims can, irrespective of origin, have similar erosive effects on defence consent.

Czech analytical monitoring indicates that themes matching the three narrative lines identified above recur in domestic political discourse, media commentary, and public debate on defence decisions (European Values Center for Security Policy, 2023). When a Czech citizen encounters the claim that NATO provokes Russia, that defence spending is a burden, or that neutrality would be safer, the erosive effect on defence consent may be similar even though the origin, intent, and legitimacy of the sources differ. The structural vulnerability diagnosed in Chapter 2, broad but shallow Alliance support, historically rooted scepticism of foreign military commitments, and support that weakens when translated into material cost or distant obligations, creates an environment in which adversarial and domestically generated scepticism can reinforce one another. The EEAS has documented this pattern across multiple EU member states, noting that hostile foreign information manipulation is most effective where it amplifies existing divisions rather than introducing completely foreign narratives into a target society (European External Action Service, 2024).

The cumulative effect on the political base for defence

The strategic significance of narrative pressure is not that it changes individual minds overnight. It is that repeated exposure to convergent messages may make support for defence spending, military assistance, and Alliance obligations more politically questionable over time. In a society where support already appears stronger in principle than in material commitment, narratives that stress provocation, cost, or the

appeal of neutrality can reinforce hesitation and make politically challenging defence decisions harder to sustain.

The Czech case does not allow for a direct causal claim linking hostile narratives to any single budgetary or institutional decision, and this chapter does not make one. The more limited conclusion is that documented hostile narrative lines, one attributable influence case, and evidence of convergence with domestically circulating sceptical claims together indicate a plausible, persistent, and strategically relevant pressure mechanism. The vulnerability identified in Chapter 2 does not, by itself, cause the success of hostile narratives, but it helps explain why such narratives can gain leverage in the Czech case. Chapter 4, therefore, turns from the pressure mechanism to the institutional question: whether Czech STRATCOM capability is set to protect public consent against this convergent pressure, or whether the institutional response remains oriented toward a different and narrower task.

Chapter 4 — Czech STRATCOM Capability: A Gap Analysis

Chapters 2 and 3 established that Czech public consent for defence is structurally vulnerable and under active pressure from convergent narratives. This chapter examines whether the Czech state's STRATCOM architecture is configured to protect that consent. The focus is on institutional arrangements, mandates, and continuity. It does not measure operational effectiveness, which would require classified material outside the scope of this paper. Finland serves as a bounded benchmark, not as a transferable template. As a democratic state that has maintained a whole-of-society defence communication architecture across decades and across changes of Government (Raitasalo, 2023), it offers concrete institutional referents against which gaps in the Czech system can be evaluated.

The current Czech STRATCOM institutional landscape

The Czech framework is not empty. At the policy level, it is explicit. The National Strategy for Countering Hybrid Interference, approved by the Government in April 2021, frames the response as a whole-of-society task and envisages the development of a national STRATCOM system (Ministry of Defence of the Czech Republic, 2021).

The Action Plan for 2025 defines three pillars: (1) systemic and holistic approach, (2) resilience of society and critical infrastructure, and (3) adequate response capability (Ministry of Defence of the Czech Republic, 2025a). The 2023 Defence Strategy reinforces this framework by adopting a whole-of-government and whole-of-society approach and by tasking the education system to promote security-relevant knowledge and willingness to participate in defence (Ministry of Defence of the Czech Republic, 2023, para. 48). The POKOS 2025–2030 concept, approved on 8 January 2025, explicitly acknowledges previous fragmentation, broadens preparation beyond the Ministry of Defence alone, and defines four pillars including STRATCOM (Ministry of Defence of the Czech Republic, 2025b).

Implementation at the level of standing institutions is narrower. The CTHH, operating within the Ministry of Interior since 1 January 2017, is a permanent unit monitoring terrorism, extremism, and disinformation campaigns related to internal security. Its mandate has not been extended to proactive defence communication aimed at sustaining consent for military investment and Alliance commitments (Ministry of the Interior of the Czech Republic, 2017). Two successive central coordinating functions have not survived. The position of Government Commissioner for Media and Disinformation, established in March 2022, was abolished in February 2023, with coordination shifted to the National Security Adviser (Government of the Czech Republic, 2023). The STRATCOM Department at the Office of the Government, which had been the closest institutional equivalent to a central STRATCOM coordinating function, was dissolved with effect from 1 January 2026 (Office of the Government of the Czech Republic, 2026). Relevant central coordinating arrangements have therefore been created, transferred, or abolished in short succession. Meanwhile, the standing CTHH remains in place, but with a mandate limited to internal security analysis rather than proactive defence communication.

Capability gaps against the three vulnerabilities

When assessed against the identified vulnerabilities, three gaps remain visible. Each gap is assessed by comparing the institutional requirements stemming from Chapters 2 and 3 with the mandates, continuity, and target groups of the mechanisms that currently exist.

First, a defence literacy gap persists at the level of societal leadership. Closing the gap between the threat assumptions embedded in Czech defence policy and the depth of public consent needed to sustain them politically requires repeated, nonpartisan, cross-sector exposure of senior civilian and military actors to a shared framework for understanding defence obligations, Alliance commitments, and national resilience. POKOS 2025–2030 broadens the target audience beyond schools to include public administration and other groups relevant to defence, an advance over the previous narrower focus. It does not, however, establish a standing mechanism to regularly integrate politicians, senior civil servants, business leaders, journalists, and civil society actors into a common defence literacy framework. What exists is a broadened citizen-preparation policy, not a resilient institution for integrating societal leadership.

Second, the system lacks coordination for proactive defence communication protected from political turmoil. The 2021 Strategy and the Action Plan both identified the need for a national STRATCOM system, but the coordinating architecture intended to carry that agenda has not survived. The Commissioner's role was short-lived, and the Office of the Government's STRATCOM Department has been dissolved. Distributed responsibility across several bodies is not necessarily a weakness, but in the Czech case, the evidence shows that policy ambition exceeds the durability of coordinating arrangements across political cycles.

Third, a functional mismatch remains between counter-disinformation and proactive defence communication. The Czech architecture contains monitoring, hybrid-awareness, and resilience functions through the CTHH, intelligence services, the Security Council of the State, and the Ministry of Defence policy documents. Open sources do not identify a standing institutional mechanism tasked specifically with explaining why defence investment, Alliance commitments, and societal preparedness are politically necessary over time. This task includes sustaining the case for those measures when they become costly or controversial.

Finland as a bounded benchmark

Finland is used as a benchmark not because its historical experience parallels that of the Czech Republic, it does not, but because it demonstrates how a democratic state can institutionalise defence communication as resilient state architecture rather than temporary policy preference. The Finnish Security Strategy for Society defines comprehensive security (*kokonaisturvallisuus*) as collaboration among authorities, business, organisations, and citizens, built around seven vital functions of society, including defence capability and psychological resilience (Security Committee of Finland, 2025a). Its implementation is monitored annually through a Security Report for Society. The Security Committee provides a permanent, broad-based cooperation body for comprehensive security preparedness and assists the Government and ministries in coordinating proactive preparedness. Its continuity is reinforced by the stated aim that the general principles of Finland's Security Strategy for Society should last across different government terms (Security Committee of Finland, 2025b).

The mechanism most directly relevant to the Czech gap analysis is the system of National Defence Courses (*maanpuolustuskurssit*), organised by the Finnish National Defence University since 1961, with regional defence courses following shortly thereafter. The national courses are held four times per year. Participants are selected by a cross-sector advisory board and drawn from senior civilian and military actors, including politicians, civil servants, business leaders, media figures, academics, and civil society leaders. More than 10,000 influential members of Finnish society have attended the courses over the years, and the programme has continued through every change of Finnish Government since 1961 (Finnish National Defence University, 2025). The Advisory Board for Defence Information (ABDI), a parliamentary forum under the Ministry of Defence, complements this ecosystem by commissioning regular public-opinion surveys and sustaining dialogue on security policy, national defence, and preparedness communication (Advisory Board for Defence Information, 2025). These mechanisms are not directly transferable as a whole. However, they identify what the Czech system currently lacks: a permanent coordination core, a recurring mechanism of leadership literacy across sectors, and institutional continuity across political cycles.

Synthesis

The Czech STRATCOM framework is better understood as partially configured than as absent. It includes explicit policy recognition of whole-of-society resilience, a standing internal security capability in the CTHH, and a broadened citizen-preparation concept in POKOS 2025–2030. These are meaningful components. They do not, however, close the three capability gaps central to this paper's research question. Open sources do not show a continuity-protected central coordinating function for STRATCOM, a standing mechanism for cross-sector defence literacy at societal-leadership level, or a resilient institutional answer to the need for proactive defence communication to the convergence problem described in Chapter 3. The Czech system recognises the problem and has assembled relevant pieces. It has not yet institutionalised them into a sufficiently stable architecture for protecting public consent over time. Chapter 5, therefore, turns from diagnosis to the question of what STRATCOM can, and cannot, realistically improve.

Chapter 5 — Recommendations: What STRATCOM Can and Cannot Fix

Chapter 4 identified three specific capability gaps in the Czech STRATCOM architecture: (1) the lack of a resilient, recurring mechanism for cross-sector defence literacy at the societal-leadership level, (2) the lack of continuity-protected central coordination for proactive defence communication, and (3) the orientation of existing institutional capability toward reactive counter-disinformation rather than sustained proactive communication. This chapter proposes targeted reforms linked directly to each gap, then specifies the limits of what STRATCOM alone can achieve. The delineation is important because the paper has insisted on rejecting causal claims that lack supporting evidence. The same approach applies to its own recommendations.

Three targeted reforms

First: Establish a standing leadership defence-literacy mechanism.

The Czech Republic should establish a standing Czech Defence and Security Course for senior civilian and military leadership, modelled on the principles of the Finnish

National Defence Courses but adapted to Czech conditions. The course should begin at an annual or semi-annual pace, following the Finnish principle of sustained, nonpartisan, cross-sector participation rather than trying to replicate Finnish design parameters that evolved over six decades. Participant selection should be conducted by a nonpartisan advisory board composed of representatives from state institutions, professional associations, and academia. A university-based host, most plausibly the University of Defence, would combine academic standing, security-clearance capacity, and relative insulation from short political cycles. Such a course would not shift public attitudes directly. However, over time, it would build a network of senior societal figures with a common framework for defence obligations, Alliance commitments, and national resilience. The POKOS 2025–2030 concept already envisages broader engagement with public administration and selected target groups (Ministry of Defence of the Czech Republic, 2025b). A standing leadership course would give that broader engagement a resilient institutional form.

Second: Anchor STRATCOM coordination above the routine executive level.

The central coordinating function for STRATCOM should be anchored in a way that is institutionally resilient across changes of Government. The preferred option is a formalised coordinating secretariat under the Security Council of the State, with cross-government backing and a level of institutional anchoring that protects it from the executive reorganisations that abolished the Government Commissioner and the Strategic Communication Department. That option is preferable to another temporary office because it better fits the Czech constitutional-administrative structure, links STRATCOM to an existing security decision-making body, and offers a better chance of survival across changes of Government. The 2021 National Strategy for Countering Hybrid Interference envisaged the development of a national STRATCOM system (Ministry of Defence of the Czech Republic, 2021), but the principal coordination arrangements intended to carry that agenda have failed to prove durable. A more firmly anchored coordinating function would create the continuity protection that the Government Commissioner for Media and Disinformation and the Office of the Government STRATCOM Department lacked. The Finnish Security Committee, whose secretariat sits at the Ministry of Defence and has operated across changes of

Government (Security Committee of Finland, 2025b), offers a concrete illustration of what such continuity can look like in practice.

Third: Reposition POKOS STRATCOM toward sustained proactive defence communication.

The STRATCOM pillar of POKOS 2025–2030 should be repositioned from general awareness-building to sustained proactive defence communication, with clearly defined institutional ownership, a dedicated budgetary line, and explicit performance indicators. Ownership should sit with the central coordinating body recommended above, while implementation should remain distributed across the relevant ministries and institutions. Performance indicators should include at least (1) public awareness and trust metrics gained from regular surveys, (2) elite-participation metrics measuring reach of proactive communication across Government and non-government leadership, and (3) continuity metrics tracking institutional stability across government changes. Building on POKOS rather than displacing it preserves the policy continuity that the Czech system has struggled to sustain. This reform would complement rather than replace the monitoring and counter-disinformation work of the CTHH, which would continue in its existing internal security area.

