Issue N 2

Volume 2
ISSN 2980-5104 (online journal)

BSEMR

THE BLACK SEA AND EASTERN MEDITERRANEAN REVIEW

OPEN ACCESS PEER REVIEWED E-JOURNAL FOCUSING ON THE BSEM

Published by the Laboratory for Black Sea and Mediterranean Studies (Faculty of Social and Economic Sciences, Aristotle University of Thessaloniki) and the School of Law (University of Nicosia)

Supported by the Black Sea and Eastern Mediterranean Academic Network (BSEMAN)

DISCLAIMER

The views expressed in the articles, commentaries, policy papers and book reviews published in this journal are those of the authors and do not necessarily represent the views of the publishers, the Editorial Board or the Editorial Team

P.O. Box 24005
1700 Nicosia, Cyprus
T: (+357)22842447
E: bsemr@auth.gr
https://lawjournals.unic.ac.cy/index.php/bsemr/index

ISSN 2980-5104 (online journal)

CONTENTS

Volume 2, Issue 2

Editorial Note by the Editor-in-Chief: Win or Perish – Perish you Will Despite Winning

The war against Iran has set the Eastern Mediterranean Region (EMR) and the Middle Eastern regions (MER) on fire, causing extensive damages. The continuing, joint assault by the USA and Israel on Iran was launched on 28 February 2026, amidst negotiations, in stark violation of International Law. This has groundly shaken and already impacted severely on the international order and on the provisions of international law. Consequently, global trade has been drastically curtailed while orderly international life and every sense of rules-based co-existence, including conflict resolution, are threatened with collapse. By its geopolitical location and nature, the broader Middle Eastern Region is a global energy hub. It hosts not only crucial global energy production and sources of other vital products such as fertilizers, but also vital trade paths and essential world navigation passages. The perils involved in the escalated military assaults in this region and the danger they pose to the global economy are evident.

Conjunctural Specificities

Several unprecedented characteristic traits stand out for observation and evaluation of this war against a sovereign state: First, it is not officially approved by the US Congress, while war objectives and agendas remain vague and seem to be 'rolling' from day to day. Secondly, most if not all, middle eastern states are, this time, entangled or affected, albeit with various degrees of severity. Included are even neighbouring NATO members, such as Turkey and EU member-states such as Cyprus. Thirdly, the atrocious war tactic of decapitating enemy leaders has intensified and appears to be being generalized in an unprecedented way. Fourthly, diplomatic initiatives are routinely invoked as holding by the American president but are consistently denied by his adversaries. More unforeseen processes have emerged, like the rolling 'fake statements and fake news' which occupy massive amounts of space in the public domain. Fifthly, oil and financial markets' prices are thrown into stressful spirals of unease or into panics; a novel condition emerges that is of the shaky market price-pendulum motion. Sixthly, underhand stock market dealings appear to be in play,

including financial market manipulations by holders of exclusive inside information.

This twin military attack brought about all kinds of turbulence and has been deemed both illegal and illegitimate, violating bilateral and multilateral norms at domestic, regional, international, and UN levels. The German president Frank Walter Steinmaier, Italian premier Georgia Meloni, Spanish prime minister Pedro Sanchez, and the Polish foreign minister Radoslaw Sikorski are among those EU leaders who either expressly or implicitly have denounced the Iran war as illegal. Members of both the Israeli and the American governments are facing litigation cases in domestic and international courts. However, even before the war began, aggressors had demonstrated contempt for the principles of international law, as applied in the entire post-Second World War period. Moreover, they repeatedly challenged law-bound governance, by violating UN Charter provisions and failing to heed the verdicts of the International Criminal Court, such as in respect of the genocide in Gaza.

Causes and Effects

These sets of facts along with their inherent consequences highlight globally unprecedented havoc, a unique global quagmire. Given such calamity, urgent global initiatives are imperative. Unless radical, responsible measures are initiated to advance solutions towards peace and global reconstitution of multilateralism, the world risks the demolition of reciprocity and rules-based co-existence. *Bona fide* governance initiatives or mutually beneficial common *modi operandi* in International Relations risk being eclipsed. The world is faced with a specter of irrationality. Indeed, the currently dominating irrationalism risks becoming entrenched. Indeed, celebration over instances of absurdity have surfaced, as individual whims are elevated to the status of policy. In the wake of such trends, at severe risk come vital 'public goods', especially global public goods.[1] Since January 2025 the new US administration has started deploying mainly strategies of blackmail and ultimatums. Indicative and disturbing are the cases of claims to Canada, Greenland, Venezuela and Iran, but also NATO-splitting utterances. Expressly or implicitly, these aim at subjugating everyone indiscriminately, whether adversaries or allies.

[1] That is, goods without which economies and societies of the entire planet cannot operate or sustain a normal life.

This is an astounding manifestation of the implosion of the 50-year-old neoliberal onslaught and, a key to deciphering current turbulent disturbances. Over this period, leaders' actions, inactions or decisions have caused a slide towards excesses of deregulation, impunity, and corruption. They have violated rules and norms, and abolished regulations to benefit own dominant industries in global competition. This has caused a boomerang effect, inevitably, as they have corroded and squandered trust, the importance of which is paramount, indeed vital. Nothing can be obtained without trust. The impropriety of blatantly trampling on rules became a frequent aberrant practice, especially whenever their own narrow profit and interests were at risk. Consequently, states violated their own doctrines of competitiveness and fair competition. Whenever such precepts endangered their expectations of profit, they were circumvented and rejected, with reckless opportunism. In this way, the trampled norm of 'Free trade' was simply weaponized for partisan profiteering. But crushed rules, undermine fair competition, multilateralism and mutual respect for the rules, in all types of transactions.

Inevitably grave market dysfunctions, trade stoppages and huge losses have arisen. As a systemic part of this war news media and outlets in their own 'games' tend to focus on news contents preferentially, by framing them emphasizing, for instance, only short-term losses and damages. Extensive corruption incidents, witnessed among government associates, suggest that various types of profiteering ploys operate, yet these are omitted. Thus, both the launching of the war on Iran and its operational management, over the first five weeks, suggest covert exploitations. Surely, the lack of clearly stated plans of exiting from it intensifies these scenarios.

Unsurprisingly, the USA, as the leading global power, has already managed: first, to isolate itself even from long term, trusting allies. Secondly, to render itself a broadly unaccountable and untrustworthy actor, both domestically[2] and globally[3]. Thirdly, perhaps the most severe American strategic-tactical failure concerns its disregard or defiance of the now irreversible condition of globalization. Intrinsic to this is the insurmountable condition of *international and transnational interdependence*

[2] See for example regular public post statements by professors: John Mearsheimer, Paul Krugman and Jeffrey Sacks over the period since the beginning of the war on Iran.
[3] No countries other than Argentina have uttered public support for the belligerence of the USA and Israel. The leaders of several countries, including the German president F.W. Steinmayer, have expressly stated their opposition.

between nations economically, trade-wise, politically, diplomatically and socially. Such 'negligence' betrays shortsightedness, which translates into governmental failure but also to frustration for concerned peoples including the Americans.

Acute Endangering of Environment, Climate and Planetary risks

The massive shelling and use of weaponry in the war have brought irreparable damage to the environment. Damage calculations vary but are surely heavy and irreversible. The specificities of contemporary digital time make high demands on governance and require novel and resilient approaches that are far more intricate than in the age of single-standing nation states or of national economies. Governmental perspicacity, versatility and judiciousness are crucial. So, even if the US administration were actually to have had a plan, or perhaps a hidden agenda such as an 'imperial strategy against China', followed up handlings, decisions and results combine to frustrate or entrap it. Indicatively, a series of US army heads have recently been removed, at the height of the campaign. Most perplexing is the *sui generis* 'political autism' of presidential briefings, quasi-official stances, which reveal the short-termism of the endless, crude blackmails and ultimatums addressed to both allies and enemies, during the second term of the Trump administration. The incessant, violent attacks, also verbal, including against civilians, give further evidence of such unjustifiable, unaccountable actions. So, it is unsafe to deduce any overt or covert strategies by such actors and aggressors in the Eastern Mediterranean and Middle Eastern war zones. Contradictory, or intentionally vague statements confuse matters further, rendering logical explanations impossible or futile.

In the current conjuncture, this war theatre unfolds while people, societies and states suffer from a historically unprecedented 'crisis of truth', the lies and fake news that affect us all, collateral damage of an extremely unprincipled neoliberal regime. Media outlets prone to systematic propaganda follow the demands of the richest bidder, rather than providing factual descriptions of reality and truth. Cumulatively, all these factors render political leadership debilitated and less accountable. They certainly also leave citizens weaker and undermine the trust essential to the functioning of political institutions, already exacerbated by AI. Double standards are the *constant* in the framing of realities. Yet, in globalization people can potentially watch war news

originating from any country, which provides for cross-checking. In every case, war reality does not differ just because people watch news about it from another country's media.

Global Chaos or Global Governance?

Organized societies normally follow certain kinds of rational management, planning and enforcing rules-based community structures and institutions. Since the mid-20th century, the USA has been broadly viewed in the West as a model liberal state, in this respect. But the adoption of extreme unilateralist practices by its government has caused splits, fears, animosity, and conflicts while promoting global chaos. For any democracy there is no worse calamity than sliding into violating its own principles and its very constitution. Yet, the idea that 'anything goes' that has ruled for so long, has wrecked key values and has now reached rock-bottom, with the USA following a 'law of the jungle' as if this nation were the sole inhabitants on earth and its government the sole actor.

In view of this dire state of affairs, statesmanship and leadership are urgently required from the nations of the UN to address the aberrations and to prevent and contain the damages which are being caused. The need for globally responsible leadership is now more urgent than ever. And so is the need for multilateralism.

In this fourth issue of BSEMR editors are pleased to host three interesting and very topical articles and one book review.

First Article: Cybersecurity and International Law: Charting Stability in the Black Sea–Eastern Mediterranean Region. This article by **Dr Gijo George** focuses on the intersection of internet technology applications such as cyber-attacks, international law, state power capacities and policy options. Regarding the Black Sea and Eastern Mediterranean regions in particular, the author holds that these applications are in full operation. Aggressive cyber and electronic operations such as the satellite navigation jamming commercial vessels are used systematically to exploit partisan strategic aims and gain advantages. He explains how such critical infrastructure intrusions and disinformation campaigns remain hidden in war conflicts by implicated state authorities. This is why they test the boundaries of existing international law while concurrently undermining it. Such threats evade identification and concrete attribution

as they fall below observation thresholds in cases of traditional armed conflict. So, they challenge the ability of states to preempt predators or respond intelligently. The author elaborates on the limits of the law and the corresponding liabilities for governance defense possibilities of concerned states. Since many cyber-tech assaults move below the threshold of state's capacity to avert dangers, damages impact on state powers. This results in non-state actors gaining undue and superior power. Such gaps challenge even the ability of states to avert attacks but also to uphold trust in their institutions and norms.

Second Article: Unequal Partners? Rethinking Burden Sharing in a Future European Defence Union. In his article **Dr Georgios Papagiannis** compares differences and key discrepancies in the defense capacity of states. Notably, he examines percentages of expenditures, as a quota of the respective gross domestic product (GDP) and the corresponding national income, among EU member states. Considerable or significant, occasionally extreme discrepancies occur. Countries, like Greece, for instance, invest a higher percentage on defense and military expenditures, while for instance more cosy Central European countries, thus far, used to spend minimal sums of their GDP. Other significant differences or discrepancies concern the defense industries and corresponding productive capacity allocation between member-states. The EU is currently proceeding towards restructuring its general defense agendas, aiming to construct viable, autonomous, self-reliant and effective defense systems. For this to succeed it is crucial that member obligations are judiciously designed and costs are allocated and shared in a balanced way. In the current rapidly reshuffling phase of NATO these preconditions are paramount. It is crucial that defense priorities and balanced tasks are set out judiciously and fairly.

Third Article: Narratives of Maritime Sovereignty: The *Mavi Vatan* Doctrine.

In his article **Mr Theodore Skarvelis** examines the recent 2019 project of *Mavi Vatan* (Blue Homeland) by Türkiye, as part of its recently adopted doctrine. In this context, the study investigates identity-driven geopolitics, where the evolving nature of *regional security* is characterized by multipolarity, but notably also by contested legality. The author notes that this strategy was developed by Turkish admirals as *Mavi Vatan* projects involve maritime geostrategic visions that challenge accepted international law

statutes and prevailing international practice norms, such as UNCLOS. Rather, these tie in with the growing narrative about Türkiye's regional encirclement and its subsequent advancing a new conception or ideology. Based on the theoretical framework of critical geopolitics, the author draws on ten interviews with Turkish Professors. He conducts a content and discourse analysis of this material, according to Critical Discourse Analysis principles, to cross-explore the narratives underpinning *Mavi Vatan*. So, the doctrine's key narrative strands are explained as involving: the reconstruction of Turkish national identity and image, the portrayal of Türkiye as a maritime nation, and narratives of historical legacy. Thus, it is noteworthy that the Blue Homeland discourse / ideology is having a remarkable influence on Turkish Foreign Policy, as is witnessed in the 2019 Türkiye-Libyan Memorandum of Understanding.

Book Review

Dr Panagiota Manoli has reviewed the book entitled: **Dynamics of the Ukraine War: Diplomatic Challenges and Geopolitical Uncertainties**, authored by Viktor Jakupec, (Springer, 2024, ISBN 978-3-031-52444-8 (eBook, 120 pages.)

This recently published book, only two years since the Russian invasion of Ukraine, is a monograph in the form of an *eBook*, forming part of the Springer's series: *Contributions to International Relations*. According to the reviewer, the book provides a realistic account of the first twenty months of the war. In its nine chapters it charts the political complexities of the Russo-Ukrainian war, especially those which are considered key for a potential resolution of this prolonged conflict. The uncertainties along with the specificities of the Russo-Ukrainian war are identified in military strategies, political decision-making, but also in the multifaceted, complex and unpredictable nature of the conflict per se. Notwithstanding the repeated diplomatic efforts, these failed, due also to 'bloc' competing political perspectives, to 'threat' perceptions which seem to constitute the essential political hurdles that result in perpetuating this Russo-Ukrainian war. The reviewer notes that for the analysis of the broad-based discussions, several interconnected themes have been considered, including the western strategies of military support to Ukraine, the sustained sanctions against Russia, the notion of *Zeitenwende* and emerging alliances, as well as the role of propaganda and the reconstruction dynamics of Ukraine.

Dr Sophia Kaitatzi-Whitlock

Volume 2, Issue 2

RESEARCH ARTICLES

Cybersecurity and International Law: Charting Stability in the Black Sea–Eastern Mediterranean Region

DR GIJO GEORGE[1]

Abstract

In an era of geopolitical flux, cyberattacks have become a new battleground that intertwines state security with private life. The Black Sea and Eastern Mediterranean regions have seen aggressive cyber and electronic operations (e.g. satellite-navigation jamming of commercial vessels) used to advance strategic aims. Such stealthy conflict —from critical-infrastructure intrusions to disinformation campaigns— test the limits of existing international law. These threats often evade easy attribution and fall below the threshold of traditional armed conflict, challenging states' ability to respond. Under current public international law (the UN Charter and Geneva Conventions), the use of force is broadly prohibited, and civilian harm must be minimized. International law is incoherent with the dominance of non-state actors (hackers, firms, etc.) in cyberspace and thus has no teeth against digital aggression. The result is routine noncompliance with little accountability, which erodes trust in institutions and norms. This paper's central research question asks: can international law, as currently structured, effectively constrain cyber aggression and preserve stability in the Black Sea–Eastern Mediterranean (region), or are new legal frameworks required? The paper addresses this through a doctrinal analysis of treaties, UN resolutions, North Atlantic Treaty Organization/European Union declarations, and state cyber doctrines. The study suggests that bridging the cyber gaps is crucial to reinforcing the rule of law and preventing the erosion of international order. In the Black Sea–Eastern Mediterranean

[1] Principal and Professor of Law, Jarbom Gamlin Government Law College, Itanagar, India.

region, strengthening cyber norms would help sustain social cohesion and uphold political credibility during crises.

Keywords: cybersecurity; international law; state sovereignty; hybrid warfare; regional security

Introduction

In today's great-power rivalry and hybrid warfare, the Black Sea–Eastern Mediterranean area has emerged as a frontline. Situated between Europe, Asia and the Middle East, it is often seen as a major geopolitical hotspot, a contested zone where larger geopolitical forces play out with implications for shipping routes, energy, infrastructure and even global food security.[2] Recently this vital corridor has faced a surge of cyber and electronic attacks –from jamming satellite navigation to hacking networks and spreading disinformation– deployed secretly to advance strategic goals.[3] These activities push the boundaries of existing law. Under Article 2(4) of the UN Charter, states must refrain from the threat or use of force against the territorial integrity or political independence of any state. Concurrently, International Humanitarian Law, specifically Additional Protocol I, mandates that parties to a conflict distinguish between combatants and civilians to minimize harm to the latter.[4] Experts warn that such ambiguous aggression in the Black Sea could make all forms of security, including safe navigation and infrastructure, very uncertain.[5] Similarly, U.S. officials note that adversaries are running advanced disinformation campaigns led by Russia, China and Iran that corrode trust and threaten any progress in the region. Cyberspace has become

[2] Heinz-Jürgen Axt, *'conflicts and Global Powers in the Eastern Mediterranean. An Introduction'* (2022) 70 *Comparative Southeast European Union Studies* 393–413.

[3] Henrik Praks, *Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage* (Hybrid CoE Working Paper 32, European Union Centre of Excellence for Countering Hybrid Threats, May 2024) 17 https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf, accessed 20 September 2025.

[4] Zhifeng Jiang, 'Regulating the Use and Conduct of Cyber Operations through International Law: Challenges and Fact-finding Body Proposal' (2020) 5 *LSE Law Review* 59, 60.

[5] Christian Bueger and Tobias Liebetrau, 'Critical Maritime Infrastructure Protection: What's the Trouble?' (2023) *Marine Policy 155* 105772, 1.

a strategic battleground blending national security and private life, endangering regional stability and putting strain on traditional legal norms.[6]

The central research question of this study asks whether current international law can effectively constrain cyber aggression and preserve stability in the Black Sea–Eastern Mediterranean (region), or whether new legal frameworks are needed. Put differently: can the UN Charter's rules governing the use of force (*jus ad bellum*) and the principles of International Humanitarian Law —often referred to as the Law of Armed Conflict— apply adequately in cyberspace? Western governments (North Atlantic Treaty Organization and European Union members) tend to insist that the existing Charter-based regime covers cyber attacks.[7] In contrast, Russia and its allies have repeatedly complained that international law lacks teeth in the cyber domain and have even proposed a new binding cyber-security treaty.[8] This divergence raises practical dilemmas. For example, would a large-scale hack on a coastal nation's power grid count as an armed attack under Article 51 and trigger collective self-defense, or would it be treated as ordinary crime? Scholars warn of routine noncompliance and eroding norms if these uncertainties persist.[9]

This article uses a doctrinal legal methodology, analyzing key texts –the UN Charter, Geneva Conventions, treaties, UN resolutions, and major alliance declarations– as well as national cyber doctrine statements, to clarify how jus ad bellum and jus in bello intersect with cyber operations. The paper proceeds as follows: Section 2 surveys the regional cyber-threat landscape; Section 3 examines applicable international legal norms (the use-of-force and IHL frameworks); Section 4 identifies

[6] Samantha Bradshaw, Hannah Bailey and Philip N Howard, *Industrialized Disinformation: 2020 Global Inventory of Organised Social Media Manipulation* (Project on Computational Propaganda, Oxford Internet Institute Working Paper 2021.1, 2021) https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/01/CyberTroop-Report-2020-v.2.pdf, accessed 20 September 2025.

[7] Lucas Kello, 'Cyber legalism: why it fails and what to do about it' (2021) *Journal of Cybersecurity 7* tyab014, 1 https://doi.org/10.1093/cybsec/tyab014.

[8] Aleksi Kajander, *Unnecessary Repetition: Russia's Latest Attempt at a New UN Convention on Cyberspace* (North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence 2023) 1 https://Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization).org/uploads/2023/08/UnnecessaryRepetitionFinalVersionExportV2-1.pdf accessed 20 September 2025.

[9] Lorraine Finlay and Christian Payne, 'The Attribution Problem and Cyber Armed Attacks' (2019) 113 *AJIL Unbound* 202 https://doi.org/10.1017/aju.2019.35 accessed 20 September 2025.

current legal gaps; Section 5 compares Western (NATO/EU) and Russian approaches; Section 6 presents a hypothetical cyber-attack case study; Section 7 suggests legal adaptations (defining cyber armed attacks and strengthening IHL in cyberspace); Section 8 reviews multilateral norm-building initiatives; and Section 9 concludes with implications and recommendations.

1. Cyber Threat Landscape in the Black Sea–Eastern Mediterranean

A. Geopolitical and Cyber Context

The Black Sea–Eastern Mediterranean region is a crossroads of competing security interests. It lies where Russia's western flank (the Black Sea) meets the Eastern Mediterranean conflicts (such as Syria and Israel–Iran tensions). Russia's full-scale war in Ukraine has turned the Black Sea into a main point of confrontation between Russia and North Atlantic Treaty Organization/European Union countries, while old disputes (for example over Cyprus and maritime boundaries) and rivalries (such as Turkey–Greece or Iran–Israel) keep the Eastern Mediterranean tense.[10] Experts describe this area as wedged between the European Union, Ukraine, Russia, Türkiye and the Caucasus, meaning any conflict there could have wide repercussions. In this environment of strategic ambiguity—frequently categorized by security analysts as a 'gray zone' between routine statecraft and open armed conflict—states increasingly employ cyber tools as part of hybrid warfare.[11] For example, in peacetime Israel–Iran confrontations or during North Atlantic Treaty Organization exercises, adversaries can quietly infiltrate networks or jam signals without open hostilities. The Internet and electronic systems have become another arena of competition: satellite communications, navigation (Global Navigation Satellite System(s)), power grids, ports and even social media can be disrupted or weaponized to gain advantage without crossing the conventional force threshold.[12] This digital front will challenge the

[10] Atlantic Council Task Force on Black Sea Security, *A Security Strategy for the Black Sea* (Atlantic Council, 15 December 2023) https://www.atlanticcouncil.org/in-depth-research-reports/report/a-security-strategy-for-the-black-sea/, accessed 20 September 2025.

[11] Amy Ormrod, David Ormrod and Jill Slay, '*Cyber Offensive Operations in Hybrid Warfare: Observations from the Russo-Ukrainian conflict'* (2023) *Journal of Information Warfare,* Vol. *22* (1), 76–87, 76.

[12] North Atlantic Treaty Organization, *Hybrid threats and hybrid warfare* (North Atlantic Treaty Organization, October 2024) https://www.North Atlantic Treaty Organization.int/North Atlantic Treaty

consistency of international law and security frameworks, because cyberattacks can cause havoc without leaving visible marks.[13]

B. Notable Cyber and Electronic Incidents

Recent years have seen illustrative examples of cyber aggression in the Black Sea–Eastern Mediterranean region. Notably, Russia has employed electronic warfare to protect its positions in the Eastern Med. Russian forces have repeatedly jammed GPS signals over Syria, Lebanon, Cyprus and surrounding waters, severely disrupting commercial navigation.[14] This Global Navigation Satellite System(s) interference in the Black Sea–Eastern Mediterranean region has threatened the safety of commercial vessels by severely disrupting their electronic navigation systems, and even degraded ships' maritime radars.[15] Similarly, a surge of false positioning signals and spoofing attacks in the Eastern Mediterranean and Persian Gulf was reported.[16] Marine authorities confirmed severe GPS disruptions affecting ships in those waters; one incident off Haifa appeared to involve a deliberate circular pattern of spoofed signals. These attacks correspond to rising regional tensions (e.g. Iran–Israel hostilities) and highlight how satellite navigation can be a target.[17]

Beyond jamming, there have been high-impact cyber intrusions on critical infrastructure. In 2015–16, coordinated cyberattacks on Ukraine's electrical grid (attributed to Russian state hackers) caused mass blackouts. According to a U.S. cybersecurity team's report, remote intruders disrupted three regional power distribution companies, impacting approximately 225,000 customers in Ukraine. The attackers used legitimate credentials and malware to open breakers and disable systems.

Organization_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf, accessed 20 September 2025.

[13] FP Analytics, *Digital Front Lines* (FP Analytics, 2023) https://digitalfrontlines.io/, accessed 20 September 2025.

[14] C4ADS, *Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria* (C4ADS 2019) 3 https://c4ads.org/wp-content/uploads/2022/05/AbovEuropean UnionsOnlyStars-Report.pdf, accessed 20 September 2025.

[15] Andrej Androjna, Tanja Brcko, Ivica Pavic and Harm Greidanus, 'Assessing Cyber Challenges of Maritime Navigation' (2020) *J Mar Sci Eng,* Vol. *8 (10),* 776.