The limits of STRATCOM

STRATCOM cannot substitute for broader political leadership and should not be expected to do so. Three specific limits are worth naming.

First, STRATCOM cannot determine the underlying political economy of Czech defence commitments, which is shaped by coalition bargaining, fiscal constraints, procurement cycles, and competing social priorities, including healthcare, pensions, and education. Better institutionalised STRATCOM would change the conditions of public debate; it would not guarantee budget outcomes.

Second, the historical interpretive repertoire documented in Chapter 2 has generational depth. Institutional communication can reduce the political resonance of specific narratives and strengthen the public's capacity to evaluate defence

commitments on their merits over time. However, the Munich legacy, the memory of 1968, and the civilisational framing of accession will not be dissolved by any reform deliverable within the time horizon of a ten-year concept.

Third, and most importantly, partisan contestation over defence is a legitimate feature of democratic politics, not an object of counter-narrative work. Citizens are entitled to debate defence spending, Alliance commitments, and burden-sharing, and a healthy democracy requires that they do. The purpose of STRATCOM is to ensure that such debate takes place based on accurate information and a shared understanding of what defence commitments entail, not to suppress disagreement or pre-determine its outcome. The reforms proposed above are designed to strengthen the institutional conditions for informed public deliberation, not to engineer any particular political outcome.

The appropriate formulation is therefore bounded. STRATCOM can mitigate this vulnerability by improving defence literacy, coordination, and sustained proactive explanation of defence commitments. It cannot resolve fiscal trade-offs, historical scepticism, partisan contestation, or the absence of sustained political leadership. Well-institutionalised STRATCOM can reduce the conditions under which hostile narratives gain leverage and provide proactive defence communication with the continuity it currently lacks. It can improve the quality of the national conversation about defence, but it cannot guarantee consensus, fiscal prioritisation, or strategic clarity from elected leaders. Chapter 6 draws the overall conclusions of the paper.

Chapter 6 — Conclusion

This paper asked why the Czech public's consent for military investment and NATO commitments is vulnerable to hostile narrative pressure. Its central argument has been that the Czech Republic's STRATCOM framework is not configured to protect the public consent on which those commitments depend. The problem is not the absence of public support for defence as such. It is that support remains broader at the level of principle than at the level of sustained spending, practical risk-sharing, and sustainable acceptance of the obligations that collective defence entails.

The analysis was carried out in four steps. Chapter 2 showed that this vulnerability is rooted in a cumulative historical and political context: the legacy of Munich, the memory of 1968, and the public framing of NATO accession all helped sustain an interpretive repertoire in which defence and alliance commitments are endorsed symbolically but less consistently internalised as obligations requiring sacrifice. Current polling indicates that this pattern remains visible. Chapter 3 then showed that hostile Russian narratives do not need to construct this vulnerability from nothing. They are most effective when they amplify existing doubts through narrative lines that resonate with domestic scepticism and reinforce the same erosive effects, even without implying common intent or direct control. Chapter 4 demonstrated that the Czech STRATCOM framework is only partially configured to respond to this condition. Policy recognition of whole-of-society resilience exists, and the state has assembled relevant elements through a hybrid-threat strategy, internal security monitoring, and broader citizen-preparation concepts. Yet the institutional architecture remains fragmented and insufficiently resilient. Chapter 5, therefore, argued that STRATCOM reform can still matter, but only in a bounded sense, by improving leadership-level defence literacy, protecting coordination from repeated institutional changes, and shifting communication from reactive counter-disinformation toward sustained proactive explanation of why defence commitments are politically necessary.

The broader conclusion is therefore straightforward. Czech STRATCOM is better understood not as a peripheral messaging function, but as part of the state architecture required to keep defence policy politically sustainable under pressure. It can mitigate vulnerability by improving defence literacy, resilient coordination, and proactive explanation of defence commitments. It cannot substitute for political leadership exercised consistently across governments nor can it eliminate legitimate democratic disagreement. Those limits are not a weakness of the argument; they are a condition of its credibility.

For the Czech Republic, the strategic issue is whether the state can sustain public consent for defence despite hostile narrative pressure. The analysis in this paper suggests that, at present, the answer is only partial. If Czech defence policy is to remain credible, resilient, and politically sustainable over time, the protection of public consent must be treated as one of the enabling conditions of national defence itself.

Abbreviation	Meaning
ABDI	Advisory Board for Defence Information
BIS	Security Information Service
CTHH	Centre Against Terrorism and Hybrid Threats
CVVM	Public Opinion Research Centre
EEAS	European External Action Service
FIMI	Foreign Information Manipulation and Interference
HNS	Host Nation Support
NATO	North Atlantic Treaty Organization
POKOS	Preparation of Citizens for National Defence
STEM	Institute for Empirical Research
STRATCOM	Strategic Communication

Bibliography

ADAY, Sean et al. 2019. Hybrid Threats: A Strategic Communications Perspective [online]. Riga: NATO Strategic Communications Centre of Excellence. Available at: https://stratcomcoe.org/publications/hybrid-threats-a-strategic-communications-perspective/79 [Accessed: 23 April 2026].

ADVISORY BOARD FOR DEFENCE INFORMATION. 2025. The Advisory Board for Defence Information [online]. Helsinki: Ministry of Defence. Available at: https://defmin.fi/en/the-advisory-board-for-defence-information-abdi [Accessed: 23 April 2026].

BAHENSKÝ, Vojtěch et al., 2025. Defence Spending: Why It Needs to Be Significantly Increased and How to Fund It [online]. Prague: Peace Research Center Prague and Centre for Public Finance, April 2025. Available at: https://centrumverejnychfinanci.cz/wpcontent/uploads/2025/04/Vydaje_na_obranu.pdf [Accessed: 23 April 2026].

BIS. 2024. Annual Report of the Security Information Service for 2023 [online]. Prague: Security Information Service. Available at: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2023-vz-cj.pdf [Accessed: 23 April 2026].

BIS. 2025. Annual Report of the Security Information Service for 2024 [online]. Prague: Security Information Service. Available at: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2024-vz-cj.pdf [Accessed: 23 April 2026].

CHAMBER OF DEPUTIES OF THE PARLIAMENT OF THE CZECH REPUBLIC. 2025. Stenographic Record of the Debate on the Government Bill Amending Act No. 219/1999 Coll., on the Armed Forces of the Czech Republic, Parliamentary Print 852, Second Reading [online]. Prague: Chamber of Deputies of the Parliament of the Czech Republic, 13 March 2025. Available at: https://www.psp.cz/eknih/2021ps/stenprot/132schuz/bqbs/b03800801.htm [Accessed: 23 April 2026].

CVVM. 2025. Citizens on the Defence of the Czech Republic and Membership in NATO - March 2025 [online]. Prague: Institute of Sociology of the Czech Academy of Sciences. Available at:

https://cvvm.soc.cas.cz/images/articles/files/5948/pm250514.pdf [Accessed: 23 April 2026].

EUROPEAN EXTERNAL ACTION SERVICE. 2024. 2nd EEAS Report on Foreign Information Manipulation and Interference Threats [online]. Brussels: European External Action Service. Available at: https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en [Accessed: 23 April 2026].

EUROPEAN VALUES CENTER FOR SECURITY POLICY. 2023. Annual Report on the State of the Czech Disinformation Scene for 2022 [online]. Prague: European Values Center for Security Policy. Available at: https://europeanvalues.cz/wp-content/uploads/2023/06/EN_Annual_Report_on_the_State_of_the_Czech_Disinformation_Scene_for_2022.pdf [Accessed: 23 April 2026].

FINNISH NATIONAL DEFENCE UNIVERSITY. 2025. Finnish National Defence Courses [online]. Helsinki: Finnish National Defence University. Available at: https://maanpuolustuskorkeakoulu.fi/en/mpk-about-us [Accessed: 23 April 2026].

GABAL, Ivan, HELŠUSOVÁ, Lenka and SZAYNA, Thomas S. 2002. The Impact of NATO Membership in the Czech Republic: Changing Czech Views of Security, Military and Defence. Camberley: Conflict Studies Research Centre, Royal Military Academy Sandhurst. Available at: https://www.files.ethz.ch/isn/97457/02_Mar_2.pdf [Accessed: 23 April 2026].

GOVERNMENT OF THE CZECH REPUBLIC. 2023. Government Commissioner for Media and Disinformation [online]. Prague: Government of the Czech Republic. Available at: https://vlada.gov.cz/cz/ppov/zmocnenci_vlady/vladni-zmocnenec-pro-oblast-medii-a-dezinformaci-194841/ [Accessed: 23 April 2026].

KLAUS, Václav. 1997. The Importance of NATO Enlargement to the Czech Republic [online]. Washington, DC: The Heritage Foundation, 12 November 1997. Available at: https://www.heritage.org/europe/report/the-importance-nato-enlargement-the-czech-republic [Accessed: 23 April 2026].

MINISTRY OF DEFENCE OF THE CZECH REPUBLIC. 2019. The Czech Armed Forces Development Concept 2030 [online]. Prague: Ministry of Defence of the Czech Republic. Available at: https://www.mo.gov.cz/assets/en/ministry-of-defence/basic-documents/cafdc.pdf [Accessed: 23 April 2026].

MINISTRY OF DEFENCE OF THE CZECH REPUBLIC. 2021. National Strategy for Countering Hybrid Interference [online]. Prague: Ministry of Defence of the Czech

Republic. Available at: https://www.mo.gov.cz/assets/en/ministry-of-defence/basic-documents/national-strategy---aj-final.pdf [Accessed: 23 April 2026].

MINISTRY OF DEFENCE OF THE CZECH REPUBLIC. 2023. Defence Strategy of the Czech Republic 2023 [online]. Prague: Ministry of Defence of the Czech Republic. Available at: https://www.mo.gov.cz/assets/en/ministry-of-defence/basic-documents/defence-strategy-of-the-czech-republic_2023_final.pdf [Accessed: 23 April 2026].

MINISTRY OF DEFENCE OF THE CZECH REPUBLIC. 2025a. Action Plan to the National Strategy for Countering Hybrid Interference for 2025 [online]. Prague: Ministry of Defence of the Czech Republic. Available at: https://mise.mo.gov.cz/assets/dokumenty-a-legislativa/dokumenty/akcni-plan-k-narodni-strategii-pro-celeni-hybridnimu-pusobeni-na-rok-2025.pdf [Accessed: 23 April 2026].

MINISTRY OF DEFENCE OF THE CZECH REPUBLIC. 2025b. Concept for the Preparation of Citizens for National Defence 2025-2030 [online]. Prague: Ministry of Defence of the Czech Republic. Available at: https://mocr.mo.gov.cz/assets/informacni-servis/zpravodajstvi/koncepce-pokos-2025-2030_final.pdf [Accessed: 23 April 2026].

MINISTRY OF FOREIGN AFFAIRS OF THE CZECH REPUBLIC. 2024. EU Puts Voice of Europe and Two Other Entities on Sanctions List as a Result of Czech Proposal [online]. Prague: Ministry of Foreign Affairs of the Czech Republic, 27 May 2024. Available at: https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/eu_puts_voice_of_europe_and_two_other.html [Accessed: 23 April 2026].

MINISTRY OF THE INTERIOR OF THE CZECH REPUBLIC. 2017. Centre Against Terrorism and Hybrid Threats [online]. Prague: Ministry of the Interior of the Czech Republic. Available at: https://mv.gov.cz/chh/clanek/centre-against-terrorism-and-hybrid-threats.aspx [Accessed: 23 April 2026].

NATO. 2023a. Allied Joint Doctrine for Strategic Communications (AJP-10), Edition A, Version 1 [online]. Brussels: NATO Standardization Office. Available at: https://nso.nato.int/nso/nsdd/main/list-promulg [Accessed: 23 April 2026].

NATO. 2025. Defence Expenditure of NATO Countries (2014-2025) [online]. Brussels: NATO Public Diplomacy Division. Available at:

https://www.nato.int/content/dam/nato/webready/documents/finance/def-exp-2025-en.pdf [Accessed: 23 April 2026].

OFFICE OF THE GOVERNMENT OF THE CZECH REPUBLIC. 2026. Information Concerning the Office of the Government of the Czech Republic [online]. Prague: Office of the Government of the Czech Republic. Available at: https://vlada.gov.cz/cz/urad-vlady/poskytovani-informaci/poskytnute-informace-na-zadost/informace-tykajici-se-uradu-vlady-cr-226052/ [Accessed: 23 April 2026].