[16] F Jiguet *et al*, 'Global Navigation Satellite System(s) spoofing in conflict zones disrupts wildlife tracking and hampers research and conservation efforts' (2025) *Nat Commun* 16, 1199.

[17] Cheng Lu, Zukun Lu, Zhe Liu, Long Huang and Feiqiang Chen, 'Overview of satellite nav spoofing and anti-spoofing techniques' (2024) *Frontiers in Physics 12* 1428544,.

This incident demonstrated that cyber weapons can have physical effects on utilities.[18] More recently, adversaries have used distributed-denial-of-service and defacement attacks as political tools. Pro-Russian hacktivist groups (e.g. KillNet, NoName, the so-called IT Army of Russia) have launched coordinated Distributed Denial of Service campaigns and website defacements against Ukrainian and allied targets.[19] Conversely, Ukrainian-affiliated IT Army volunteers have struck back at Russian government and military sites in a hybrid form of retaliation.[20]

Information operations are also a major factor. Russian and allied actors frequently carry out disinformation and influence campaigns aimed at countries in the Black Sea–Eastern Mediterranean region.[21] U.S. officials warn that these advanced disinformation efforts, spearheaded by Russia, threaten to undermine progress in the Black Sea area.[22] For example, social media stories have been used to sway public opinion about the conflicts in Syria or migrant crises in the Balkans.[23] The cyber dimension of security in this region is already active and diverse: electronic jamming, network intrusions, hacktivism and disinformation all combine as ambiguous tactics. However, legal experts note that disinformation rarely meets the threshold of a use of force or armed conflict unless it causes physical consequences, thus occupying a regulatory gap.[24]

---

[18] Doney Abraham, Siv Hilde Houmb and Laszlo Erdodi, 'Cyber-Attacks on Energy Infrastructure—A Literature Overview and Perspectives on the Current Situation' (2025) *Applied Sciences 15* 9233, 9233.

[19] US Department of Health & Human Services, Health Sector Cybersecurity Coordination Center (HC3), '*Pro-Russian Hacktivist Group "KillNet" Threat to HPH Sector', HC3*, 30 January 2023, 1 https://www.hhs.gov/sites/default/files/russian-threat-actors-targeting-the-hph-sector-tlpclear.pdf, accessed 20 September 2025.

[20] Anna Lysenko and Seva Gunitsky, 'The invisible front: Ukraine's IT army and the evolution of cyber resistance' (2025) *41 Post-Soviet Affairs* 263–288, 263.

[21] Natalie Sabanadze and Galip Dalay, '*Understanding Russia's Black Sea strategy: How to strengthen European Unionrope and North Atlantic Treaty Organization's approach to the region',* Chatham House Research Paper, 28 July 2025, 16 https://www.chathamhouse.org/2025/07/understanding-russias-black-sea-strategy, accessed 20 September 2025.

[22] Centre for Strategic and International Studies (CSIS), 'Navigating Security Challenges in the Black Sea Region', *Transcript, CSIS*, 11 January 2024, 1 https://www.csis.org/analysis/navigating-security-challenges-black-sea-region, accessed 20 September 2025.

[23] Anna Triandafyllidou and Stein Monteiro, 'Migration narratives on social media: Digital racism and subversive migrant subjectivities' (2024) *First Monday,* Vol. 29 (8), 13 .

[24] Benjamin Jensen, Brandon Valeriano and Sam Whitt, 'How cyber operations can reduce escalation pressures: Evidence from an experimental wargame study' (2024) 61 *Journal of Peace Research* 119, 1.

C. Key Actors and Vulnerabilities

The main state actors in this area are the coastal countries and other regional powers. These include Russia, Turkey, Greece, Ukraine, Romania, Bulgaria, Cyprus, Israel, Iran and others. Many of these countries (Turkey, Greece, Romania, Bulgaria and soon Ukraine) are members of North Atlantic Treaty Organization or the European Union and follow Western cyber-defense approaches.[25] Russia remains the most aggressive cyber adversary in the Black Sea region, employing both official forces and proxy groups.[26] Research highlights that Russia's cyber network is extensive, complex and often opaque. It mixes federal security services with government-tolerated hackers, cybercriminal rings and even private military companies.[27] Russian patriotic hackers and state security agencies, cybercriminals and private military companies blend together to create the Russian cyber web.[28] This multidirectional ecosystem – ranging from Russia's Federal Security Service (Federal'naya sluzhba bezopasnosti)/Russia's Main Intelligence Directorate (Glavnoye razvedyvatel'noye upravlenie) operations to volunteer hacktivists (KillNet, Advanced Persistent Threat groups, etc.) – makes attribution difficult and increases Russia's cyber reach.[29] Turkey also engages actively: its armed forces and intelligence services conduct cyber reconnaissance and defensive operations in the Eastern Med (especially around contested waters and energy

[25] Yavor Todorov, 'Navigating Uncharted Waters: Tackling Maritime Cybersecurity Challenges in the Black Sea Region' (2024) *Information & Security: An International Journal,* Vol. *55* (2), 113–132, 113.
[26] Sabanadze and Dalay (n 20).
[27] Justin Sherman, '*Untangling the Russian Web: Spies, Proxies, and Spectrums of Russian Cyber Behavior', Atlantic Council*, 19 September 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web/, accessed 20 September 2025.
[28] Justin Sherman, 'Unpacking Russia's cyber nesting doll', *Atlantic Council*, 20 May 2025, https://www.atlanticcouncil.org/content-series/russia-tomorrow/unpacking-russias-cyber-nesting-doll/, accessed 20 September 2025.
[29] Annegret Bendiek, Jakob Bund and Mika Kerttunen, 'The Attribution Dividend: Protecting Critical Infrastructure from Cyber Attacks', SWP Comment 2024/C 46, 9 October 2024, https://www.swp-berlin.org/10.18449/2024C46/, accessed 20 September 2025.

exploration).[30] Iran, Israel and Gulf states have also sharpened their cyber capabilities as tensions rise.[31]

Non-state actors and proxies magnify these threats. In Russia's orbit, hacktivist collectives (KillNet, NoName, Anonymous Sudan proxies, etc.) freely target rival states.[32] Conversely, nationalist hacktivists in Ukraine, Greece, and elsewhere have arisen. Criminal organizations also play a role; for example, cybercriminal gangs may cooperate with, or be coerced by, state agencies.[33] Commercial hackers-for-hire and so-called patriotic 'hackers' can serve as covert force multipliers. Both sides increasingly weaponize dual-use technology: maritime GPS, telecom satellites, undersea cables and civilian internet infrastructure can become vulnerable nodes.[34] Critical sectors at risk include energy (electric grids, pipelines), transportation (ports, logistics networks, shipping), telecommunications (Internet Service Providers, cell networks, satellite comms), and finance. For example, a denial-of-service attack or malware incident targeting a port authority or maritime traffic control system could bring commerce to a standstill.[35] Civilian networks often carry both military and public communications, which means that dual-use cyber infrastructure can become a point of conflict. Under international humanitarian law, such infrastructure is a military target only if it meets

[30] International Institute for Strategic Studies, 'Turkiye' in *Cyber Capabilities and National Power Vol. 2*, Research Paper, International Institute for Strategic Studies, September 2023, 141 https://www.iiss.org/globalassets/media-library---content---migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_12-turkiye.pdf, accessed 20 September 2025.

[31] Ibid.

[32] Julia Dickson and Emily Harding, 'How a Cyber Alliance Took Down Russian Cybercrime"', C*enter for Strategic and International Studies*, 28 July 2025, https://www.csis.org/analysis/how-cyber-alliance-took-down-russian-cybercrime, accessed 20 September 2025.

[33] Janine Schmoldt, 'Cyber proxies: covert state–non-state interactions in cyberwarfare', in Tim Stevens and Joe Devanny (eds), *Research Handbook on Cyberwarfare* (Cheltenham: Edward Elgar Publishing, 2024) 131–47, 132.

[34] A Ertan, K Floyd, P Pernik and T Stevens (eds), *Cyber Threats and North Atlantic Treaty Organization 2030: Horizon Scanning and Analysis* (North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization) Publications, 2020), https://Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization).org/uploads/2020/12/Cyber-Threats-and-North Atlantic Treaty Organization-2030_Horizon-Scanning-and-Analysis.pdf, accessed 20 September 2025.

[35] M. V. Clavijo Mesa, C. E. Patino-Rodriguez and F. J. Guevara Carazas, 'Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains' (2024) *Information 15,* 710.

strict criteria.[36] Overall, the Black Sea–Eastern Mediterranean region's strategic importance – from oil and gas routes to key ports and information points.[37]

3. International Legal Framework for Cyber Operations

A. UN Charter: Use of Force and Self-Defense

International law's starting point is the UN Charter. Article 2(4) prohibits the threat or use of force by states, a foundational rule presumed to apply across domains.[38] In 2013 a UN Group of Governmental Experts explicitly affirmed that international law, and in particular the Charter of the United Nations, is applicable to the use of information and communications technologies.[39] Likewise, North Atlantic Treaty Organization and European Union statements now affirm that cyber operations are governed by the same jus ad bellum norms as conventional force.[40] Notably, North Atlantic Treaty Organization's 2014 Wales Summit Declaration recognized that the use of cyber capabilities could, if used in a manner that meets the threshold of an 'armed attack' under Article 51 of the UN Charter, could lead to the invocation of Article 5 of the North Atlantic Treaty (collective defense).[41] This means a cyber-attack whose effects are comparable to those of a conventional armed attack could trigger the Charter's self-defense rule.[42] Indeed, North Atlantic Treaty Organization officials have emphasized that cyber defense is a core mission and that a cyber attack could be

[36] International Committee of the Red Cross, '*International Humanitarian Law and Cyber Operations during Armed conflicts',* International Committee of the Red Cross position paper, November 2019, https://www.International Committee of the Red Cross.org/sites/default/files/document/file_list/International Committee of the Red Cross_International Humanitarian Law-and-cyber-operations-during-armed-conflicts.pdf, accessed 20 September 2025.

[37] Atlantic Council Task Force on Black Sea Security (n 9).

[38] Michael N Schmitt, 'Cyberspace and the Jus ad Bellum: the State of Play' (2024) *International Law Studies 103,* 195.

[39] Harriet Moynihan, '*The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention',* Chatham House Research Paper, 29 November 2019, https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf, accessed 20 September 2025.

[40] Schmitt and Pakkam (n 37).

[41] Joe Burton and Tim Stevens, '4 System, Alliance, Domain: A Three-Frame Analysis of North Atlantic Treaty Organization's Contribution to Cyber Stability' in Robert Chesney (ed), *Cyberspace and Instability* (Edinburgh: Edinburgh University Press 2022), 129–52, 133.

[42] Schmitt and Pakkam (n 37).

grounds for invoking Article 5, provided the cyber assault causes sufficiently grave damage.[43]

At the same time, there are uncertainties in the law. The concept of "use of force" in Article 2(4) of the UN Charter was originally drafted with guns and bombs in mind, so applying it to digital attacks is debated.[44] Some scholars suggest an effects-based test, meaning only cyber operations that cause actual physical harm or destruction should count as the use of force.[45] Others argue that crippling a country's critical infrastructure (like its power grid, dams or nuclear plants) could itself be considered an armed attack if it causes physical damage.[46] On this point, the Tallinn Manual 2.0 (a well-known but nonbinding study) and many experts say that the scale of consequences matters. Cyber actions that result in death, injury or substantial property damage likely qualify as use of force and even as an armed attack under Article 51, while mere espionage or data theft would not.[47] The U.S. and North Atlantic Treaty Organization have similarly indicated that a cyber attack causing casualties or major destruction could be treated like an armed attack that justifies self-defense. However, in ambiguous cases – for example, an espionage intrusion or a ransomware hack – the threshold for force is usually not reached.[48]

If a cyber operation does amount to an armed attack, the right of self-defense under Article 51 of the UN Charter is triggered.[49] That means victim states may lawfully defend themselves – individually or collectively – against the attacker. Western countries maintain that Article 51 applies to cyber attacks in no other case than this: i.e.