RAITASALO, Jyri. 2023. Finnish Defense 'Left of Bang'. *PRISM*. 10(2), 78-91. Available at: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3323915/finnish-defense-left-of-bang/ [Accessed: 23 April 2026].

SECURITY COMMITTEE OF FINLAND. 2025a. Security Strategy for Society: Government Resolution [online]. Helsinki: Finnish Government, 16 January 2025. Available at: https://julkaisut.valtioneuvosto.fi/items/0126122a-1e8a-4ffa-9868-6286292efc01 [Accessed: 23 April 2026].

SECURITY COMMITTEE OF FINLAND. 2025b. The Security Committee [online]. Helsinki: Security Committee of Finland. Available at: https://turvallisuuskomitea.fi/en/security-committee/ [Accessed: 23 April 2026].

STEM. 2024. Decline in Trust in the Army Among the Czech Public Is Linked to Political Preferences [online]. Prague: STEM, 18 June 2024. Available at: https://www.stem.cz/en/decline-in-trust-in-the-army-among-the-czech-public-is-linked-to-political-preferences/ [Accessed: 23 April 2026].

ZIMMERMANOVÁ, Lucie and KŘÍŽ, Zdeněk. 2019. The Evolution of the Munich Betrayal Myth: Analysis of the Munich Conference Interpretation in Czech Textbooks Before and After the Velvet Revolution. *The Journal of Slavic Military Studies*. 32(2), 178-209. DOI: 10.1080/13518046.2019.1616921.

BEST ESSAY OF THE COMMAND SENIOR ENLISTED LEADERS COURSE

WO Ben HOWARTH: Between Inclusion and Security: Estonia's Generational Path toward Integrating its Russian-Speaking Minority under the Shadow of Russia

Supervisor: Dr. Viljar VEEBEL

Statement on the Use of AI Tools:

ChatGPT and Copilot were utilised to assist in sourcing references for this essay. All references were independently verified for legitimacy and academic rigor. Grammar and spelling were reviewed using the basic Grammarly package. The content, structure, and arguments presented are entirely the author's own.

In April 2007, Estonian authorities removed the Bronze Soldier monument from Tallinn's Tõnismägi Square. For many Russian-speaking Estonians, the monument had served as a focal point for commemorations on 9 May, coinciding with Russia's Victory Day celebration. Its relocation to a military cemetery elsewhere in the city provoked significant civil unrest and riots, later termed the Bronze Night (Monument of contention). At the time of its removal, Estonia had been a member of the European Union (EU) for three years, and the move was interpreted in different ways. For some, it symbolised Estonia's attempt to distance itself from its Soviet past and to consolidate a coherent Estonian national identity. However, many Russian speakers perceived it as an assault on their collective memory and cultural identity (Davydova, 2008, p.393). Other commentators (Saarts, 2008) and academics (Juurvee & Mattiisen 2020, p.11-13 & Ehala, 2009, p.143) did not see the riots as orchestrated from Moscow alone, but argue they were the result of long-standing issues of inequality, political exclusion, unbalanced representation, and majoritarian governance. This suggests that the removal of the statue tapped into deeper grievances about status, recognition and exclusion in Estonian society.

Whilst many Russian speakers hold Estonian citizenship, they also maintain cultural ties to Russia through language, memory, and cultural practices. This dynamic reflects a broader challenge common to post-Soviet societies, where national loyalty is intertwined with historical narratives and ethnic heritage. The civil unrest of the Bronze Night illustrated deep tension in cultural and national identification among Estonia's Russophone population, but a divergence in thinking exists in theories as to the source of the unrest. Whilst the monument relocation and Russian information operations were triggers, could the socio-economic marginalisation of the Russian-speaking minority have helped create a domestic demographic prone to civic mobilisation and vulnerable to manipulation from foreign powers, namely Russia?

This essay will explore Estonia's delicate balance between safeguarding national security and adhering to the liberal democratic norms expected by its Western European partners. It will posit that liberal inclusion and national security, often portrayed as opposing forces, have instead evolved interdependently. In its

generational path toward integrating its Russian-speaking minority, each dynamic has shaped the other, with Estonia regulating its policies against the backdrop of an enduring threat of Russian aggression and the demands of European integration. Central to this thesis is the change in policy after the Bronze Night, where historical reconciliation was melded with economic inclusion and political agency. Issues that, if neglected, risked reinforcing divisions that Russia could readily exploit for geopolitical leverage.

It will start by outlining the historical context and identity formation of Estonia's Russian-speaking population, tracing how Soviet-era russification and post-Soviet demographic shifts shaped current dynamics. This setting will provide the backdrop for an analysis of Estonian citizenship and integration policies, assessing how Estonia's legal framework and post-independence reforms affected inclusion and political participation. From here, it will segue into an exploration of external influences, primarily Russia's compatriot and passportisation policy and the role of Russian-language media. Finally, it considers security, cohesion, and nation-building, evaluating Estonia's efforts to balance liberal freedoms with national security in a hostile geopolitical environment.

Estonia's Russian-speaking population emerged as a direct result of Soviet russification policies, which aimed to alter the demographic balance of satellite states and strengthen Moscow's control. This policy had deep historical roots in the Russian Empire's westward expansion and its self-conception as a European power (Brüggemann & Kasekamp, 2008, p.428). During the Soviet period, organised population transfers into Estonia served to ensure that no non-Russian majority region could challenge central authority while providing labour for industrialisation and infrastructure projects (Hirsch, 2005, p.62-98).

The industrialisation of northeastern Estonia, particularly in Ida-Virumaa, attracted thousands of migrants. Between the 1960s and 1980s, many Russian speakers from across the Soviet Union moved to Estonia, drawn by higher living standards and better housing than elsewhere in the Soviet Union (ibid). These migrations established enduring Russian-speaking communities that maintained strong familial and cultural ties to Russia through shared language, Soviet-era education, and historical memory.

The collapse of the Soviet Union in 1991 abruptly ended this system. The newly restored Estonian state adopted a restorationist citizenship model, automatically granting citizenship only to those who had held it before Soviet annexation in 1940 and their descendants (Galbreath, 2005, p.35). Ethnic Russians who had migrated during Soviet rule were excluded. The Aliens Act (*Välismaalaste seadus*) of 8 July 1993 designated these Russian-speakers as 'foreigners', requiring residence permits (Aliens Act of the Republic of Estonia, 1993). In 1995, Estonia passed the Citizenship Act, introducing a path to naturalisation that included language and civics tests. However, many Russian-speakers saw these conditions as exclusionary and as favouring Estonian linguistic identity while disregarding their Soviet past. Those who did not or could not naturalise became 'non-citizens' or 'stateless aliens', lacking national voting rights and occupying a legally marginal position. These exclusionary laws framed Russian-speakers as 'occupiers' or potential 'fifth column' actors with political and cultural discourse in the 1990s, often portraying them as security risks or remnants of Soviet colonisation (Schulze & Pupcenoks, 2024, p.1039).

Human Rights Watch (Human Rights Watch, 1993, Online) reported that such policies deepened civic mistrust throughout the 1990s, even as Estonia pursued membership of international institutions such as the EU and North Atlantic Treaty Organisation (NATO). Liberal reforms, designed to meet EU and NATO accession standards, required the demonstration of democratic values and minority rights. Yet the underlying security logic of its citizenship model persisted. While Estonia liberalised its market economy and legal institutions, its approach to citizenship remained cautious, with inclusion often subordinated to security. EU accession in 2004 prompted partial liberalisation, but some scholars argue that inclusion was securitised and adopted primarily to satisfy Western expectations while preserving domestic control (Schulze & Pupcenoks, 2024, p.1039-1041). A report by the International Centre for Defence and Security (ICDS) emphasised that socio-economic marginalisation and limited political avenues for Russian-speakers helped create a domestic environment where there was an increasing potential for civil unrest amongst Russian-speakers (Juurvee & Mattiisen, 2020, p.11). Further qualitative evidence argues that economic discrimination and perceptions of political ostracism helped consolidate a distinct Russian-speaking identity (Cheskin, 2015, p.84).

The education system illustrates the duality between both ethnic groups. Estonia maintained a dual network of Estonian and Russian language schools, often with minimal interaction between linguistic communities (Council of Europe, 2022). This separation produced different outcomes with second-generation Russian youth lagging behind their Estonian peers in higher education transitions and civic participation. These divisions persisted well into the 2010s and are visible in employment and incarceration data. For example, in 2021 ‘stateless aliens’ made up 5% of the Estonian general population but represented 24% of the prison population (Norberg & Norberg, 2024). The EU and the Organisation for Economic Co-operation and Development (OECD) criticised the marginalisation of Russian-speakers’ political rights (Kondan et al., 2021), with studies as recent as 2019 (Musset et al., 2019, p.27-47) highlighting that socio-economic divides between ethnic Estonians and Russian-speaking minorities remain pervasive. A more recent study from 2021 argues that among Russian-speakers, unemployment and the risk of poverty is significantly higher, the share of Russian-speakers in lower-skilled jobs is disproportionately large and those with Russian citizenship or undetermined status are faring worse in income and job security (Kondan et al., 2021). These metrics demonstrate a significant void in Russian-speakers' capacity to determine their own agency. Structural limitations, implemented in the decade after Estonia’s independence, continue to hinder certain demographics within the Russian-speaking diaspora. This in turn, erodes their trust in domestic political structures and further hinders civic integration.

In the immediate post-Cold War years, Estonia’s citizenship and language laws reflected an acute desire to restore a cohesive, ethnically Estonian national identity after decades of Soviet occupation. These measures, often characterised by critics as exclusionary or illiberal, were nevertheless defended by Estonian policymakers as essential to consolidating state sovereignty and protecting against potential external subversion. Brubaker’s triadic nexus helps explain this dynamic. In his model, the nationalising state, an external homeland, and a transnational minority form a triangle of pressures that drive exclusionary politics (Fedorenko & Umland, 2021, p.60).

The policies Estonia has established, attempting to balance the tension between domestic cohesion, liberal inclusivity and national security have been crafted in the persistent shadow of Russian hybrid influence. The Kremlin’s perception of the

Russian diaspora as part of the ‘Russian World’ (Russkii Mir) compounds these internal divisions. Since the 2000s, this concept, endorsed by the Russian state, has sought to unite all ethnic Russians and Russian-speakers globally around shared culture, history, and faith (Orzechowski, 2024, p.22-23). This worldview underpins policies such as passportisation, through which Russia confers citizenship upon ethnic Russians abroad to justify political or military interventions. As the Royal United Services Institute (Melvin, 2020, Online) explains, passportisation functions as a hybrid tool blending soft power with coercion. By granting passports in places like Abkhazia, South Ossetia, and Transnistria, Russia constructs legal grounds for ‘protecting’ its compatriots (Toal & O’Loughlin, 2013, p.240-241). The 2014 annexation of Crimea and subsequent expansion of Russian nationality into Donetsk and Luhansk represent clear extensions of this strategy.

These hybrid tactics erode host states’ sovereignty and are conducted alongside media influence, economic coercion, and proxy operations. Russian-language media remains central in shaping diaspora perceptions of politics and history. In Estonia, 92% of Russian-speakers report daily consumption of Russian television channels (Coolican, 2021, p.14). Such outlets often frame the Soviet Union as a liberator from Nazism, in contrast to the Estonian national narrative of Soviet occupation (Polynin 2023, p.5). These conflicting historical memories foster divergent senses of belonging and political orientation.

During World War II, the Baltic states experienced two occupations. First by the Soviet Union (1940–1941), then by Nazi Germany (1941–1944), and again by the Soviets until 1991. The Baltic narrative views these occupations as illegal and oppressive, marked by deportations and cultural suppression. In contrast, the Soviet perspective framed the annexation as voluntary and the post-war period as liberation from fascism. In Estonia, the dual occupation narrative strengthens national identity and pride, emphasising resistance to foreign rule. Conversely, it can alienate Russian-speaking minorities who may view the Soviet era more positively. These divisions are deepened by the differing media outlets consumed by ethnic Estonians and Russian-speakers. These conflicting perceptions continue to shape historical interpretation and fuel diplomatic tensions with Russia.

Estonian security authorities consistently identify Russia as the principal external threat. The Estonian Internal Security Service (KAPO) reports repeated cases of espionage, sabotage, and information operations targeting Russian-speaking communities (kapo.ee, 2025). Given repeated incidents and credible reporting from security services, it is reasonable to treat the threat as plausible rather than purely hypothetical. Viewing Estonian measures to integrate the Russian minority should not be viewed in isolation. Given this persistent threat environment, Estonia's restrictive integration policies can be interpreted as proportionate security measures rather than purely illiberal acts. Whilst restricting certain elements of civil society based on language or origin can appear illiberal to external bodies, such as the United Nations (OHCHR, 2023), the infringement of its human-rights obligations was seen as a necessary measure given both the historical and contemporary international context, with the Estonian government arguing they are essential for national cohesion and resilience. Through this lens, the risk to Estonia's international reputation was viewed as morally justifiable. As Kallas (2016, p.11) argued, automatic inclusion of Russian-speakers could weaken statehood and democratic integrity by diluting loyalty. Seen through a realist lens / security-oriented perspective, these restrictive measures served as pre-emptive resilience tools rather than purely discriminatory and were not designed to exclude but to prevent exploitation of internal divides by hostile powers.

However, one must caution against over-simplification. Estonia's efforts to balance liberal freedoms with state security generated an inadvertent paradox. Kadri Liik argues that a direct link exists between domestic inequalities and grievances among Russian-speakers, which provided fertile ground for protest that Moscow could amplify (Liik, 2007, p.73). Hard-line, often illiberal, policies aimed at Estonian nation-building and forced assimilation were seen through a prism of securitirisation. And yet it is feasible to suggest that their effect was contradictory and perhaps aided the narrative promulgated from Moscow.

In the years after the Bronze Night, Estonian policymakers have sought to manage historical memory more carefully with an emphasis on civic patriotism over ethnic nationalism, framing integration as a collective security imperative rather than an assimilationist project. Over time, Estonia has implemented targeted reforms to reduce statelessness. The government now grants automatic citizenship to children born in

Estonia to parents of undetermined nationality if they have resided in the country for at least five years and are not citizens elsewhere (OHCHR, 2023).

A calibrated approach that couples short-term security vigilance with long-term inclusion offers the most sustainable path. Whilst research indicates that Russian-language media reinforces Moscow's geopolitical narratives, the picture is not uniform. Many Russian-speakers in Estonia consume a mix of Russian and Western media, and local Russian-language outlets have countered disinformation with credible reporting (Coolican, 2021, p.14–15). Reactions to Russia's 2022 invasion of Ukraine reveal this complexity. While some expressed solidarity with Russians in Ukraine, many publicly opposed the war and affirmed loyalty to Estonia (Fukuhara, 2023, p.79-80).

This reassertion of control over the media narrative is a defensive tool that counters disinformation and is an absolute necessity in the near term. But genuine enduring security will depend on policymakers' ability to widen access to Estonian-language education, promote independent local media in Russian, and address socio-economic inequities to prevent alienation. This approach gained urgency after 2014 and the Russian annexation of Crimea and was reinforced by the 2022 full-scale invasion of Ukraine, which confirmed the risks of identity-based manipulation. In December 2022, amendments to the Basic Schools and Upper Secondary Schools Act mandated a phased transition to Estonian-language instruction for most subjects by 2030–33 (Riigikogu p.9, Para 21).

This shift represents a generational watershed. While older cohorts remain more sceptical as persistent disparities remain, younger Russian-speakers, already more fluent in Estonian, largely support these measures with surveys showing a steady rise in language proficiency and civic identification among the youth (Harrik, 2025, Online). These incremental measures demonstrate an evolving balance between national cohesion and human rights obligations. Integration policies now emphasise language training, civic education, and community initiatives to foster contact between Estonian and Russian speakers (Kunitsõn & Kalev, 2021, p.2).

Recent sociological studies support this growing heterogeneity among Russian-speaking Estonians. A 2023 study by Andu Rämmer et al. in Narva found that young people with higher Estonian proficiency were more engaged with Estonian society and media. The 'Feeling Cornered' survey (Krum et al., 2023, p.7-10) similarly showed increasing disillusionment with Russian propaganda and growing alignment with Estonian civic values. Earlier research by Gerli Nimmerfeldt (2012) demonstrated that many second-generation Russian-speakers possess dual or layered identities, identifying both ethnically with Russia and civically with Estonia.

These findings highlight a pragmatic shift: younger Russian-speakers emphasise education, employment, and social participation over ethnocultural boundaries. They consume more Estonian media, use multiple languages daily, and express hybrid or civic identities. This enhanced assimilation model combines language acquisition with civic inclusion and suggests that integration, while incomplete, is deepening organically through generational change.

In conclusion, Estonia's post-1991 trajectory reveals the difficult balance between liberalism and security. The state's restorationist citizenship policy and language laws reflected an existential need to safeguard sovereignty but also produced exclusionary effects. EU and NATO accession compelled liberalisation, yet reforms remained filtered through a security lens. Over time, successive governments have attempted to calibrate their integration policies between the twin imperatives of nation-building and social inclusion. On one hand, the pursuit of a culturally homogeneous Estonian identity has driven policies promoting the Estonian language and civic loyalty. On the other hand, there has been a cautious effort to avoid alienating Russian-speaking communities to the point of unrest or political radicalisation.

The 2007 Bronze Night remains a vivid reminder of the fragility of Estonia's identity politics. For the Estonian state, it represented de-Sovietisation and national sovereignty. And yet, it serves as a powerful example of how both historical grievance and accumulated social frustration among Estonia's Russian-speaking minority can manifest. Whilst for many Russian speakers the decision symbolised an official denial of their historical narrative and collective memory, beneath the symbolic tensions lay deeper structural grievances rooted in persistent socio-economic marginalisation.

Whilst the unrest was in part a reaction to the perceived historical erasure of the Russian diaspora, the exclusionary policies and perceived marginalisation imposed on Russian-speakers created the environment where this anger was able to manifest.

Russia's ongoing interference, from soft-power cultural diplomacy to hybrid warfare, continues to shape Estonia's calculus. Since 2022, reforms have accelerated, reflecting both external threat perception and internal generational change. Younger Russian-speakers' increasing integration has made more assertive policies politically feasible, while also softening the long-term need for securitisation. The evidence suggests that Estonia's identity politics are gradually stabilising with linguistic convergence, civic inclusion, and shared democratic values replacing older binaries of occupation and exclusion.

Ultimately, Estonia's success depends on transforming security-driven integration into civic inclusion. Liberal ideals and national security need not be contradictory as they were in the 1990s through the 2000s. When combined through inclusive education, equitable citizenship, and cultural recognition, they reinforce one another and remove a weapon from Russia's hybrid warfare playbook. Estonia's generational transition shows that resilience arises not from rigid boundaries but from a shared sense of belonging, one capable of withstanding external pressure while deepening democratic cohesion at home.

Bibliography

Books

Galbreath, D. J. 2005. *Nation-Building and Minority Politics in Post-Socialist States.* London: I.B. Tauris, 2005.

Hirsch, F. 2005. *Empire of Nations: Ethnographic Knowledge and the Making of the Soviet Union.* Ithaca: Cornell University Press, 2005.

Martínez, F. 2018. *Remains of the Soviet Past in Estonia.* Tallinn: University of Tartu Press, 2018.

Journal Articles

Astapova, A. 2021. An Estonian–Russian Language Club as a Venue for Grassroots Ethnic Integration. *Nationalities Papers*, vol. 50, no. 3, pp. 498–514. DOI: 10.1017/nps.2020.75.

Brüggemann, K., and Kasekamp, A. 2008. The Politics of History and the 'War of Monuments' in Estonia. *Nationalities Papers*, vol. 36, no. 3, pp. 425–448. DOI: 10.1080/00905990802080646.

Cheskin, A. 2015. Identity and Integration of Russian Speakers in the Baltic States: A Framework for Analysis. *Ethnopolitics*, vol. 14, no. 1, pp. 72–93. DOI: 10.1080/17449057.2014.933051.

Davydova, O. 2008. Bronze Soldier Goes Transnational: Mediascapes and the Formation of Identities in Internet Discussions. *Ethnopolitics*, vol. 7, no. 4, 2008, pp. 391–411. DOI: 10.1080/17449050802243459.

Ehala, M. 2009. The Bronze Soldier: Identity Threat and Maintenance in Estonia. *Journal of Baltic Studies*, vol. 40, 2009, pp. 139–158. DOI: 10.1080/01629770902722294.

Fedorenko, K., and Umland, A. 2021. A Triadic Nexus Conflict? Ukraine's Nationalizing Policies, Russia's Homeland Nationalism, and the Dynamics of Escalation in 2014–2019. In: **Aasland, A. & Kropp, S. (eds.)** *The Accommodation of Regional and Ethno-cultural Diversity in Ukraine.* Cham: Palgrave Macmillan, 2021, pp. 55–80. DOI: 10.1007/978-3-030-80971-3_3.

Fukuhara, Y. 2023. 'We Belong to Estonia': Influence of Russia's Invasion of Ukraine on Russian Speakers in Estonia. *European Studies*, vol. 22, 2023, pp. 75–87.

Kallas, K. 2016. Claiming the Diaspora: Russia's Compatriot Policy and Its Reception by Estonian-Russian Population. *Journal on Ethnopolitics and Minority Issues in Europe*, [online] 15(3), pp.1–25, 2016. Available at: https://www.ecmi.de/fileadmin/downloads/publications/JEMIE/2016/Kallas.pdf [Accessed 22 Oct. 2025].

Kunitsõn, N., and Kalev, L. 2021. Citizenship Educational Policy: A Case of Russophone Minority in Estonia. *Social Sciences*, vol. 10, no. 4.

Nimmerfeldt, G. 2012. *Ethnic and Civic Identities of Russian Youth in Estonia.* Tallinn University.

Norberg, D., and Norberg, K. P. 2024. Estonia's 'Return to Europe': The Relationship Between Neoliberalism, Statelessness, and Westward Integration in Post-

Independence Estonia. *Political Geography*, vol. 108, p. 103009. DOI: 10.1016/j.polgeo.2023.103009. Available here: https://www.sciencedirect.com/science/article/pii/S0962629823001877.

Orzechowski, M. 2024. Russkiy Mir (Russian World): An Exemplification of All-Russian Nationalism. *Polish Political Science Yearbook*, vol. 53, no. 3, 2024.

Polynin, I. 2023. Patching Identity: How Russian-Language Media in Estonia Reconstitutes Our Understanding of Citizenship. *Frontiers in Political Science*, vol. 5 (2023). DOI: 10.3389/fpos.2023.1140084.

Rämmer, A., Kivimäe, A., Kötsi, K. & Žuravljova, M. 2023. Youth-Centred Research-Based Model—An Innovative Tool in Youth Work. *Journal of Youth Studies*, vol. 3, no. 3, 2023, pp. 1004–1012.

Saarts, T. 2008. The Bronze Nights: The Failure of Forced Europeanization and the Birth of Nationalist Defensive Democracy in Estonia. *Eurozine*, 10 Oct 2008. Available at: https://www.eurozine.com/the-bronze-nights/.

Schulze, J. L., and Pupcenoks, J. 2025. Securitizing Russian-Speakers in Estonia and Latvia: The Frame-Policy Nexus Before and After Russia's Invasion of Ukraine. *Nationalities Papers*, vol. 53, no. 5, pp. 1035–1059. DOI: 10.1017/nps.2024.97.

Toal, G., and O'Loughlin, J. 2013. Inside South Ossetia: A Survey of Attitudes in a De Facto State. *Post-Soviet Affairs*, vol. 29, no. 3, 2013, pp. 228–261. DOI: 10.2747/1060-586X.29.3.228.

Policy Reports & Institutional Publications

Aliens Act of the Republic of Estonia (1993, as amended 2001). *Legislationline*. [online] Available at: https://legislationline.org/taxonomy/term/13347 [Accessed 26 Oct. 2025].