[43] North Atlantic Treaty Organization, 'Cyber defence', https://www.North Atlantic Treaty Organization.int/cps/en/North Atlantic Treaty Organizationhq/topics_78170.htm, accessed 20 September 2025.
[44] Schmitt and Pakkam (n 37).
[45] Thomas Eaton, 'Self-Defense to Cyber Force: Combatting the Notion of "Scale And Effect"' (2021) *36 American University International Law Review,* 697.
[46] Samuli Haataja, 'Cyber operations against critical infrastructure under norms of responsible state behaviour and international law' (2023) *International Journal of Law and Information Technology,* Vol. 30 (4), 423.
[47] Schmitt and Pakkam (n 37).
[48] F. Oorsprong, P. Ducheine and P. Pijpers, 'Cyber-attacks and the right of self-defense: a case study of the Netherlands' (2023) *6 Policy Design and Practice,* 217.
[49] International Committee of the Red Cross, 'International humanitarian law and cyber operations during armed conflicts' (2020) *102 International Review of the Red Cross,* 481.

when the attack reaches the armed-attack level.[50] The North Atlantic Treaty Organization policy line is consistent: Article 5 can be invoked if and when a cyber attack causes extensive destruction, injury or death akin to a kinetic assault.[51] North Atlantic Treaty Organization deliberately keeps thresholds ambiguous: as its officials note, setting clear numbers could reveal their red lines and weaken deterrence. In contrast, Russia has recently questioned whether any consensus exists on classifying malicious cyber operations as armed attacks under Article 51.[52] In UN working groups, Russia and some others have even argued that International Humanitarian Law does not automatically apply in cyberspace.[53] This dispute underscores the tension: Western allies favor extending traditional self-defense law to cover cyber aggression, while Russia suggests new rules might be needed.[54]

B. International Humanitarian Law

When cyber operations occur in an armed conflict, the law of armed conflict (International Humanitarian Law) governs their conduct.[55] The core International Humanitarian Law principles—distinction (targeting only military objectives), proportionality (weighing military advantage against collateral damage), and precaution (active measures to spare civilians)—are generally understood to apply in cyberspace, as affirmed by the 2015 (UN) Group of Governmental Experts report.[56] The International Committee of the Red Cross emphasizes that even cyber attacks must at all times distinguish between military and civilian targets.[57] Thus, cyber operations may only be directed against combatants or military objectives; attacks on civilians or

[50] Michael N Schmitt, 'Cyber Symposium – *The Evolution of Cyber Jus ad Bellum Thresholds*', *Lieber Institute for Law and Warfare*, 28 July 2022, https://lieber.westpoint.edu/evolution-cyber-jus-ad-bellum-thresholds/, accessed 20 September 2025.
[51] North Atlantic Treaty Organization (n 42).
[52] Kajander, *Unnecessary Repetition* (n 7).
[53] Ibid.
[54] Ibid.
[55] Michael N Schmitt, 'Wired warfare 3.0: Protecting the civilian population during cyber operations' (2019) 101 *International Review of the Red Cross,* 333–355, 334.
[56] International Committee of the Red Cross (n 48).
[57] L. Gisel, T Rodenhäuser and K. Dörmann, 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts' (2020) 102 *International Review of the Red Cross,* 287–334, 289.

purely civilian objects are prohibited.[58] This is challenging in practice because Information and Communications Technology infrastructure is often dual-use. For example, a satellite or undersea cable may carry both civilian data and military communications. International Humanitarian Law treats such an object as a military objective only if (a) its use makes an effective contribution to military action, and (b) its damage offers a definite military advantage. Otherwise it remains protected.[59] In concrete terms, hacking a power plant to create tactical advantage must still not kill civilians or destroy humanitarian services, and indiscriminate or unfocused cyber attacks are forbidden.[60]

Proportionality imposes a similar constraint. Even if a target is legitimate, an attack is unlawful if the expected civilian harm is excessive relative to the anticipated military gain.[61] The International Committee of the Red Cross notes that in the interconnected Information and Communications Technology environment, some incidental harm to civilian networks is almost inevitable, but this does not suspend the proportionality rule.[62] For example, if an aggressor state launches malware that disables an enemy's air defense radar (a military objective), but it also cripples civilian air-traffic control and causes major collateral damage, that might be disproportionate. Likewise, an attack that floods a city's electric grid to hamper military rail transport (arguably a dual-use target) would likely exceed proportionality bounds due to civilian suffering.[63] Cyber actors must also take precautions to minimize harm (Article 57 Additional Protocol I (to the 1949 Geneva Conventions)), such as using precision malware or time delays.[64] The foundational International Humanitarian Law rules limiting civilian harm carry over to cyber warfare, though their application can be complex when effects are non-physical or systemic.[65]

---

[58] Schmitt (n 54).
[59] Sophie Ryan, 'Submarine Communication Cables and Belligerent Rights in Armed conflict' (2024) 38 *Ocean Yearbook,* 459, 459–503, 460.
[60] International Committee of the Red Cross (n 35).
[61] Maxime Nijs, 'Humanizing siege warfare: Applying the principle of proportionality to sieges' (2020) *International Review of the Red Cross, Vol.* 102 (914), 683–704.
[62] International Committee of the Red Cross (n 35).
[63] Schmitt (n 54).
[64] Ibid.
[65] International Committee of the Red Cross (n 48).

C. Other Normative Developments

Beyond treaty law, various expert bodies have reaffirmed that existing international law is fully applicable to cyber operations.[66] The Tallinn Manuals on cyber warfare (first edition 2013, second 2017) are not binding law, but they compile authoritative interpretations by international law scholars.[67] They proceed on the assumption that jus ad bellum and International Humanitarian Law apply to cyberspace, subject to technical nuance (e.g. use of force requires physical effects). Likewise, the 2013 (UN) Group of Governmental Experts report on cyber norms declared that the use of information and communications technologies must adhere to the Charter.[68] The 2021 (UN) Group of Governmental Experts and Open-Ended Working Group (at the UN) reports reaffirmed this stance: the 2021 (UN) Group of Governmental Experts explicitly stated that international law, in particular the UN Charter, in its entirety applies to the information and communications environment.[69] The (UN) Group of Governmental Experts also identified International Humanitarian Law principles like distinction and proportionality as established international legal principles for cyber warfare, though it noted further study was needed on implementation.[70] Most states on the UN stage have endorsed these conclusions, repeatedly affirming that cyberspace is not a lawless arena.[71]

In late 2024 the European Union Council went further by unanimously adopting a declaration that international law fully applies to cyberspace.[72] The declaration underscores that the UN framework of responsible state behavior – grounded in the Charter, human rights law and International Humanitarian Law – remains essential for

[66] Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc **A/76/135** (14 July 2021) para 2.
[67] Ori Pomson, 'Methodology of identifying customary international law applicable to cyber activities' (2023) *Leiden Journal of International Law* **36,** 1023–1047, 1026.
[68] Schmitt and Pakkam (n 37).
[69] UN Group of Governmental Experts Report on Responsible State Behaviour (n 65), para 69.
[70] Ibid, para 71(f).
[71] Michael N Schmitt, 'Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace' (2020) 3 *Texas National Security Review* 32.
[72] Council of the European Union, '*Declaration by the European Union and its Member States on a Common Understanding of the Application of International Law to Cyberspace'*, ST-15833-2024-INIT, 18 November 2024, https://data.consilium.European_Unionropa.European_Union/doc/document/ST-15833-2024-INIT/en/pdf, accessed 20 September 2025.

cyber stability.[73] In other words, European Union states officially embrace the mainstream view that no new jus ad bellum regime is needed: rather, they pledge to clarify and implement how existing obligations reach digital activities.[74] Similarly, leading countries (the U.S., North Atlantic Treaty Organization members) have published cyber doctrine positions affirming that all armed conflict rules and self-defense rights in the Charter are unaffected by the medium of cyber.[75] For instance, the U.S. National Cyber Strategy and legal policies emphasize that states must abide by UN law in cyberspace.[76] In contrast, Russia's governments have repeatedly proposed new binding cyber treaties and hinted that current law does not satisfactorily address cyber threats.[77] In UN forums, Russia has at times caused a stir by questioning the applicability of International Humanitarian Law to peacetime cyber operations and arguing there is no consensus on whether cyber attacks qualify as armed attacks.[78] These positions reflect a desire by some actors to negotiate new international rules on cybersecurity, whereas most Western states prefer to build consensus around existing legal norms.

Overall, the authoritative trend is clear: leading analyses (Tallinn Manuals, UN expert reports) assume that pre-existing legal principles govern state cyber conduct.[79] The prevailing interpretation among North Atlantic Treaty Organization/European Union members is that law's broad ban on force and requirement to protect civilians extends into cyberspace.[80] What remains unsettled is how to operationalize these principles – e.g. by developing clearer definitions of armed attack in cyber terms,

[73] Harriet Moynihan, 'The vital role of international law in the framework for responsible state behaviour in cyberspace' (2021) *Journal of Cyber Policy,* Vol. 6 (3), 394–410, 397.
[74] Schmitt and Pakkam (n 37).
[75] Schmitt (n 70).
[76] The White House, '*National Cybersecurity Strategy',* 1 March 2023,https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, accessed 21 September 2025.
[77] Lauren Zabierek, Christie Lawrence, Miles NEuropean Unionmann and Pavel Sharikov, '*US-Russian Contention in Cyberspace', Belfer Center for Science and International Affairs*, Harvard Kennedy School, June 2021, https://www.belfercenter.org/publication/us-russian-contention-cyberspace, accessed 20 September 2025.
[78] Kajander, *Unnecessary Repetition* (n 7).
[79] François Delerue, *Cyber Operations and International Law* (Cambridge: Cambridge University Press, 2020), 353–76, 364.
[80] Gisel, Rodenhauser and Dörmann (n 56).

setting standards for attribution, and agreeing on mutual cyber assistance.[81] But the message of the international community (UN, International Committee of the Red Cross, allied declarations) is that there is no need to reinvent law a priori; rather, states should adapt the current framework to the unique features of cyber operations.[82]

D. Regional Alliances and Collective Defense

Regional security organizations have explicitly extended collective defense concepts to cover cyber threats. North Atlantic Treaty Organization has been at the forefront: already in 2014 it declared that cyber defense is part of its core task of collective defense, meaning that a cyber attack could, in principle, trigger Article 5.[83] At the Wales Summit, Allies acknowledged that the scope of Article 5 could encompass cyber incidents depending on effects, and they later reaffirmed cyber as a distinct operational domain (2016 Warsaw Summit).[84] The Brussels Communiqué (2021) reiterated that a cyber aggression could invoke Article 5, but that decisions must be made case-by-case.[85] This means North Atlantic Treaty Organization will consider a cyberattack on a member state just as it would any attack: it will assist the Party or Parties so attacked such action as it deems necessary under Article 5.[86] The only difference is one of ambiguity: Allied leaders purposely avoid publicizing the threshold for cyber trigger, thereby deterring adversaries by leaving them uncertain. North Atlantic Treaty Organization's position – blurry but consistent – is that effects comparable to 2007 Estonia or 9/11 could justify collective response, but no fixed line is given.[87]

[81] Finlay and Payne (n 8).
[82] International Committee of the Red Cross (n 35).
[83] North Atlantic Treaty Organization (n 42).
[84] Sarah Wiedemar, '*North Atlantic Treaty Organization and Article 5 in Cyberspace', CSS Analyses in Security Policy* No 323, Center for Security Studies, ETH Zürich, May 2023, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse324-EN.pdf, accessed 20 September 2025.
[85] Ibid.
[86] Ibid.
[87] Michaela Prucková, 'Cyber attacks and Article 5 – a note on a blurry but consistent position of North Atlantic Treaty Organization', *North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence*, 2021 https://Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization).org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-North Atlantic Treaty Organization/, accessed 20 September 2025.

The European Union, which has its own mutual defense clause (Article 42(7) Treaty on European Union), likewise extends legal protections to cyberspace.[88] European Union Member States have adopted a common understanding affirming that the UN framework (Charter, International Humanitarian Law, etc.) fully applies in cyberspace.[89] The European Union cyber diplomacy vision links hard defense (e.g. cybercrime law enforcement, Computer Emergency Response Team cooperation) with soft-power norms building.[90] The European Union has also emphasized cooperative measures – joint cyber exercises, information sharing, and capacity building – to buttress Black Sea–Eastern Mediterranean (region) stability.[91]

At the national level, Black Sea–Eastern Mediterranean (region) countries generally align with these alliance policies. North Atlantic Treaty Organization members like Turkey, Romania, Bulgaria and Greece incorporate the UN Charter's principles into their cyber strategies (often citing North Atlantic Treaty Organization doctrine and European Union law).[92] For instance, Turkey's 2016 Cybersecurity Strategy calls on all actors (individuals and the state) to fulfil all legal responsibilities in providing cyber security.[93] Ukraine, even before full European Union/North Atlantic Treaty Organization accession, regards cyber attacks from Russia as acts of war

[88] Aistė Mickonytė, 'Obligation to Mutual Assistance Under Article 42(7) Treaty on European Union: The Conundrum of Intentional Ambiguity' (2024) *ICL Journal, Vol. 18,* 311–338, 315.