Council of Europe. 2022. *Fifth Opinion on Estonia: Advisory Committee on the Framework Convention for the Protection of National Minorities.* Strasbourg: Council of Europe, 2022. Available at: https://rm.coe.int/5th-op-estonia-en/1680a6cc9e [Accessed 29 Sep. 2025]

Human Rights Watch. 1993. *World Report 1993 – Estonia, Latvia and Lithuania.* New York: Human Rights Watch, 1993. Available at: https://www.refworld.org/reference/annualreport/hrw/1993/en/23487 [Accessed 05 Oct. 2025]

International Centre for Defence and Security (Juurvee & Mattiisen). 2020. *The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Threats.* Tallinn:

ICDS, 2020. Available Here: https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdfhttps://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf [Accessed 26 Sep. 2025].

Liik, K. 2007. The 'Bronze Year' of Estonia-Russia Relations. *Estonian Ministry of Foreign Affairs Yearbook 2007.*Tallinn: ICDS, 2007. Available at: https://icds.ee/wp-content/uploads/2010/03/Kadri_Liik_Bronze_Year.pdf?utm

KAPO (Estonian Internal Security Service). 2025. *Annual Review 2024–2025.* Tallinn: KAPO, 2025. Available at: https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2024-2025.pdf [Accessed 10 Oct. 2025]

Kondan, S., Sahajpal, M. & Trimbach, D. 2021. Identifying the Needs of Estonia's Russian-speaking Minority: COVID-19, Data Disaggregation, and Social Determinants of Health. *Foreign Policy Research Institute Report*, 11 May 2021. Available here: https://www.fpri.org/article/2021/05/identifying-the-needs-of-estonias-russian-speaking-minority-covid-19-data-disaggregation-and-social-determinants-of-health/ [Accessed 16 Oct. 2025]

Musset, P., Field, S., Mann, A. & Bergseng, B. 2019. *OECD Reviews of Vocational Education and Training: Vocational Education and Training in Estonia.* Paris: OECD Publishing.

Office of the United Nations High Commissioner for Human Rights (OHCHR). 2023. *Estonia: New law banning mother-tongue education for minorities may violate human rights, warn UN experts*. [online] 17 Aug. 2023. Available at: https://www.ohchr.org/en/press-releases/2023/08/estonia-new-law-banning-mother-tongue-education-minorities-may-violate-human [Accessed 22 Oct. 2025]

Krumm, Reinhard, Stamberg, Tõnis & Strapatšuk, Irina. 2023. *Peace and Security Feeling Cornered: An Analysis of the Russian-Speaking Minority in Estonia.* Tallinn: Friedrich Ebert Stiftung, 2023.

Riigikogu. 2024. *Basic Schools and Upper Secondary Schools Act.* Tallinn: Government of Estonia, 2024.

Media and Online Sources

Coolican, S. 2021.*The Russian Diaspora in the Baltic States: The Trojan Horse That Never Was.* LSE IDEAS Strategic Update, Dec 2021.

ERR News / Harrik, Airika. 2025. Study: Russian-speaking Youth in Estonia Reflect Diverse Values and Identities. *ERR News*, 17 Apr 2025.

Melvin, N. 2020. *Russia's Policy of Passport Proliferation*. Royal United Services Institute. [online] 1 May 2020. Available at: https://www.rusi.org/explore-our-research/publications/commentary/russias-policy-passport-proliferation [Accessed 26 Oct. 2025].

CWO Julien BOISVERT: From the South China Sea to the High North: China's Adaptive Playbook

Supervisor: CSM Paul MULHERN

Statement on the Use of AI Tools:

AI has been used to conduct research, support bibliographies, refine sentence structure, and correct grammar and syntax.

Introduction

The Arctic is a strategically significant region, vital for natural resources and climate regulation, playing a critical role in the planet's environmental and geopolitical future (Nesheiwat, 2021). Recognising this, China perceives the Arctic as both an opportunity and a testing ground for its advancing great-power ambitions. This perspective has prompted Beijing to adapt specific strategies from its South China Sea (SCS) playbook for application in the Arctic, also known as the High North.

In this essay, the author will argue that China's Arctic approach is best understood as an adaptation of its SCS playbook, rather than a replication per se of its behaviours in the SCS. To contextualise his work, the author will begin by providing a quick summary of China's SCS playbook. Once the SCS playbook is explained, the author will propose five main arguments to support his thesis.

First, the author will illustrate how China pushes the boundaries of judicial and procedural legitimacy by strategically deploying international law. Second, the author will demonstrate how Beijing continues to utilise coercive-diplomatic strategies, albeit in a more measured fashion, through its narrative surrounding the Polar Silk Road (PSR). Third, the author will show how financial control and infrastructure development are incorporating the Arctic region into wider Chinese policies and logistics ambitions, in line with China's future needs. Fourth, the author will demonstrate how environmental interdependence and the associated scientific capabilities provide both justification and capacity for China's sustained Arctic involvement.

Finally, the author will demonstrate how China employs technology as an instrument of influence to shape norms and standards that embed its presence in regional governance. The author will then introduce a few counterarguments, outline implications for NATO and regional actors, and conclude with a short conclusion.

China's South China Sea playbook

Fravel (2011) describes China's SCS strategy as one of delay and consolidation, intending to postpone resolution while building facts that deepen control. To do so, China's South China Sea (SCS) playbook consists of a set of policies and plans. This hybrid strategy combines military, diplomatic, economic, and legal instruments to consolidate national influence over a highly contested maritime domain. The crux of this tactic is Beijing's affirmation of sovereignty over the Nine-Dash Line, which claims China's maritime territories overlapping with those of various Southeast Asian states, including Vietnam, the Philippines, and Malaysia (Djelantik, 2021).

China's recent military modernisation plays a distinct role in this strategy. With a steady increase in defence expenditure, China has enhanced its maritime capabilities and reinforced its ability to project power across the SCS (Perwita, 2018). Military activities are then combined with soft power diplomacy and economic partnerships, in which development and support are aimed at cultivating regional interdependence and demonstrating goodwill (Djuyandi et al., 2025; Pitra, 2019).

In the SCS strategy, China's energy diplomacy is also intricately linked to its military efforts and aims to secure offshore resources and sustain long-term economic growth (Badaruddin and Zulham, 2020). To achieve this, China has developed dual-use technological innovation, specifically in offshore extraction, through joint programs with other states, thereby promoting bilateral resource-sharing arrangements that also reinforce territorial control and mitigate international obstruction (Tian et al., 2022; Pitra, 2019).

To summarise, China's SCS strategy has evolved from maintaining regional stability to actively asserting sovereignty claims, with China often escalating over incidents at sea prompted by perceived challenges from the United States and other regional actors (Zhou, 2024).

China: a maritime power with Arctic legitimacy

The analogy between the SCS and Arctic playbook is not perfect: the SCS is a partly enclosed sea marked by overlapping sovereignty claims, with a dense history of incidents and extensive island-building aimed at expanding China's territorial boundaries. In contrast, the High North, or Arctic, is a global maritime and land (and ice) region governed by the intricacies of international law, regional institutions, and growing great-power scrutiny. However, patterns familiar from the SCS do appear in China's Arctic posture: a sustained legal-normative narrative under the United Nations Convention on the Law of the Sea (UNCLOS), infrastructure and scientific investments and partnerships that double as governance tools and strategic signalling that communicates resolve while preserving diplomatic manoeuvrability (Cassota et al., 2015).

China's broader historical maritime posture alternates between triumphalism and accommodation, a pendulum that can swing quickly in response to geopolitical context (Sen, 2018). Under Chinese President Xi Jinping, military and economic strategies are synchronised across maritime theatres. However, the Arctic's institutional density, the salience of U.S.–NATO relations, and Russia's importance as a partner incentivise China's caution (Lokman, 2022).

To do so, China's Arctic strategy is adjusted to a quite different strategic environment, where China's balance remains tilted more towards accommodating. While the underlying mechanics of strategic signalling persist, public references to navigational freedoms, the emphasis on scientific legitimacy, and visible yet non-provocative deployments such as northern expeditions, icebreaker operations, and data collaborations aim to normalise China's presence and deter exclusion from the region. In contrast to the SCS, China pursues a calibrated mix of presence and partnership in the Arctic, rather than overt power projection, while investing in scientific, commercial, and technological capabilities. However, these investments could be quickly redirected to military use if the geopolitical context intensifies.

Seeking judicial recognition

A recurring feature of China's maritime strategy is the search for judicial and procedural legitimacy while pushing the boundaries of legal interpretation. In their research, Cassotta et al. (2015) conceptualised China as an 'emerging regulatory sea power' whose engagement tests the jurisdictional edges of existing frameworks, as climate change reshapes opportunities in the Arctic Ocean. The argument is not that Beijing completely rejects international law, but that it works through it by foregrounding UNCLOS freedoms of navigation, scientific research, and high-seas rights, while concurrently advocating for legal interpretations amenable to its long-term access and accrued influence.

In January 2018, China issued its first Arctic white paper: China's Arctic Policy, positioning itself as a near-Arctic State and emphasising its role as an essential stakeholder in Arctic affairs (State Council of China, 2018). This self-designation based on geographical proximity to the Arctic Circle was strongly criticised by the United States, which argued that 'there are only Arctic and non-Arctic states', with 'no third category' (Pompeo, 2019). China has defended its terminology by noting that other non-Arctic countries, such as the United Kingdom, have used similar language and referred to themselves as the Arctic's nearest neighbour in their own Arctic policy paper (UK Government, 2018).

China's dispute management reveals a stable pattern in which law functions as a political instrument and ambiguity to turn legal claims into negotiating power (Gupta 2005). In the SCS, this manifested in arguments about historical rights and selective readings of UNCLOS; in the Arctic, the emphasis shifts toward universalist principles such as stewardship, commons governance, impact of climate change supported by science, and maritime safety standards that legitimise its participation without overt challenges to other nations (Cassotta et al., 2015).

The use of Soft Power

China's White Papers described above also emphasise its scientific rights in the region. It states that while non-Arctic states may lack sovereignty, they retain rights to

scientific research, navigation, overflight, fishing, and resource exploration in international Arctic waters (State Council of China, 2018). It also underscores China's intention to contribute to Arctic governance through established rules and mechanisms (Swanström and Månsson, 2025).

As an example, China's Arctic Council observer status serves as a pathway to voice its preferences without openly challenging the primacy of Arctic states (Gayazova, 2013). Indeed, observer status enables China's active participation in information-sharing and working-group activities, thereby allowing It to normalise its increased presence as a provider of scientific and public information and as a key stakeholder in global maritime governance. This participation offers key advantages by allowing China to present its contributions as benefiting collective goods, demonstrating Its Status as a trusted partner, and deepening its operations within that legal grey zone—a textbook SCS play.

Enhancing economic governance: replicating the SCS playbook with a different tone.

As we have seen above in its SCS playbook, China's use of signalling its narrative by combining diplomatic, economic, and operational indicators has been extensively documented. This often encompasses military patrol activities, movements of considerable resources between hubs, and island-building. Tensions or crisis bargaining involves calibrated escalation and rhetorical ambiguity intended to deter rivals and consistently test the thresholds (Fravel 2011; Ramadhani 2014). In the Arctic, China's signalling technique must operate differently, where enhancing its economic governance, deploying finance, increasing trade, and infrastructure to shape strategic space, sits at the centre of China's Arctic adaptation, aiming to position itself as an indispensable connectivity and economic partner.

Biedermann (2021) and Zhang, Ding and Ding (2024) present the Polar Silk Road (PSR) as establishing a narrative that links China's Belt and Road Initiative (BRI) to the High North Sea lanes, thus showcasing Beijing's long-term intent to embed the Arctic into its International trade, specifically with its European partners. The PSR also frames the Northern Sea Route (NSR) and connections as competitive alternatives to the Suez Canal, potentially shortening Asia–Europe transit and diversifying between

chokepoint risk (Biedermann 2021). Chinese state-linked firms are experimenting with seasonal voyages, while energy moguls are co-developing Arctic resource projects in Russia, providing Beijing with both learning opportunities and stakes in route reliability.

Du (2021) introduces an additional regional layer of cooperation with Japan and South Korea in Arctic science and technology, which can expand capacity and reduce political friction. That trilateral emphasis on research or exploration sailings, observation networks, and maritime technology mirrors the joint development rhetoric once prevalent in the SCS. Collaborative bilateral partnerships with Iceland, Norway, or Sweden on Arctic energy and health systems offer additional models of joint Arctic research initiatives that support China's Arctic expertise development (Tulopov, 2013).

A friend is one who has the same enemies as you have (Abraham Lincoln)

Another significant aspect of China's Arctic strategy is its close relationship with Russia. While both countries have forged a strategic, albeit cautious, partnership in the Arctic, it is still mainly grounded in shared economic interests and geopolitical necessity for now. China has invested heavily in Russian energy projects such as Yamal LNG and Arctic LNG-2 to secure long-term access to Arctic hydrocarbons, while also helping Russia offset Western Sanctions (Thingstad et al., 2023). Sino-Russian cooperation also extends to the NSR and China's PSR, with China financially supporting infrastructure development in the High North and Russia exercising control over access and navigation (Kobzeva, 2021). Both countries also engage in scientific collaboration and joint coast guard operations, introducing an area of increased military cooperation (Strelnikov and Kharina, 2024).

Technological innovation as the backbone of China's Arctic access

For China, technology is both an enabler and an argument for its Arctic presence. Zhan et al. (2020) highlight China's innovations in ship design, ice navigation, and environmental safeguards as a key pathway to sustainable Arctic shipping. For China, these developments are part of a broader, comprehensive national security framework that integrates civil and military innovation (Puranen et al., 2023). Dual-use technologies, including satellite communications, remote sensing and newly acquired

autonomous platforms capable of under-ice operations, support China's scientific missions and maritime presence while also enhancing situational awareness that could pivot into strategic or military utility if needed.

Technical competence, coupled with modern practices, also bolsters safety, lowers insurance and operational risk, and reduces costs for shippers and investors. This, again, aligns China's activities with international good practice and presents appealing economic opportunities. As in the SCS, where dredging, construction, and surveillance systems amplified presence, technology in the Arctic amplifies legitimacy: those who can operate safely and transparently in extreme conditions gain influence over how operations are governed.

Indeed, for China, operating infrastructure such as ports, logistics hubs, digital platforms, and ice-navigation systems does more than move goods; it also embeds standards, practices, and data flows that can become de facto rules (Fravel, 2011). While development logics often advanced geographic depth in the SCS, in the Arctic, infrastructure-led initiatives bolster influence without true militarisation, anchoring China further in the region's political economy, thus making its interests harder to exclude. Where SCS signalling aimed to consolidate claims and deter rivals from resource activities, Arctic signalling seeks to secure a recognised place in governance, enhanced logistics, and standard-setting without triggering or threatening the regional balance, thereby enhancing China's ability to shape regional practices in subtle ways that endure (Kuus, 2020).

Counterarguments

As mentioned earlier, the analogy between China's SCS and Arctic strategies is not perfect, and several counterarguments could explain why the adaptive playbook comparison may tend to overstate China's coercive intent in the region.

First, the Arctic's institutions and legal framework, anchored in UNCLOS and the Arctic Council, create a far stronger rules-based environment than in the SCS region, thus limiting any unilateral actions (Koivurova, 2010). Unlike the fragmented sovereignty disputes in the SCS, Arctic institutions impose legitimacy costs that restrain behaviour

(Jakobson, 2019). The U.S., Canada, Nordic, and NATO attentiveness to dual-use infrastructure results in greater scrutiny than in the SCS.

Second, China's Arctic posture could be guided by environmental or climate change impacts rather than geopolitics, in which its emphasis on scientific research and climate observation is not a coercive practice but rather a form of national resilience planning (Yang et al., 2022). In fact, China's participation in the Arctic Council as an observer may reflect a desire for enhanced cooperation rather than manipulation, and China's main objective could indeed be to contribute to public goods, thereby legitimising its presence through transparency rather than dominance (Zhang et al., 2020).

Finally, despite the Sino-Russian alliance, Russia's strategic role in the Arctic limits Beijing's freedom of action, as China's dependence on Russian infrastructure and joint ventures restricts its operational reach. While cooperation with Russia facilitates access, Moscow's control over the NSR and the politicisation of Arctic energy projects keep China dependent on Russia rather than being a true dominant player yet (Biedermann, 2021). One can also argue that China's polar expeditions are mainly symbolic, lack a sustained strategic campaign, and demonstrate no significant Arctic capability.

Collectively, these arguments may suggest that China's Arctic posturing reflects a pragmatic adaptation to geographical constraints rather than the beginning of assertive maritime tactics, thereby distinguishing it sharply from the coercive dynamics of the SCS.

Implications for Arctic and allied actors

China's SCS playbook has proven to be adaptable. To avoid similar tensions in the Arctic, NATO and regional Allies must maintain awareness of legal issues and scientific developments, treating them as strategic terrain. Since China's strategy proceeds through legal-scientific legitimacy, investing in open, high-integrity science frameworks, transparent data standards, and clear interpretations of navigational rights will help shape the rules of practice that govern future traffic. Continued engagement

with China in these areas can both harness its capabilities and discipline behaviour within multilateral norms, including with Russia (Gayazova 2013; Cassotta et al., 2015).

NATO and its Allies should also assess how infrastructure projects might create unintended governance or security consequences: logistics hubs, cables, data networks, digital systems, transport routes and ice-navigation services can create dependencies, potentially giving China (and Russia) excessive influence or control over regional decision-making and operations. NATO and its Allies should develop resilience mechanisms that distinguish beneficial interdependency from coercive control, including interoperability standards, diversified routing, and transparent public-private governance (Kuus 2020; Biedermann 2021).

The impact of climate change can create shared incentives for collective observation and forecasting. Joint projects that prioritise safety at sea and environmental protection can channel strategic competition into constructive outcomes while preserving oversight of dual-use capabilities (Yang et al., 2022). By collaborating on issues such as these, NATO and Arctic nations can foster trust and reduce regional tensions, potentially also isolating Russia.

Conclusion

The Arctic is strategically vital but still poorly understood. It is a region still marked by governance gaps and mounting geopolitical complexity. China's Arctic strategy, or playbook, exhibits an unmistakable resemblance to its SCS behaviour, but noting the differences and its evolution is helpful. In the High North, Beijing advances its maritime interests by focusing on law, science, and infrastructure, rather than engaging in sovereignty contests. The result is an adaptive approach that seeks to shape regional order from within: making its activities and narratives compatible with UNCLOS, embedding itself in the political and economic order of Arctic logistics and energy pathways, and positioning scientific contributions as public goods that justify its presence.

While the variables are less about the movement of grey hulls for now and more about the movement of data, standards, capital, and routings, China's Strategy is not frozen in time, and the SCS playbook has demonstrated China's agility and adaptation. The strategic challenge is to manage China's integration into Arctic governance in ways that capture authentic public goods — safety, environmental stewardship, and scientific knowledge — without creating asymmetric dependencies or eroding transparency. Clarity on legal interpretations, vigilance over dual-use infrastructures, and investment in shared scientific capacity offer a clear and balanced path.

The Arctic is where China refines a method of influence appropriate to a densely institutionalised and environmentally fragile space. It is a method that elevates the politics of legitimacy, the power of connectivity, and the quiet of the Soft Powers. Appreciating that method while also monitoring its continuities and similarities with the SCS may be essential for anticipating how China may seek to shape the world's newest roads and the norms that will govern them.'

Bibliography

Nesheiwat, Julia. 2021. Why the Arctic Matters. *Atlantic Council – Energy Source*, 17 Jun. 2021. Available at: https://www.atlanticcouncil.org/blogs/energysource/why-the-arctic-matters/.

Fravel, M. Taylor. 2011. China's Strategy in the South China Sea. *Contemporary Southeast Asia*, vol. 33, no. 3, 2011, pp. 292–319. DOI: 10.1355/cs33-3b. Available at: https://taylorfravel.com/documents/research/fravel.2011.CSA.china.strategy.scs.pdf.

Djelantik, Sukawarsini. 2021. Kekuatan Nasional Tiongkok dalam Sengketa Laut Tiongkok Selatan. *Indonesian Journal of International Relations*, vol. 5, no. 2, 2021, pp. 292–319. DOI: 10.32787/ijir.v5i2.248.

Perwita, Anak Agung Banyu & Ersandi, Ivena. 2018. The Implementation of Japan-Philippines Maritime Diplomacy as a Proactive Approach to Respond to the Assertive China in the South China Sea *(2012-2017)*. Vol. 1, No. 2, July-December 2018. DOI: 10.33822/mjihi.v1i2.428.

Djuyandi, Yusa, Azmi, M., and Dermawan, W. 2025. Analysis of China's Aggressive Behaviour in the South China Sea During the COVID-19 Pandemic (2020–2021).

Journal of Public Policy, vol. 11, no. 3, 2025, pp. 353–366. DOI: 10.35308/jpp.v11i3.12245.

Pitra, Hendra. 2019. China's Coercive Diplomacy through South China Sea Conflict and Belt & Road Initiatives. *Jurnal Pertahanan – Media Informasi TTG Kajian & Strategi Pertahanan yang Mengedepankan Identity Nasionalism & Integrity*, vol. 5, no. 2, 2019, pp. 48–62. DOI: 10.33172/jp.v5i2.522.

Badaruddin, M. and Zulham, C. 2020. China's Petropolitics: Its Business and Diplomacy in the South China Sea. *Journal of International Studies on Energy Affairs*, vol. 1, no. 2, 2020, pp. 159–193. DOI: 10.51413/jisea.vol1.iss2.2020.

Tian, Cheng, Yang, J., Lin, Z., Li, X., Cheng, Z., and Liu, C. 2023. Development of Resource-Exploitation Equipment for the South China Sea. *Strategic Study of CAE*, vol. 25, no. 3, 2023, pp. 84–96. DOI: 10.15302/j-sscae-2023.03.008.

Zhou, Xia. 2024. China's Position on the South China Sea Issue: From Maintaining Stability to Protecting Rights. *Международные Отношения (International Relations)*, no. 1, 2024, pp. 101–112. DOI: 10.7256/2454-0641.2024.1.70153.

Cassotta, Sandra, Hossain, Kamal, Ren, J., and Goodsite, M. E. 2015. Climate Change and China as a Global Emerging Regulatory Sea Power in the Arctic Ocean: Is China a Threat for Arctic Ocean Security? *Beijing Law Review*, vol. 6, no. 3, 2015, pp. 199–207. DOI: 10.4236/blr . 2015.63020.

Sen, Ranjit. 2018. China's South China Sea Strategy: Balancing Triumphalism and Accommodation. *International Journal of East Asian Studies*, vol. 7, no. 1, 2018, pp. 27–47. DOI: 10.22452/ijeas.vol7no1.2.

Lokman, Kamarulnizam. 2022. The PRC's Military Strategies on the Security Architecture of East and South China Sea under President Xi Jinping. *Intellectual Discourse*, vol. 30, no. 2, 2022. DOI: 10.31436/id.v30i2.1895.

State Council of the People's Republic of China. 2018. *China's Arctic Policy (White Paper).* Beijing: State Council Information Office, 26 Jan. 2018. Available at: https://english.www.gov.cn/archive/white_paper/2018/01/26/content_281476026660336.htm.

Pompeo, Michael. 2019. *Remarks at the Arctic Council Ministerial.* U.S. Department of State, 6 May 2019. Available at: https://archive.org/details/CSPAN_20190506_223400_Secretary_of_State_Pompeo_Remarks_on_U.S.-Arctic_Policy/start/180/end/240.

UK Government. 2018. *Beyond the Ice: The UK's Arctic Policy Framework.* London: HM Government, 2018. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/697251/beyond-the-ice-uk-policy-towards-the-arctic.

Gupta, Sourabh. 2005. Chinese Strategies for Resolution of the Taiwan and South China Sea Disputes. *International Studies*, vol. 42, nos. 3-4, 2005, pp. 247–264. DOI: 10.1177/002088170504200304.

Swanström, N. & Borges Månsson, F. 2025. The New Frontier: Sino-Russian Cooperation in the Arctic and Its Geopolitical Implications. Special Paper, September 2025. Stockholm: Institute for Security and Development Policy. ISBN 978-91-88551-71-9.

Gayazova, Oksana. 2013. China's Rights in the Marine Arctic. *The International Journal of Marine and Coastal Law*, vol. 28, no. 1, 2013, pp. 61–95. DOI: 10.1163/15718085-12341264.

Ramadhani, Eka. 2014. China's Crisis Bargaining in the South China Sea Dispute (2010–2013). *JAS (Journal of ASEAN Studies)*, vol. 2, no. 2, 2014, pp. 103–121. DOI: 10.21512/jas.v2i2.302.