[89] Council of the European Union, *Declaration on a Common Understanding of International Law in Cyberspace*, ST 15833/24, 18 November 2024, https://data.consilium.European Unionropa.European Union/doc/document/ST-15833-2024-INIT/en/pdf, accessed 20 September 2025.

[90] T. Lațici, '*Understanding the European Union's approach to cyber diplomacy and cyber defence'*, European Unionropean Parliamentary Research Service, Briefing PE 651.937, May 2020, https://www.European Unionroparl.European Unionropa.European Union/RegData/etudes/BRIE/2020/651937/EPRS_BRI%282020%29651937_EN.pdf, accessed 20 September 2025.

[91] European Unionropean Commission and High Representative of the Union for Foreign Affairs and Security Policy, *The European Union's strategic approach to the Black Sea region*, Joint Communication JOIN(2025) 135 final, Brussels, 28 May 2025, https://enlargement.ec.European Unionropa.European Union/document/download/170d9b3a-d45f-4169-80fa-9adb753c0921_en?filename=European Union+Strategic+Approach+Black+Sea+Strategy.pdf.

[92] Emre Halisdemir, '*National Cybersecurity Organisation: TURKEY', North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence*, Tallinn 2021, https://Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization).org/uploads/2021/08/TUR_country_report_final_clean_ver_2408.pdf, accessed 20 September 2025.

[93] Nezir Akyeşilmen, 'Türkiye in the Global Cybersecurity Arena: Strategies in Theory and Practice' (2022) *Insight Turkey, Vol. 2*4 (3), 109, 111.

requiring military-grade responses.[94] The bloc of Western-aligned states in the region stresses that international law's use-of-force and collective defense rules apply in cyberspace. Russia, on the other hand, while still formally acknowledging some charter norms, continues to push for a treaty that it believes would give it more leverage.[95] This split in rhetoric reflects the broader question: whether to work within the existing legal order (with improvements) or to renegotiate it. For Black Sea–Eastern Mediterranean (region) security, most stakeholders have so far opted for the former path.

4. Gaps and Challenges in the Current Legal Regime

A. Absence of a dedicated cyber treaty

Cyberspace currently has no analogue to the nuclear or chemical arms-control regimes, leaving a significant legal lacuna.[96] States rely on general UN Charter prohibitions against force and existing humanitarian law, but there is no bespoke treaty on cyber-weapons or cyberwar.[97] Attempts to create one have floundered on technical and political grounds. A treaty demands that states quantify or monitor capabilities (easy with nukes or tons of gas, impossible with virtual weapons), agree on the effects of technology (rapid, unpredictable innovation in IT), and verify compliance (cyber tools are often dual-use and covert).[98] The cyber domain's intangibility and speed undermine conventional arms-control approaches. Critics therefore warn that any treaty could be obsolete by the time it is adopted.[99]

Nonetheless, proposals for a cyber-specific accord have been floated. One approach is a multilateral information security or cyber arms-control treaty.[100] Russia

[94] Decree of the President of Ukraine No 447/2021, 26 August 2021, *On the Cybersecurity Strategy of Ukraine,* National Security and Defense Council of Ukraine.https://www.rnbo.gov.ua/en/Diialnist/4976.html, accessed 20 September 2025.
[95] Kajander, *Unnecessary Repetition* (n 7).
[96] T Reinhold, H Pleil and C REuropean Unionter, 'Challenges for Cyber Arms Control: A Qualitative Expert Interview Study' (2023) 16 *Zeitschrift für Außen- und Sicherheitspolitik* 289, 293.
[97] Gisel, Rodenhauser and Dörmann (n 56).
[98] Przemysław Roguski, '*An Inspection Regime for Cyber Weapons: A Challenge Too Far?'* (2021) 115 *American Journal of International Law Unbound,* 111–115, 114.
[99] Reinhold, Pleil and REuropean Unionter (n 95).
[100] Ibid.

(supported by China and others) has repeatedly advocated negotiating a binding cybersecurity convention – arguing that existing law needs clarification and supplementation.[101] In 2018–20, Russian drafts in the UN sought an international legally binding agreement for information security. Other ideas include confidence-building measures and voluntary codes of conduct as interim steps.[102] For instance, the European Union is pursuing a UN Programme of Action on responsible state behavior in cyberspace, aiming to strengthen norms through dialogue rather than a new treaty.[103] These mixed proposals – from hard law to soft law – reflect the debate: some experts urge a traditional arms-control framework for cyberspace, while others stress flexible, behavioral regulations to address the unique challenges.[104]

B. Attribution and enforcement difficulties

A core practical gap in cyber law is attribution. Unlike a missile launch, a cyberattack can be routed through third-party servers or disguised via malware, making it extremely hard to trace the culprit.[105] Identifying the state or group behind an intrusion is sometimes difficult and often requires extensive technical intelligence. Because attackers can hide behind proxy networks, states rarely have incontrovertible proof.[106] Even when evidence is strong, the lack of a global enforcement mechanism means responses are piecemeal. victims typically resort to ad hoc measures: private incident response teams, unilateral indictments of hackers, or targeted sanctions. There

[101] Arun Sukumar and Arindrajit Basu, 'Back to the territorial state: China and Russia's use of UN cybercrime negotiations to challenge the liberal cyber order' (2024) *Journal of Cyber Policy,* Vol. *9* (2), 256, 259.

[102] Kajander, *Unnecessary Repetition* (n 7).

[103] Council of the European Union, 'Cyberspace: Council approves declaration on a common understanding of application of international law to cyberspace', Press release, 18 November 2024, https://www.consilium.European Unionropa.European Union/en/press/press-releases/2024/11/18/cyberspace-council-approves-declaration-to-promote-common-understanding-of-application-of-international-law/, accessed 20 September 2025.

[104] Reinhold, Pleil and REuropean Unionter (n 95).

[105] William C Banks, 'The Bumpy Road to a Meaningful International Law of Cyber Attribution' (2019) 113 *American Journal of International Law* (AJIL Unbound), 191–196, 195 https://doi.org/10.1017/aju.2019.32.

[106] Florian J. Egloff, 'Public attribution of cyber intrusions' (2020) *Journal of Cybersecurity,* Vol. 6 (1).

is no international cyber-Gendarmerie or agreed process to investigate transnational hacks.[107]

The consequence is a patchwork of responses. Some like-minded countries (notably the Five Eyes) publicly attribute major incidents and impose coordinated sanctions, but these actions are political, not judicial, and do not bind all states. It is usually difficult for the victim to hold the wrongdoing State accountable for cyber-operations.[108] The result is that many cyber intrusions go unpunished. Cyber criminals and state-aligned hackers often operate with relative impunity, knowing that even if detected they may face only reprisal by a few states.[109] This attribution hurdle thus undermines any consistent enforcement of international law.

C. State-centric law vs. non-state actors

Traditional international law is built around state actors, but cyberspace is dominated by non-state entities – hacktivists, criminal gangs, and multinational tech companies.[110] This dissonance renders the law incoherent with the dominance of non-state actors in cyberspace.[111] States negotiate treaties and resolve disputes with each other, but a cyberattack can originate from an independent hacker group or even a private corporation.[112] These actors are not straightforwardly controlled by governments, so the usual state-to-state law framework lacks teeth to rein them in.

Moreover, non-state actors often fill gaps left by governments. For example, large tech firms have become de facto norm-setters and responders: they can negotiate cybersecurity standards, patch vulnerabilities, and even attribute attacks (e.g. naming

[107] Dennis Broeders, 'Private active cyber defense and (international) cyber security—pushing the line?' (2021) *Journal of Cybersecurity,* Vol. *7* (1).
[108] Delerue (n 78).
[109] Egloff (n 106).
[110] A Sukumar, D Broeders and M Kello, 'The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy' (2024) *Contemporary Security Policy,* Vol 45 (1), 7, 16.
[111] Katagiri Nori, 'Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks' (2021) *Journal of Cybersecurity,* Vol. 7 (1).
[112] Finlay and Payne (n 8).

which malware was used).[113] In this fragmented landscape, powerful private cybersecurity companies or norm entrepreneurs can shape outcomes in ways the formal international legal system cannot.[114] States themselves sometimes act indirectly via proxies or volunteer hacker organizations. The state-centric design of international law struggles to capture these realities; the law provides no direct sanction against an independent hacker collective, and any state responsibility hinges on proving that the state itself directed or controlled the attack.[115]

D. Norm erosion and compliance

These gaps together contribute to an ongoing erosion of legal norms. Because cyber attackers rarely face clear consequences, a culture of noncompliance has emerged.[116] The toothlessness of the legal framework makes noncompliance, practical and cyber operations pain-free for perpetrators.[117] States routinely ignore or reinterpret rules. High-profile cases – from Russia's cyber-interference in Ukraine to persistent intellectual-property theft by other powers – test the limits of the law with little accountability.[118] Over time this undermines confidence in international institutions. When major powers flout cyber norms without censure, smaller states lose faith that the legal rules of the road have any bite.[119] The resultant atmosphere of impunity and distrust erodes the very notion of a stable, law-based digital order.

[113] S Romanosky and B Boudreaux, 'Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government' (2020) 34 *International Journal of Intelligence and CounterIntelligence* 463–493, 468.

[114] Robert Gorwa and Anton Peez, 'Big Tech Hits the Diplomatic Circuit: Norm entrepreneurship, Policy Advocacy, and Microsoft's Cybersecurity Tech Accord' in Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace: Behaviour, Power and Diplomacy* (Lanham, MD: Rowman & Littlefield, 2020) 283–304, 291 https://osf.io/g56c9/ accessed 20 September 2025.

[115] Justin Key Canfil, 'The Illogic of Plausible Deniability: Why Proxy conflict in Cyberspace May No Longer Pay' (2022) *Journal of Cybersecurity,* Vol. 8 (1).

[116] N Katagiri, 'Why international law and norms do little in preventing non-state cyber attacks' (2021) *Journal of Cybersecurity,* Vol. 7 (1).

[117] Nori Katagiri, 'Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks' (2021) *Journal of Cybersecurity,* Vol. 7 (1).

[118] Kristen E Eichensehr, 'Ukraine, Cyberattacks, and the Lessons for International Law' (2022) 116 *American Journal of International Law* 145, 145–49, 148.

[119] Kello (n 6).

5. Divergent State Approaches to Cyber Norms

A. Western/North Atlantic Treaty Organization/European Union perspective

The United States, European Union members and other North Atlantic Treaty Organization allies generally maintain that existing international law – especially the UN Charter – already governs cyberconflict.[120] In the view of Western governments, Article 2(4)'s prohibition on the use of force applies fully to cyberoperations, and Article 51's self-defense right can be invoked if a cyberattack rises to the level of an armed attack.[121] Western statements routinely reaffirm this stance. For example, North Atlantic Treaty Organization leaders declared in 2014 that international law, including international humanitarian law and the UN Charter, applies in cyberspace.[122] They emphasized that cyber defense is a core part of collective defense, even if decisions to invoke Article 5 (collective self-defense) would be made on a case-by-case basis.[123] Similarly, the UN Group of Governmental Experts in 2013 (including the U.S. and European Union states) stated that the Charter of the United Nations is applicable to state Information and Communications Technology operations.[124]

The European Union has echoed this interpretation. In November 2024, the European Union and its Member States approved a common declaration reaffirming that international law particularly the UN Charter fully applies to cyberspace.[125] This declaration explicitly rejects the idea that cyberspace is a legal vacuum: it asserts that cyberspace is governed by the UN framework of responsible state behaviour, emphasizing that states must obey long-standing rules even in digital operations.[126] In practice, Western allies tend to focus on clarifying how existing law applies (for instance, what level of cyber-kinetic effect qualifies as a use of force) rather than

[120] Security Council, '*Record of the open debate on Maintenance of international peace and security: cybersecurity'*, UN Doc S/2021/621, 1 July 2021, https://docs.un.org/en/S/2021/621, accessed 20 September 2025.
[121] Schmitt and Pakkam (n 37).
[122] Kubo Mačák, 'Unblurring the lines: military cyber operations and international law' (2021) 6 *Journal of Cyber Policy* 411, 413.
[123] Prucková (n 86).
[124] UN Group of Governmental Experts Report on Responsible State Behaviour (n 65).
[125] Council of the European Union (n 71).
[126] Moynihan (n 72).

writing new treaties.[127] Toward that end, North Atlantic Treaty Organization has commissioned restatements like the Tallinn Manual, and the European Union is supporting UN-based confidence and capacity building through the ongoing Programme of Action (PoA) process.[128] Western policy privileges an incremental approach: maintain the current UN framework, while refining definitions of armed attack in cyber context, rather than fundamentally rewriting the rules.[129]

B. Russia and allies' stance

By contrast, Russia (backed by some partner states) contends that the current legal framework is inadequate to address cyber threats. Since the early 2010s, Moscow has argued repeatedly for a new binding treaty on state conduct in cyberspace. In its UN statements, Russia frames this not as a rejection of international law, but as a necessary clarification and extension of it.[130] Russia presented a cyber treaty as a critical means to clarify how existing international law applies and to introduce additional norms.[131] Russia's proposals often highlight so-called gaps – areas where international law has not explicitly anticipated digital tools. For instance, Russia and China have pushed UN resolutions to elaborate new legal rules on sovereignty in cyberspace, seeking limits on illegal cross-border hacking and intelligence gathering.[132]

Russia's 2018–2020 initiatives vividly illustrate this approach. After disagreements in the UN Group of Experts, Russia successfully led the creation of an Open-Ended Working Group (at the UN) to negotiate a more inclusive treaty process. In UN forums, Russian delegates have repeatedly called for a legally binding instrument on information security. In their view, such a treaty would explicitly codify the interplay of sovereignty, non-intervention, and use of force in the cyber domain.[133] Western and

[127] Haataja (n 45).
[128] Robert Collett and Nayia Barmpaliou, '*International cyber capacity building: global trends and scenarios', European Union Institute for Security Studies*, September 2021..
[129] Schmitt and Pakkam (n 37).
[130] Sukumar and Basu (n 100).
[131] Elaine Korzak, '*Russia's Cyber Policy Efforts in the United Nations', North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence,* Tallinn Paper No 11, 2021, https://Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization).org/uploads/2021/06/Elaine_Korzak_Russia_UN.docx.pdf, accessed 21 September 2025.
[132] Sukumar and Basu (n 100).
[133] Ibid.

North Atlantic Treaty Organization countries have generally opposed a new treaty in the First Committee, arguing instead for implementing voluntary norms. Russia counters that without a formal agreement, states will continue to flout rules and interpret them opportunistically. This divide reflects broader political splits: supporters of a treaty (Russia, China, some Global South countries) tend to emphasize state sovereignty and security, whereas most Western states warn that a rigid treaty could be used to justify censorship or constraints on the free internet.[134] Even though Russia now concedes international law's core validity, it insists a treaty is indispensable to fill current gaps and enhance cyber stability.[135]

6. Case Study – Cyber Intrusion on Critical Infrastructure

A. Scenario setup

Imagine a sudden, coordinated cyber-attack against critical infrastructure in the Black Sea–Eastern Mediterranean region. In this scenario, a malicious malware campaign (e.g. a modified industrial-control system virus) is launched against a nation's power grid and a major seaport's management systems. Within hours, the citylights in a capital go dark, hospitals lose backup power, and automated port cranes grind to a halt, halting grain exports. Emergency services struggle without communications. Computer forensics trace the operation to a sophisticated hacker unit using tools apparently aligned with a hostile state's military cyber-intelligence program, although attribution is delayed by layers of proxies. The scale of disruption is severe: it causes human harm (e.g. power failures endanger medical patients) and economic losses. Because this hypothetical attack is linked (directly or indirectly) to a state adversary and mimics the effects of conventional warfare, it raises the question: how would international law categorize it?

For context, real-world precedents underscore the stakes. In December 2015, Ukraine's power grid was similarly struck by malware, cutting electricity to hundreds of thousands. Analysts attributed that incident to a Russian unit called Sandworm. No

[134] Ibid.
[135] Korzak (n 130).

fatalities were reported, but the attack demonstrated how a cyber breach could paralyze civilian infrastructure.[136] In our scenario, we assume an even more disruptive campaign in the strategically sensitive Black Sea–Eastern Mediterranean (region) zone.

B. Legal characterization

Legally, a key question is whether this cyber-operation constitutes a use of force under UN Charter Article 2(4), and if so whether it rises to the level of an armed attack triggering the victim's Article 51 right of self-defense.[137] International law provides few bright-line rules for cyber cases, but several principles guide the analysis. First, any cyber act with force-like effects – physical damage, destruction, or casualties – potentially violates the force prohibition, even if carried out without guns or bombs.[138] For example, Tallinn Manual 2.0 (the international experts' guide) holds that a cyber operation causing real-world physical damage would qualify as a violation of sovereignty or non-intervention, and potentially as a use of force if intended to coerce or harm.[139]

States assess the effects and scale. Low-level intrusions (brief website defacements, data theft, minor service outages) are analogous to espionage or nuisance; they do not constitute a use of force in the Charter sense.[140] By contrast, an attack inflicting serious destruction – say, melting equipment or causing loss of life – would likely be deemed akin to a conventional attack.[141] In our scenario, because hospitals lost power and civilians faced danger, one could argue an armed attack occurred. The authoritative Tallinn Manual rules (though not legally binding) would support treating an extensive cyber blackout with life-threatening consequences as triggering self-defense.[142] Other factors include intent and context: if it is clear the assault was

[136] Congressional Research Service, '*Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience'*, CRS Report R48067, 17 May 2024, https://www.everycrsreport.com/files/2024-05-17_R48067_ec9b146372fac1c17e466dabba91199bfafbe564.html, accessed 21 September 2025.

[137] Schmitt (n 70).

[138] Haataja (n 45).

[139] Ibid.

[140] Schmitt and Pakkam (n 37).

[141] International Committee of the Red Cross (n 48).

[142] Ben Hines, 'Reinterpreting the Legality of Forcible Self-Defence in Response to Non-Kinetic Cyber Attacks' (2024) *Melbourne Journal of International Law, Vol.* 25 (1), 411-428, 414.

coordinated by a state actor with military objectives, this strengthens the armed-attack characterization.[143] Conversely, if damage were limited to data theft or temporary disruption without physical harms, some legal scholars might view it as unlawful interference short of armed aggression. The lack of casualties or purely economic impact, for example, has in past incidents kept them below the armed-attack threshold. Ultimately, the legal classification hinges on a holistic judgment: the level of impact (damage, human harm), the target's nature (critical civilian infrastructure), and the attribution.[144]

C. Policy response and implications

How would affected states respond? If the attack is judged an armed attack, the victim state (and its allies) could invoke collective self-defense under Article 51 of the UN Charter – including potentially North Atlantic Treaty Organization's Article 5.[145] North Atlantic Treaty Organization summits have affirmed that cyberattacks can count as Article 5 triggers depending on their severity.[146] In our scenario, if power outages were extensive and attributed to an adversary, the struck country might call an Article 4 consultation or even ask for collective action. North Atlantic Treaty Organization's 2016 Warsaw Summit declared cyberspace a new operational domain and reaffirmed that defense obligations apply to cyber operations.[147] Thus, serious Black Sea–Eastern Mediterranean (region) cyber aggression could, in theory, mobilize Alliance solidarity (possibly involving defensive cyber operations, sanctions, or even kinetic backup).

However, if decision-makers deem the effects below the armed-attack threshold, the incident may be treated as a criminal or law-enforcement matter. The victim might arrest (or indict) identifiable hackers, bolster cybersecurity patrols, and

[143] Eduardo Cavalcanti de Mello Filho, 'Armed Attacks against Merchant Vessels: "Looking behind the Flag" to Find the victim State' (2024) 29 *Journal of conflict & Security Law,* 281-309, 283.
[144] Eichensehr (n 117).
[145] François Delerue, 'The Threshold of Cyber Warfare: from Use of Cyber Force to Cyber Armed Attack', in *Cyber Operations and International Law* (Cambridge: Cambridge University Press, 2020), ch 6, 273–342, 275.
[146] North Atlantic Treaty Organization, *Vilnius Summit Communiqué*, Press Release (2023) 001, 11 July 2023, https://www.North Atlantic Treaty Organization.int/cps/en/North Atlantic Treaty Organizationhq/official_texts_217320.htm, accessed 21 September 2025.
[147] Wiedemar (n 83).

appeal to international institutions (e.g. UN condemnation) rather than go to war.[148] Historically, states often prefer cyber responses such as naming-and-shaming, intelligence sharing, and targeted sanctions when evidence is inconclusive. For instance, in response to past hacks, Western states have imposed sanctions on hostile actors instead of military retaliation.[149]

The ambiguity of cyber attribution thus critically shapes the choice of response. If evidence finally confirms clear state sponsorship, the victim state might feel justified in a military counter-strike or collective defense – but only if political and legal thresholds are met. Otherwise, states are more likely to pursue proportional countermeasures (such as offensive cyber operations in self-defense) or diplomatic/legal recourse.[150] Even after something like the 2015 Ukraine blackout, the response was cyber resilience building and international pressure, not open warfare.[151] In our hypothetical, leaders would weigh the costs of escalation against the need to uphold norms: a visible cyber assault on people's lives certainly tests the line between a law-enforcement issue and an act of war. The choice of pathway – collective defense under North Atlantic Treaty Organization, or policing the incident – would ultimately depend on allies' judgment of the attack's gravity and the confidence of attribution. This analysis contends that maintaining strategic ambiguity regarding cyber thresholds is detrimental to regional stability. States must instead adopt 'declaratory deterrence,' explicitly defining the critical infrastructure attacks that will trigger collective defense.[152]

7. Bridging the Gap: Legal adaptations

[148] Finlay and Payne (n 8).

[149] Martha Finnemore and Duncan B Hollis, 'Beyond Naming and Shaming: Accusations and International Law in Cybersecurity' (2020) 31 *European Unionropean Journal of International Law* 969, 976.

[150] W. C. Banks, 'The Bumpy Road to a Meaningful International Law of Cyber Attribution' (2019) 113 *AJIL Unbound* 191, 195.

[151] Eichensehr (n 117).

[152] F J Egloff and M Smeets, 'Publicly attributing cyber attacks: a framework' (2023) *Journal of Strategic Studies 46* 502–533, 514 https://doi.org/10.1080/01402390.2021.1895117

A. Clarifying Armed Attack in Cyberspace

Current law uses the Nicaragua scale and effects test (ICJ 1986) to identify an armed attack.[153] The paper proposes concretely defining digital analogues. For example, states could adopt objective thresholds akin to kinetic strikes: if a cyber operation inflicts physical destruction, casualties or major system failure, it counts as an armed attack. Several governments already suggest similar criteria. Germany's stance explicitly notes that indirect injury or death from a cyber-operation may count, and France regards considerable economic damage as a factor.[154] Likewise, widespread disruption of critical infrastructure (power grids, water systems, etc.) should be treated as the functional equivalent of a bombing run.[155] Conversely, low-level intrusions (even if politically sensitive) would remain below the threshold. In practice, a treaty or declaration might enumerate concrete indicators (e.g. fatalities, blackout >X hours, market losses >Y) to trigger Article 51 response.[156] Intent should also be weighed: operations deliberately designed to mimic the effects of conventional attacks should be treated identically, whereas cyber espionage or routine crime (the hacking of non-essential data for theft) would not.[157] By analogizing to physical armed attacks, states make clear that a cyber bomb (e.g. a virus that bursts a dam or crashes an airliner's systems) is as unlawful as any artillery shell.[158] Defining a digital armed-attack with objective benchmarks – scale (casualties, outages), effect (physical destruction), and hostile intent – would give governments a bright line for lawful self-defense.[159]

B. Applying Jus in Bello to Cyber

In an armed conflict, all cyber weapons and tactics must comply with established International Humanitarian Law (the law of armed conflict). This means cyber operations in war must respect distinction, proportionality, and precautions just

[153] Finlay and Payne (n 8).
[154] Schmitt and Pakkam (n 37).
[155] Haataja (n 45).
[156] Jakub Spáčil, 'Cyber Operations against Critical Financial Infrastructure: a Non-Destructive Armed Attack?' (2022) *International and Comparative Law Review,* Vol. *22* (2), 27–42, 28.
[157] Schmitt and Pakkam (n 37).
[158] Ibid.
[159] Ibid.

like bombs or bullets.[160] The International Committee of the Red Cross emphasizes that any cyber act reasonably expected to cause injury, death or physical damage is an attack subject to International Humanitarian Law.[161] Even non-physical assaults – for example a digital strike that shuts down hospital systems or contaminates water treatment controls – would qualify as attacks because they endanger civilians.[162] Accordingly, cyber weapons (malware, botnets, viruses, etc.) are not exempt. States should explicitly require that all new cyber capabilities undergo the same Article 36 review as conventional arms.[163] In target selection, commanders must distinguish between military and civilian cyber infrastructure: for instance, a missile guidance network (military objective) can be lawfully disrupted, but a civilian banking server cannot, even if attacked by code.[164] Likewise, measures of last resort are needed: war planners should avoid collateral data loss by, for example, freezing the malware if it drifts into non-military systems. The paper suggests codifying these principles by stating that all cyber means are means of warfare under International Humanitarian Law, triggering existing rules.[165] This might take the form of military manuals or international guidelines stating that (a) civilian networks and data are protected objects, (b) attackers must foresee and mitigate any incidental civilian harm, and (c) commanders must conduct weapon reviews for new cyber tools.[166] Strengthening these norms – as the Tallinn Manual has begun to do in its commentary – would close such loopholes. There is no cyber exception to the laws of war. Digital attacks must observe distinction and precaution just like any other weapon.[167]

C. Enhancing Attribution and State Responsibility

[160] International Committee of the Red Cross (n 48).