Biedermann, Raphäel. 2021. China's Impact on the European Union's Arctic Policy: Critical Junctures, Crossovers, and Geographic Shifts. *Asia Europe Journal*, vol. 19, no. 4, 2021, pp. 467–487. DOI: 10.1007/s10308-021-00605-7.

Zhang, Ming, Ding, T., and Ding, C. 2024. Research on the Competitiveness of the Arctic Transportation Route under the Belt and Road Initiative. *Transportation Journal*, vol. 64, no. 1, 2024. DOI: 10.1002/tjo3.12019.

Du, Ying. 2021. Development of Arctic Sea Route and Cooperation between China, Japan and South Korea in the Digital Era. In: *Advances in Economics, Business and Management Research*, 2021. DOI: 10.2991/aebmr.k.210213.005.

Tulupov, D. 2013. Scandinavian Vector of China's Arctic Policies. *Mirovaya ekonomika i mezhdunarodnyye otnosheniya (World Economy and International Relations)*, no. 9, 2013, pp. 61–68. DOI: 10.20542/0131-2227-2013-9-61-68.

Tingstad, Abbie; Pezard, Stephanie; Shokh, Yuliya. 2024. *China-Russia Relations in the Arctic: What Are the Northern Limits of Their Partnership?* Santa Monica (CA): RAND Corporation, November 2024. Report PE-A2823-1. DOI: 10.7249/PEA2823-1.

Kobzeva, Mariya A. 2021. Cooperation between Russia and China in Arctic Shipping: Current State and Prospects. *Arctic and North (Arktika i Sever)*, no. 43, June 2021, pp. 89-108. DOI: 10.37482/issn2221-2698.2021.43.89.

Strelnikova, I. & Kharina, O. A. 2024. Transformation of China's Interests in the Arctic and Potential Areas for Cooperation with Russia in the Context of International Political Turbulence, *China Report*, 60(3), pp. 287-306. DOI: 10.1177/00094455241288085.

Zhang, Q., Wan, Z., and Fu, S. 2020. Toward Sustainable Arctic Shipping: Perspectives from China. *Sustainability*, vol. 12, no. 21, 2020, p. 9012. DOI: 10.3390/su12219012.

Puranen, Matias and Kopra, Sanna. 2023. China's Arctic Strategy – A Comprehensive Approach in Times of Great Power Rivalry. *Scandinavian Journal of Military Studies*, vol. 6, no. 1, 2023, pp. 239–253. DOI: 10.31374/sjms.196.

Kuus, Merje. 2020. Regulatory Power and Region-Making in the Arctic: China and the European Union. *European Urban and Regional Studies*, vol. 27, no. 4, 2020, pp. 321–324. DOI: 10.1177/0969776420925539.belfe.

Koivurova, T. M., 2010. *Limits and possibilities of the Arctic Council in a rapidly changing scene of Arctic governance*. Polar Record, 46(2), pp. 146-157.

Jakobson, L., 2019. *China's Arctic Aspirations and the Constraints of Geopolitical Realities*. Arctic Review on Law and Politics, 10(1), pp. 45-67.

Yang, X., Rao, Y. & Chen, H., 2022. *Influence of Barents–Kara Sea Ice on East Asian Precipitation Patterns*. Journal of Climate Studies, 35(7), pp. 2235-2251.

CSM Damian MACIOROWSKI: Military Considerations of Cyberspace: Can Small States Acquire an Advantage in Offensive Cyber Capabilities?

Supervisor: Mr. Louis WIERENGA

Statement on the Use of AI Tools:

I have used Perplexity to assist in source research and citation formatting.

I have used Grammarly for spelling and grammar checks.

Introduction

Over the past decades, cyberspace has irreversibly revolutionized the methods used by states to pursue their national interests. Through its direct impact on the fundamental structures of state security and the lives of its citizens, it has become an essential pillar of political, military, and social activities. Cyberspace is no longer just an arena for the exchange of information but also an operational domain in which military activities, sabotage of critical infrastructure, and advanced information operations carried out by specialized groups sponsored by governments are conducted. The result is an ever-increasing number of attacks targeting IT infrastructure, the energy sector, the finance sector, and communication systems. Their effects can be destabilising for entire countries and regions. Therefore, developing extensive defensive and offensive cyber capabilities has become a strategic imperative for modern nation-states. As cyberspace evolves into a new battlefield, are small states proficient at developing cyber capabilities not just for defence but also to shape global events and safeguard their interests? If a single cyberattack can disrupt the infrastructure of a worldwide superpower, what might happen if small nations mastered such digital weapons for their own defence and influence?

In contrast to larger states, smaller states generally exhibit a more pragmatic approach to international relations. Their limited military power against bigger states often leads them to steer clear of direct conflicts and motivates them to seek compromise (Areng, 2014). Offensive cyber capabilities enable smaller nations to offset the conventional military advantages of larger adversaries by providing an asymmetric means of deterrence and counteraction.

To substantiate this thesis, this essay will proceed in four main parts. First, it will examine the low barriers to entry in cyberspace, demonstrating how small states can acquire offensive cyber capabilities without the massive financial investments required for conventional military forces. Second, it will analyse the asymmetric nature of cyberspace and how this operational environment favours smaller actors who can

exploit vulnerabilities in larger adversaries' systems. Third, it will explore the critical role of human capital, focusing on how small states can develop and retain qualified cyber specialists despite competition from the private sector. Finally, the essay will address the necessary infrastructure, procedures, and normative frameworks that enable small states to conduct effective and sustainable offensive cyber operations. Through this analysis, the essay will demonstrate that small states can achieve strategic advantages in cyberspace that would be unattainable through conventional military means.

Conceptual Framework: Small States and Cyber Domain Asymmetry

The authors of the publication ‘Small States and International Security: Europe and Beyond’ define a small state not only by its population or territory but, above all, as an entity that is the weaker party in an asymmetrical relationship, unable to independently change the nature or functioning of that relationship without the involvement of a larger partner (Archer et al., 2014). The material resources and the economic, military, and political potential of these states are also significant. Small states are, in addition, characterized by limited ability to influence the international environment, which, from a security perspective, often means they pursue their goals through cooperation.

According to research conducted by Harvard Kennedy School, cyberspace has emerged as a domain where small states can surmount the constraints of their traditional capabilities (Nye, 2010). Crucially, the threshold for entering competition in this domain is significantly lower than in classic military operations. Moreover, Lina Areng presents that specialist expertise, international cooperation, and technological innovation play a significant role in this process. Thanks to their smaller and more flexible structure, small countries can develop efficient mechanisms for managing and responding quickly to threats in cyberspace (Areng, 2014).

Governments and the private sector must take comprehensive measures to improve cybersecurity. According to the content of this year's World Economic Forum report, the evolving sophistication of cyberattacks, characterized by cascading effects across multiple domains, requires states to develop adaptive operational strategies, doctrines, and international cooperation frameworks (WEF, 2025). For small states, this

complexity presents both challenges and opportunities for strategic niche development. That is why cyberspace is now seen as a key arena in the fight for broadly understood national security, economic stability, and the preservation of state sovereignty.

Low entry, cost-effectiveness balance

A fundamental aspect supporting the argument of a low threshold for entering cyberspace operations is undoubtedly the favourable cost-to-effect ratio. It is estimated that even the most advanced offensive tools enabling operations in cyberspace cost significantly less than the purchase and maintenance of conventional weapons, such as air defence systems, ships, or aircraft (Ottis, 2009).

According to SOCRadar's '2024 Dark Web Report', the average prices for basic offensive cyber tools are as follows:

- Remote Access Trojan - $2,171
- Loaders - $3,566
- Mid-tier 0-day - $10,000
- Mailing and Spam Services - $100
- DDoS Services - $20
- Malware Encryption Services - $484

Combining these tools allows for advanced offensive operations to be carried out for less than $15,000 (SOCRadar, 2024). This amount usually covers the tool price, infrastructure leasing, and the service provider. The data presented by the TECHx report on the cost of cyber tools available on the Dark Web is particularly telling. On the one hand, the infostealer family of tools, which are very popular nowadays and designed to steal data from devices connected to the Internet, costs $400. On the other hand, basic tools for creating and running phishing campaigns cost a few dozen dollars. The most expensive tools on this list are ransomware and exploits, which can cost up to several million dollars. However, these are the most advanced tools, the use of which can cause complete paralysis and irreversible damage to the attacked organisations or critical infrastructure (TECHx, 2025).

The ratio of these costs to the potential effect of operational activities stands in sharp contrast to the costs of conventional weapons. For comparison, the cost of purchasing a single F-35 fighter jet is around $100 million (SimpleFlying, 2023). The high costs of crew training, maintenance, logistics, and infrastructure further increase its price. For most countries, especially those with limited defence budgets, such high barriers limit their access to powerful military capabilities.

However, cyber operations fundamentally change this dynamic. Countries with relatively modest resources can develop real operational capabilities without incurring the enormous costs associated with traditional weaponry. An example of this paradigm is Estonia, which, despite its limited financial and military resources, has achieved a global position in cybersecurity.

Estonia as an example and its contribution to the development of NATO cybersecurity

A particularly salient example of a nation with limited military and financial resources yet considerable operational capabilities in cyberspace is Estonia. When massive cyberattacks paralyzed state and private infrastructure in 2007, Estonia took decisive action to secure its own systems. As a result, it has become one of the global centers of cybersecurity innovation. According to one of the leaders of Estonia's digital transformation, Jaan Priisalu, Estonia has evolved into a symbol and benchmark for the whole world in terms of technology development and cybersecurity strategy (ERR, 2017).

Its small military potential and limited resources have not prevented Estonia from making an unprecedented contribution to NATO and the international cybersecurity architecture. Established on Estonia's initiative in 2008, the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn brings together 39 member states and is one of the key training, research, and defence institutes in the field of cybersecurity (CCDCOE, 2025). However, this is not Estonia's only contribution to the development of NATO's operational capabilities in cyberspace.

It played a key role in the creation of the Tallinn Manual, a document setting out the principles of international law in cyberspace. It identifies 154 principles governing cyber operations and provides extensive commentary on each of them. It also addresses topics such as state sovereignty and responsibility, human rights, and maritime, air, and space law in the context of cyberspace. The Tallinn Manual has become an essential normative act for legal advisors (CCDCOE, 2025). It also influences the cybersecurity policies and doctrines of other countries and organisations.

Thanks to its involvement in global cybersecurity development, Estonia has built a broad competence base, enabling it to increase its influence on the international stage significantly. Indicators presented by e-Estonia

- 99,6% of electronic bank transfers,
- 98% of tax returns filed online,
- and 99% of prescriptions issued electronically,

make Estonia one of the most digitally advanced countries in the world (e-Estonia, 2025).

As a result, it significantly influences the setting of normative standards and solutions in cyberspace. Estonia has evolved into a model that shows that even small countries with the right strategies can become key players in the international cybersecurity arena. However, it must be noted that Estonia's international prominence stems primarily from defensive and normative contributions rather than documented offensive cyber operations, which, if they exist, remain classified or deliberately obscured from public view. The country's strategic influence derives from setting international standards and providing collective defence infrastructure, which may constitute an alternative form of 'soft power advantage' in cyberspace rather than kinetic offensive superiority.

Asymmetry and anonymity in cyberspace

The asymmetric nature of cyberspace distinguishes the digital domain from traditional theaters of conflict, making it one of the most important phenomena in contemporary international security. The advantages usually associated with a larger armed force or a more powerful economy do not apply in cyberspace. Therefore, in the digital

environment, even a single actor with the appropriate technical knowledge, creativity, and ability to quickly adapt to changing conditions can gain an advantage over a world power state (Areng, 2014).

A key feature of asymmetry in cyberspace is the disproportion between the effort required to carry out an attack and its potential impact. The 2007 cyberattacks on Estonia demonstrate how relatively simple DDoS attacks, launched by non-state actors, can paralyze an entire nation's digital infrastructure, affecting banking, media, and government services (Li, 2024). Moreover, cyberattacks are often nonlinear, meaning that an attack on one segment of the network infrastructure can escalate its effects. This effect results from the interconnections between systems, which are often interdependent. The failure of one system can trigger a cascading effect, causing other systems to fail, thereby increasing the attack's overall impact.

Asymmetry in the cyber domain also manifests itself in temporal dynamics. While large states need time to make decisions due to complex bureaucratic processes, small actors can quickly change tactics, thus adapting to the situation (Li, 2024). The advantage in decision-making speed allows them to effectively circumvent traditional defence mechanisms and exploit security gaps before they are fixed. However, to achieve this advantage, coordination among the state's internal organisational structures is required.