[161] International Committee of the Red Cross (n 35).

[162] B. Abbou and others, 'When all computers shut down: the clinical impact of a major cyber-attack on a general hospital' (2024) *Frontiers in Digital Health* 6 1321485.

[163] Natalia Jevglevskaja, 'Challenges to Article 36 Reviews Posed by (Autonomous) Cyber Capabilities', in *International Law and Weapons Review: Emerging Military Technology under the Law of Armed conflict* (Cambridge, Cambridge University Press 2021), 239–70, 244 0.

[164] Schmitt (n 54).

[165] International Committee of the Red Cross (n 48).

[166] Schmitt (n 54).

[167] International Committee of the Red Cross (n 48).

Cyber attackers often hide behind layers of anonymity or proxy actors. To address this issue, the paper recommends strengthening collective attribution mechanisms and clarifying how state responsibility is applied.[168] This could involve international protocols for joint investigation of major intrusions. For example, an independent multi-state panel (similar to the Organisation for the Prohibition of Chemical Weapons for chemical attacks) could examine high-profile incidents and publicly report findings.[169] At a minimum, victim and transit states should form rapid-response teams (e.g. joint Computer Security Incident Response Team/Computer Emergency Response Team task forces) to share forensic evidence on attacks.[170] The (UN) Group of Governmental Experts's Norm 27 already urges cooperation among national cybersecurity agencies and diplomats in incident analysis.[171] The paper further proposes that states make such cooperation routine. For instance, agreements to share malware signatures, network logs or threat intelligence across borders would greatly improve situational awareness and certainty.

Under the general rule of international law, a state is responsible in cyber conflicts if it knows or intends that malicious cyber actors (even private contractors or proxy militias) are operating from its territory.[172] This follows the principle that a state should not knowingly allow its territory to be used for wrongful acts. In other words, harboring or contracting out hacking-for-hire would violate a duty of due diligence.[173]

---

[168] Yuval Shany and Michael N Schmitt, 'An International Attribution Mechanism for Hostile Cyber Operations' (2020) 96 *International Law Studies* 196, 199.

[169] *François Delerue*, 'Reflections on the Opportunity of an International Attribution and Accountability Mechanism for Cyber Operations', *QIL QDI*, 31 July 2024, https://www.qil-qdi.org/reflections-on-the-opportunity-of-an-international-attribution-and-accountability-mechanism-for-cyber-operations/, accessed 21 September 2025.

[170] European Union Agency for Cybersecurity (ENISA), '*2020 Report on Computer Security Incident Response Team-LE Cooperation: A study of the roles and synergies among selected European Union Member States/EFTA countries', ENISA*, January 2021, https://www.enisa.EuropeanUnionropa.European Union/sites/default/files/publications/ENISA%20Report%20on%20Computer Security Incident Response Team-LE%20Cooperation%20-%20A%20study%20of%20the%20roles%20and%20synergies%20among%20selected%20countries.pdf, accessed 21 September 2025.

[171] UN Group of Governmental Experts Report on Responsible State Behaviour (n 65).

[172] Antonio Coco and Talita de Souza Dias, 'Cyber Due Diligence: A Patchwork of Protective Obligations in International Law' (2021) 32 *European Union Journal of International Law* 771, 776 https://doi.org/10.1093/ejil/chab056.

[173] Ibid.

On the other hand, a state that is merely the unwitting source of random malware (without knowledge) would not be held immediately responsible. Importantly, states must investigate and punish cybercrime within their borders.[174] This means enacting laws to prosecute cyber-attacks and enforcing them strictly – much like how states treat terrorism.[175] To make accountability credible, the paper encourages establishing that directing or controlling a proxy cyber militia is equivalent to state action.[176] An aggressor state cannot hide behind non-state hackers without consequence. Once attribution is confirmed, diplomatic and legal measures (such as sanctions or indictments) should be applied.[177]

D. Clarify Reporting and Transparency Obligations

Finally, the paper recommends new norms regarding reporting and openness to build mutual confidence. States should announce in advance which cyber actions would cross their red lines, such as attacks causing large-scale casualties or targeting specific critical systems. After an incident, they should promptly notify relevant parties – allied states, affected nations, or the UN – with technical details of what occurred.[178] The 2021 UN Group of Governmental Experts even recommends that a victim state formally notify the State from which the activity is emanating and seek cooperation in confirming the facts. Adopting such steps (even as voluntary guidelines) would reduce misunderstanding and rumor.[179] The paper suggests a model similar to arms-control transparency measures: timely incident reports and requests for clarifications (possibly via diplomatic hotlines or the existing Nuclear Risk Reduction Centers) should be standard practice. Over the longer term, coalitions of willing states could compile an annual overview of significant cyber incidents, analogous to the IAEA incident

[174] Ibid.

[175] Jennifer Trahan, 'The Criminalization of Cyber-Operations under the Rome Statute' (2021) *19 J Int'l Crim Just* 1133, 1138.

[176] Canfil (n 114).

[177] Chimène I Keitner, 'Attribution by indict ment' (2019) 113 *American Journal of International Law* 207–12, 208.

[178] UN Group of Governmental Experts Report on Responsible State Behaviour (n 65).

[179] Ibid.

reporting or UN arms reports.[180] Carving out expectations of notice and fact-sharing – rather than post-facto secrecy – would anchor cyberspace in greater accountability.[181]

8. Multilateral and Diplomatic Initiatives

A. UN Group of Governmental Experts and Open-Ended Working Group (at the UN) Processes

At the United Nations, two tracks – the UN Group of Governmental Experts and the Open-Ended Working Group – have become the primary forums for cyber norm-building.[182] The 2013–2015 (UN) Group of Governmental Experts and Open-Ended Working Group (at the UN) (2019–2021) explicitly affirmed that existing international law applies to cyberspace, producing lists of responsible-behavior norms.[183] These bodies rely heavily on case study–driven diplomacy. For instance, Australia submitted detailed hypothetical scenarios to show how the UN Charter and Geneva law govern cyber (e.g. cyber-attacks on hospitals or ports).[184] Numerous state non-papers contain fictional incidents to flesh out the rules. Importantly, the Open-Ended Working Group (at the UN) allows space for stakeholders: intersessional meetings often include technical experts, industry, Non-Governmental Organizations and academics.[185] The paper encourages continuing this practice: expert panels can

[180] Open, informal, cross-regional group of the Open-Ended Working Group (at the UN) Confidence Builders, '*Confidence-Building Measures – A recap and a vision for the future permanent mechanism*', *UN Office for Disarmament Affairs*, Joint Working Paper, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_%282021%29/Open-Ended Working Group (at the UN)_Confidence_Builders_Working_paper_on_CBMs_in_the_permanent_future_mechanism.pdf, accessed 21 September 2025.

[181] N. Tsagourias and F Middleton, 'Fact-Finding and Cyber Attribution' in R Buchan, D Franchini and N Tsagourias (eds), *The Changing Character of International Dispute Settlement: Challenges and Prospects* (Cambridge: Cambridge University Press, 2023) 439–66, 443.

[182] Nanette S Levinson, 'Idea entrepreneurs: The United Nations Open-Ended Working Group & cybersecurity' (2021) *Telecommunications Policy,* Vol. *45* (6), 102142.

[183] UN Group of Governmental Experts Report on Responsible State Behaviour (n 65).

[184] Department of Foreign Affairs and Trade (Australia), '*Australia Non Paper: Case studies on the application of international law in cyberspace',* Non-paper, DFAT, 2020, https://www.dfat.gov.au/sites/default/files/australias-Open-Ended Working Group (at the UN)-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf, accessed 21 September 2025.

[185] Levinson (n 181).

analyze model incidents (like election hacking or grid failures) and present them at UN forums. Through such concrete examples, states refine their positions.[186] The (UN) Group of Governmental Experts reports also proposed cooperative measures (like instructing states to notify each other of vulnerabilities) and recommended inviting bodies like the International Law Commission to study how law applies to cyber.[187] The UN processes serve as diplomatic laboratories: by discussing specific cases and negotiating voluntary norms (the 2015 (UN) Group of Governmental Experts's 11 norms, for instance), they gradually build a shared understanding of how the charter applies online.[188]

B. North Atlantic Treaty Organization/European Union and Regional Cooperation

Military and regional alliances are key venues for operationalizing cyber norms. North Atlantic Treaty Organization, for example, has long affirmed that a significant cyberattack could invoke Article 5 collective defense.[189] North Atlantic Treaty Organization's Cooperative Cyber Defence Centre of Excellence (Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization)) even trains armed forces on legal scenarios.[190] Notably, the Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization) Cyber Law Toolkit and its legal exercises (like Locked Shields and Cyber Coalition) integrate jus ad bellum and jus in bello issues into war games, ensuring that national forces practice respecting international law.[191] North Atlantic Treaty Organization's recent summits (Wales 2014,

[186] Sheetal Kumar, 'The missing piece in human-centric approaches to cybernorms implementation: the role of civil society' (2021) *Journal of Cyber Policy,* Vol. 6 (3), 375–393, 379.
[187] UN Group of Governmental Experts Report on Responsible State Behaviour (n 65).
[188] Levinson (n 181).
[189] Finlay and Payne (n 8).
[190] North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization), *Training Catalogue, 2024* (Updated 10 September 2024), https://Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization).org/uploads/2024/09/2024_North Atlantic Treaty Organization_CCD_COE_Training_Catalogue_final_revSept2024.pdf, accessed 21 September 2025.
[191] North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, 'Cyber Law Toolkit 2024', 2023, https://Cooperative Cyber Defence Centre of Excellence (North Atlantic Treaty Organization).org/news/2023/cyber-law-toolkit/, accessed 21 September 2025.

Warsaw 2016) have formally recognized cyberspace as an operational domain and committed Allies to strengthen network resilience.[192]

The European Union also supports joint cyber resilience in the Black Sea–Eastern Mediterranean region. The European Union's new Black Sea Security Strategy explicitly commits to building capacity, cooperation and information sharing on hybrid and cyber threats among regional partners.[193] It calls for using CSDP missions, European Union technical assistance and coordination with North Atlantic Treaty Organization to protect critical infrastructure. This could involve joint exercises (for example, drills simulating power-grid attacks with allied navies participating), shared cyber defense training, and coordinated public warnings when a wave of digital attacks is detected.[194] For instance, the European Union and North Atlantic Treaty Organization have launched structured dialogues on cybersecurity, and European Union programs now fund cyber defense capacity-building in Eastern Mediterranean countries.[195] These multilateral activities should reinforce the norms identified in UN fora, by familiarizing Black Sea/East Mediterranean militaries and technocrats with the same legal standards (e.g. rules for targeting, incident reporting).