Cyberspace also opens new opportunities to circumvent traditional geographical and physical limitations. Unlike kinetic operations, where operational range is limited by terrain and distance, such physical constraints are irrelevant in cyber attacks (Akdağ, 2025) This characteristic allows small states to access neutral or enemy systems regardless of their location. Taking control of such a system is referred to as proxy and is synonymous with gaining ground in kinetic operations. It allows the attack to be transferred to an environment that is not attributed to the state conducting the operations. Acquiring this capability provides for the anonymization of operations, making the attack very difficult to attribute (Prasad et al., 2025).

One of the most interesting aspects of cyberspace from an attacker's perspective is the ability to maintain anonymity. It allows small countries to conduct offensive

operations without revealing their identity. Cloud infrastructure, VPNs, and anonymizing communication protocols enable attackers to hide their identities and locations, making it much more difficult to defend against and respond to their actions. As a result, small countries can conduct long-term campaigns without the risk of direct confrontation. Cyberspace provides anonymity unavailable in other operational domains.

Rain Ottis, in 'Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability' argues that the challenges associated with attribution are critical to the operational advantage that small states can achieve. He notes that in the case of Estonia's attack in 2007, the attackers remained anonymous, and none of their campaigns proved to have direct state support (Ottis, 2009). These attacks appeared to be carried out by individuals or hacktivist groups acting at random.

Thus, through technical means, small states can conceal their actions, lower the risks of retaliation, and conduct ongoing campaigns beyond the reach of traditional detection and deterrence mechanisms. This degree of anonymity, unavailable in land, sea, air, or space domains, fundamentally alters the cost-benefit calculus for small actors, reinforcing cyber as an arena of unique asymmetric potential.

Human capital and talent management

Strategic investments in recruitment, development, and, above all, the retention of qualified personnel are key to enabling small countries to gain an advantage in offensive cyberspace capabilities. Due to their limited populations, they are often forced to maintain compulsory military service, which can significantly improve the process of recruiting qualified specialists.

Estonia and Finland have adopted models based on mandatory military service with a cyber component. In Estonia, compulsory military service lasts 11 months and includes basic and specialized training. One of the many specialized training areas is cybersecurity, which focuses, among other things, on offensive capabilities. (Hurt, 2021). The Finnish armed forces have developed an even more advanced system in which candidates for cyber soldiers must, after completing compulsory basic training,

pass a cybersecurity test. On this basis, they are assigned to serve in the Finnish Defense Forces C5 Agency (Hurt, 2021). Thanks to this selection process, these countries can implement a talent management system as early as the stage of qualifying candidates for compulsory military service.

However, this is not the only way to identify young talent. Many governments have implemented extensive programs for developing cybersecurity in elementary and secondary schools. Singapore has developed SG Cyber Youth, a national program led by the Cyber Security Agency of Singapore that systematically reaches out to secondary school students. The CSA plans to reach 10,000 young people in just three years through training boot camps and competitions. The best students have the opportunity to participate in the central Capture the Flag competition, which serves as a talent selection mechanism (Singapore CSA, 2025). Estonia's Centre for Digital Forensics and Cyber Security has created a system of interlinked competitions for different school levels. Between 2017 and 2021, over 150,000 students aged seven and above participated in this program (e-Estonia, 2022).

A fundamental challenge for all military organisations, especially in the face of competition from the private sector offering significantly higher salaries, is retaining qualified specialists. Small countries such as Estonia focus on creating a ‘win-win’ model that benefits both the Armed Forces and volunteers. This system allows cyber conscripts to earn certificates or university ECTS points through military service. A similar solution is also used in Sweden (Hurt, 2021).

Countries seeking to improve their offensive capabilities in cyberspace can also strategically build a reserve of cyber specialists. This system enables the development of a large pool of experts at a significantly lower cost than professional military personnel, which is particularly important for countries with limited financial resources. Moreover, reservists who work as cybersecurity specialists in the private sector daily bring up-to-date knowledge of the latest techniques, tools, and procedures used in the civilian environment to the armed forces, enabling a two-way transfer of knowledge and experience, which increases the armed forces' awareness of technical innovations in the private sector while strengthening the state's operational capabilities in the cyber domain (Baezner, 2020). The reserve model also addresses personnel shortages by

providing experts with flexible terms of service that are an attractive alternative to full-time military service, with its financial and organisational constraints.

The key to success for small countries is to ensure that military service adds value to a specialist's professional career. Combining compulsory military service with a cyber component, practical training in offensive operations, cooperation with the academic and private sectors, and the creation of flexible reserve structures can effectively build and maintain a highly qualified specialist workforce.

Possible hazards and risks

Despite many favorable factors that enable small states to gain an advantage through offensive cyberspace capabilities, several critical counterarguments must be addressed. One of these is the growing reliance on digital infrastructure and private-sector service providers. As Tan (2019) observes in ‘A Small State Perspective on the Evolving Nature of Cyber Conflict’, the interconnection of critical infrastructure systems increases the potential for attacks on supply chains and infrastructure sabotage, which, in turn, can significantly limit both offensive and defensive operations. Structural dependence on private companies managing critical state infrastructure creates the risk of fragmentation and conflicting priorities. Etzioni argues that excessive delegation of key cybersecurity functions to the private sector may simultaneously weaken state control and responsibility over the operation of these systems (Etzioni, 2011).

A key threat to the attainment of offensive cyberspace capabilities is the exodus of skilled workers to the private sector. The World Economic Forum reports that the global cybersecurity industry urgently needs 4 million additional specialists to fill the talent gap, with only 15% of companies expecting a significant increase in cyber competencies by 2026 (WEF, 2024). ISC2 data further reveals that despite growing cyber threats, the global active workforce in the cyber sector has stalled at 5.5 million people, leaving a gap of 4.8 million workers, 19% increase in the shortage year-on-year (ISC2, 2024). This poses a massive challenge for small countries competing with lucrative private sector salaries.

Finally, there is the problem of false attribution and potential escalation of conflict. In his publication *Escalation Dynamics and Conflict Termination in Cyberspace*, Lin defines this phenomenon as catalytic escalation. It involves conducting a ‘false flag’ operation in which third parties, such as hostile states or APT groups sponsored by them, provoke conflict between two states (Lin, 2012). Research on attribution in cyberspace conducted by UNIDIR states that false attribution can result from hasty political decisions or technical fraud, such as spoofing. This threat can lead to a deterioration in relations or escalate into direct conflict between states (Kastelic, 2023).

Conclusion

This essay has demonstrated that small states have real capacity to achieve superiority in offensive cyberspace operations, despite the limitations imposed by their size and resources. The arguments presented in this paper demonstrate that the dynamic and asymmetric structure of cyberspace enables states with limited military capabilities to challenge traditional power hierarchies and pursue their interests in ways previously impossible.

Thanks to low barriers to entry, even states with limited resources can develop effective offensive capabilities in cyberspace by leveraging the flexibility of their structures and speed of decision-making. Examples such as Estonia and Finland show how strategic investments in talent management, educational programs, and public-private sector cooperation transform limitations into strengths, enabling these countries to become key players in global cybersecurity. System integration and the ability to operate under anonymity further allow small countries to defend themselves effectively and conduct offensive operations regardless of geographical constraints.

Despite this, several challenges are associated with the attainment and maintenance of cyberoperations capacity. The risks inherent in overreliance on infrastructure, the maintenance of skills, and the ambiguous nature of attribution and escalation in cyber wars underscore the need for holistic, adaptable approaches. These approaches are needed to balance innovation, adaptability, and cooperation with robust legal and procedural mechanisms.

In summary, examples from small nations such as Finland and Estonia show that, with conscious policy formulation, foresight, and cross-border collaboration, the constraints inherent to size and resources can not only be mitigated but also turned into sustainable pillars of digital capacity and security in cyberspace. The future course of global cybersecurity will increasingly depend on the ability of small nations to adapt, innovate, and utilize the asymmetrical advantage efficiently afforded by the digital environment.

Bibliography

Akdağ, Yavuz. 2025. Great Power Cyberpolitics and Global Cyberhegemony. *Perspectives on Politics.* 2025.

Archer, Clive and Alyson Bailes, Anders Wivel. 2014. *Small States and International Security : Europe and Beyond.* London : Routledge, 2014.

Areng, Liina. 2014. *Lilliputian States in Digital Affairs and Cyber Security.* Tallinn : NATO Cooperative Cyber Defence Centre of Excellence, 2014.

Baezner, Marie. 2020. *CSS Cyber Defense Report: Study on the use of reserve forces in military cybersecurity.* Zurich : Center for Security Studies, 2020.

CCDCOE. 2025. *NATO Cooperative Cyber Defence Centre of Excellence.* [Online] 2025. [Cited: 10 21, 2025.] https://ccdcoe.org/research/tallinn-manual/.

CCDCOE. 2025. *NATO Cooperative Cyber Defence Centre of Excellence.* [Online] 2025. [Cited: 10 21, 2025.] https://ccdcoe.org/about-us/.

e-Estonia. 2022. *Estonian Business and Innovation Agency.* [Online] 2022. [Cited: 10 16, 2025.] https://e-estonia.com/cybersecurity-education-in-estonia-from-kindergarten-to-nato-cyber-defence-centre/.

e-Estonia. 2025. *Estonian Business and Innovation Agency.* [Online] 2025. [Cited: 09 20, 2025.] https://e-estonia.com/wp-content/uploads/e-estonia_story_main_facts.pdf.

ERR. 2017. *Estonia's reaction to cyber attacks influenced global security policy.* [Online] 2017. [Cited: 09 20, 2025.] https://news.err.ee/592075/estonia-s-reaction-to-cyber-attacks-influenced-global-security-policy.

Etzioni, Amitai. 2011. *Cybersecurity in the Private Sector.* Dallas : National Academy of Sciences, 2011.

Hurt, Somer. 2021. *Cyber Conscription, Experience and Best Practice from Selected Countries.* Tallinn : International Centre for Defence and Security, 2021.

ISC2. 2024. *Cybersecurity Workforce Growth & Skills Gap Insights.* Virginia : International Information System Security Certification Consortium, 2024.

Kastelic, Andraz. 2023. *Non-Escalatory Attribution of International Cyber Incidents.* Geneva : United Nations Institute for Disarmament Research, 2023.

Li, Tony Yuan. 2024. *Asymmetry in the Digital Age: Cyber Deterrence Strategies for Small States.* Tampa : The University of South Florida Libraries, 2024.

Lin, Herbert. 2012. *Escalation Dynamics and Conflict Termination in Cyberspace.* Alabama : Air University Press, 2012.

Nye, Joseph S. 2010. *Cyber Power.* Belfer Center for Science and International Affairs. Cambridge : Belfer Center for Science and International Affairs, Harvard University, 2010.

Ottis, Rain. 2009. *Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability.* Tallinn : NATO Cooperative Cyber Defence Centre of Excellence, 2009.

Prasad, Nilantha and Abebe Diro, Matthew Warren, Mahesh Fernando. 2025. A survey of cyber threat attribution: Challenges, techniques, and future. 2025.

SimpleFlying. 2023. *Simple Flying.* [Online] 2023. [Cited: 09 20, 2025.] https://simpleflying.com/how-much-does-an-f-35-cost/.

Singapore CSA. 2025. *SG Cyber Youth.* [Online] 2025. [Cited: 10 16, 2025.] https://www.csa.gov.sg/our-programmes/talent-and-skills-development/sg-cyber-talent/sg-cyber-youth/.

SOCRadar. 2024. *Annual Dark Web Report.* Newark : SOCRadar, 2024.

Tan, Eugene E.G. 2019. *A Small State Perspective on the Evolving Nature of Cyber Conflict: Lessons from Singapore.* Washington : National Defense University Press, 2019.

TECHx. 2025. *Techxmedia.* [Online] 2025. [Cited: 9 20, 2025.] https://techxmedia.com/en/dark-web-study-reveals-cost-of-cybercrime-tools-and-ransomware/.

WEF. 2025. *Global Cybersecurity Outlook.* Geneva : World Economic Forum, 2025.

WEF. 2024. *Tackling cybersecurity's global talent shortage.* Geneva : World Economic Forum, 2024.

BALTIC DEFENCE COLLEGE