C. Multi-Stakeholder Diplomacy

Creating norms should not be left to governments alone. Achieving broad support requires engaging industry, academia and civil society. Prominent industry accords have already begun this work: for instance, the Microsoft-led Cybersecurity Tech Accord and the Siemens Charter of Trust set voluntary standards (banning data ransom,

[192] Mikkel Storm Jensen, 'Five good reasons for North Atlantic Treaty Organization's pragmatic approach to offensive cyberspace operations' (2022) 22 *Defence Studies* 464, 466.
[193] European Unionropean Commission and High Representative of the Union for Foreign Affairs and Security Policy (n 90).
[194] Annegret Bendiek and Mika Kerttunen, '*Enhancing European Union-North Atlantic Treaty Organization Cooperation in Preparedness and Critical Infrastructure Protection',* SWP Working Paper No 06, June 2025, https://www.swp-berlin.org/publications/products/arbeitspapiere/SWP_WP_Enhancing_European_Union-North_Atlantic Treaty Organization_Cooperation_Critical_Infrastructure_Protection_Bendiek_Kerttunen.pdf, accessed 21 September 2025.
[195] European Union CyberNet, '*Mapping of European Union-funded External Cyber Capacity Building Actions 2022',* European Unionropean Commission, 2023, https://www.European Unioncybernet.European Union/wp-content/uploads/2023/04/mapping-report-on-European Union-funded-external-cyber-capacity-building-actions-2022.pdf, accessed 21 September 2025.

protecting medical and election systems, etc.).[196] Likewise, the 2018 Paris Call for Trust and Security in Cyberspace is a multi-stakeholder pledge (endorsed by 70+ states, 1500 companies and Non-Governmental Organizations) around nine principles – including protecting individuals and critical infrastructure from cyberattack.[197] Such initiatives amplify legal norms by translating them into industry practice and public expectation. The paper suggests that official diplomacy regularly seek input from these constituencies. For example, UN Open-Ended Working Group (at the UN) sessions have benefited from civil society briefings, and North Atlantic Treaty Organization encourages expert academia to advise on rule nuances.[198] Standards bodies also play a role. International technology standards (such as ITU guidelines or ISO protocols) can incorporate legal requirements for precautions and resilience.[199] By including private-sector experts and Non-Governmental Organizations, states can use technical know-how and moral influence. A rule, for example, prohibiting cyberattacks on hospitals will have more impact if hospital networks and software vendors also commit to defending against such exploits.[200] Organizing regular public–private roundtables or issuing joint codes of conduct (as some digital coalitions have done) can unite legal norms with practical measures. For example, the Paris Call demonstrates this approach. It involves broad participation from governments, industry and Non-Governmental Organizations, giving many parts of society a stake in upholding these norms (for

[196] Roxana Radu, Matthias C Kettemann, Trisha Meyer and Jamal Shahin, 'Normfare: Norm entrepreneurship in internet governance' (2021) *Telecommunications Policy,* Vol. *45* (6), 102148.

[197] Kaja Ciglic and John Hering, 'A Multi-Stakeholder Foundation for Peace in Cyberspace' (2021) *Journal of Cyber Policy 6,* 360–374, 366.

[198] Ian Johnstone, Arun Sukumar and Joel Trachtman, 'Building cybersecurity through multistakeholder diplomacy: Politics, processes, and prospects' in Ian Johnstone, Arun Sukumar and Joel Trachtman (eds), *Building an International Cybersecurity Regime: Multistakeholder Diplomacy* (Edward Elgar Publishing, 2023).

[199] Irene Kamara, 'European Unionropean cybersecurity standardisation: A tale of two solitudes in view of European Unionrope's cyber resilience' (2024) *Innovation: The European Union Journal of Social Science Research* 1–20, 11..

[200] Priya Urs, Talita Dias, Antonio Coco and Dapo Akande, '*The International Law Protections against Cyber Operations Targeting the Healthcare Sector', Oxford Institute for Ethics, Law and Armed conflict*, University of Oxford, April 2023, https://www.elac.ox.ac.uk/wp-content/uploads/2023/04/ELAC-Research-Report_International-Law-Protections-against-Cyber-Operations-Targeting-the-Healthcare-Sector.pdf, accessed 21 September 2025.

example, tech companies learn to secure their software and media organizations learn to flag propaganda).[201]

D. Confidence-Building Measures

Finally, states should negotiate confidence-building measures to reduce cyber tensions. Historical analogies are instructive; during the Cold War, hotlines and incident-reporting agreements helped prevent escalation.[202] A similar toolkit can be adapted for cyberspace. For instance, quick channels for sharing information between adversaries can defuse crises. The 2013 U.S.-Russia cyber pact is a good example; it established direct contacts between US-Computer Emergency Response Team and its Russian counterpart to exchange threat indicators in real time.[203] It also repurposed the old US–Russia nuclear hotline (the Nuclear Risk Reduction Center) to allow formal inquiries about suspected cyberattacks, and even set up a secure voice line between Washington and Moscow for cyber incidents.[204] The paper recommends extending such ideas to North Atlantic Treaty Organization/European Union networks – for instance, establishing a regional incident-warning hotline linking Black Sea countries' Computer Emergency Response Teams. Other specific CBMs include: conducting joint cyber exercises (e.g. simulating cross-border attacks while respecting no-fire lines), pre-notification of major exercises to avoid misidentification, and sharing anonymized data on threats. On deterrence, Allied states could publicly affirm that a massive cyber attack on a North Atlantic Treaty Organization or European Union member would activate collective defense (echoing Article 5), thereby raising the costs for potential aggressors.[205] Confidence-building means range from practical tech collaboration

[201] Ciglic and Hering (n 196).

[202] Paul Meyer, 'Confidence-building measures in cyberspace' in Eneken Tikk and Mika Kerttunen (eds), *Routledge Handbook of International Cybersecurity* (Routledge 2020).

[203] Lora Saalman, Fei Su and Larisa Saveleva Dovgal, '*Cyber Risk Reduction in China, Russia, the United States and the European Union', Stockholm International Peace Research Institute (SIPRI)*, June 2024, https://www.sipri.org/sites/default/files/2024-06/cyber_risk_reduction.pdf, accessed 21 August 2025.

[204] Rose Gottemoeller and Daniil Zhukov, *'Nuclear Risk Reduction Centers: A Stable Channel in Unstable Times', Stanley Center for Peace and Security*, October 2023, https://stanleycenter.org/wp-content/uploads/2023/10/Nuclear-Risk-Reduction-Centers-Gottemoeller-Zhukov.pdf ,(accessed 21 August 2025.

[205] OSCE, '*10 Years of OSCE Cyber/Information and Communications Technology Security Confidence-Building Measures',* OSCE Secretariat, 2023)https://www.osce.org/files/f/documents/f/7/555999_1.pdf, accessed 21 August 2025.

(information sharing, shared Computer Emergency Response Team platforms) to diplomatic commitments (joint statements or sanctions pledges for violations). By baking these measures into alliances, the region can deter rash cyber aggression and mitigate accidents before they spiral.[206]

9. Implications for Regional Stability and Conclusion

A. Reinforcing Rule of Law

Clarifying the application of universal international law to regional threats ultimately strengthens the rules-based security architecture in the Black Sea–Eastern Mediterranean nexus. When states clearly define the conditions for self-defense and the obligations during conflict, unpredictability decreases.[207] Applying existing international law to cyberspace provides a victim state with a "tool kit" to identify violations, assign responsibility, resolve disputes peacefully or take lawful countermeasures. A well-defined legal framework makes state behavior more predictable and reduces the risk of uncontrolled escalation. If governments agree in advance on what counts as a legal or illegal cyber act, responses become deliberate instead of knee-jerk.[208] This predictability supports justice – victims see that wrongdoing is addressed through the law (sanctions, indictments, collective defense) rather than through revenge or a power vacuum. A transparent legal regime (with adapted jus ad bellum and jus in bello principles) also helps vulnerable states resist coercion, as they can point to shared rules when defending their actions. Over time, internalizing these norms will help treat cyberspace aggression as a regulated domain, not an anarchic Wild West.[209] Closing the legal gaps reaffirms the system of laws that

[206] Robert Collett, 'Understanding cybersecurity capacity building and its relationship to norms and confidence building measures' (2021) *Journal of Cyber Policy,* Vol. 6(3) 298–317, 302.

[207] Russell Buchan, 'Non-forcible measures and the law of self-defence' (2023) *International & Comparative Law Quarterly,* Vol. *72* (1) 1–33.

[208] United Nations General Assembly, '*Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States'*, UN Doc A/76/136, 28 May 2021, https://digitallibrary.un.org/record/3933543/files/A_76_136-EN.pdf, accessed 21 August 2025.

[209] Gisel, Rodenhauser and Dörmann (n 56).

all parties have pledged to follow, reinforcing a rules-based order amid constant digital threats.,*B. Maintaining Social and Political Cohesion*

For people in the region, strong cyber norms would increase trust in institutions and reduce public panic during cyber incidents. If citizens see their governments responding to a cyber crisis with established legal measures – for example, notifying allies, providing clear explanations and sanctioning the perpetrators – confidence remains intact. This also prevents rumors or panic that might otherwise spread after mysterious outages or disinformation campaigns.[210] Moreover, by involving diverse stakeholders (governments, tech companies, civil society) in building these norms, the public sees cyber defense as a collective effort rather than a secret arms race.[211] For instance, the Paris Call demonstrates this. It has broad participation from governments, industry and Non-Governmental Organizations, giving many parts of society a stake in upholding these norms (for example, tech companies commit to secure their software and media organizations learn to flag propaganda).[212] Consequently, when an incident occurs, multiple trusted voices can promote a coherent, lawful response rather than discord. In practical terms, clear cyber rules help authorities quickly classify an event (as a crime, not war) and respond appropriately, avoiding overreaction that can frighten populations.[213] Thus, reinforcing international norms in cyberspace directly supports social cohesion – citizens of Black Sea/East Med states will be less likely to feel abandoned or vulnerable if they know a legal playbook governs their defense.[214]

C. Summary of Recommendations

[210] R. Shandler and M. A. Gomez, 'The hidden threat of cyber-attacks – undermining public confidence in government' (2023) *20 Journal of Information Technology & Politics* 359, 365.

[211] K. Ciglic and J. Hering, 'A multi-stakeholder foundation for peace in cyberspace' (2021) *Journal of Cyber Policy,* Vol. *6* (3), 360–374.

[212] Arun Sukumar, Dennis Broeders and Monica Kello, 'The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy,' (2024) *Contemporary Security Policy,* Vol. 45 (1), 7.

[213] ENISA, '*Best Practices for Cyber Crisis Management,'* February 2024, https://www.enisa.European Unionropa.European Union/sites/default/files/2024-11/ENISA%20Study%20Best%20Practices%20Cyber%20Crisis%20Management.pdf, accessed 21 September 2025.

[214] Sabanadze and Dalay (n 20).

In conclusion, bridging the cyber gap in the Black Sea–Eastern Mediterranean requires both legal adaptation and cooperative diplomacy. Legally, states must refine jus ad bellum by explicitly defining what a cyber armed attack means (for instance, catastrophic physical effects) and clarifying the thresholds for self-defense. They must also integrate jus in bello into cyber by affirming that digital operations obey all International Humanitarian Law rules (distinction, proportionality, and Article 36 weapon reviews). In parallel, responsibility and transparency are vital: international mechanisms should be strengthened so that attribution of cyber incidents is credible (through joint investigations and evidence-sharing), and states should agree to cooperative reporting (notification of attacks and red-lines) to prevent misperception. Diplomatically, Non-Governmental Organization's multilateral forums (the UN Group of Governmental Experts and Open-Ended Working Group) must continue unpacking these norms through case-study discussions. Regional and alliance structures (North Atlantic Treaty Organization, the European Union, Black Sea security initiatives) should incorporate these norms into exercises, training and policy (for example, by simulating cyber incidents in military drills and issuing joint statements on cyber defense). Crucially, these efforts should engage all stakeholders: governments should invite the private sector, technical experts and civil society into norm-building (as in the Paris Call and industry accords), since broad adherence to the rules enhances stability. Confidence-building measures – from Computer Emergency Response Team information-sharing to incident hotlines – will further deter reckless behavior. By combining clear legal rules with robust international collaboration, the cyber gap in the Black Sea–Eastern Mediterranean can be closed, thus preventing the erosion of international order and preserving both security and societal cohesion in the region.

Bibliography

Abbou B and others, ‘When all computers shut down: the clinical impact of a major cyber-attack on a general hospital’ (2024) 6 Frontiers in Digital Health 1321485

Abraham D, Houmb SH and Erdodi L, ‘Cyber-Attacks on Energy Infrastructure—A Literature Overview and Perspectives on the Current Situation’ (2025) 15 Applied Sciences 9233

Akyeşilmen N, 'Türkiye in the Global Cybersecurity Arena: Strategies in Theory and Practice' (2022) 24(3) Insight Turkey 109

Androjna A and others, 'Assessing Cyber Challenges of Maritime Navigation' (2020) 8 J Mar Sci Eng 776

Atlantic Council Task Force on Black Sea Security, *A Security Strategy for the Black Sea* (Atlantic Council 2023)

Axt H-J, 'Conflicts and Global Powers in the Eastern Mediterranean. An Introduction' (2022) 70 Comparative Southeast European Studies 393

Banks WC, 'The Bumpy Road to a Meaningful International Law of Cyber Attribution' (2019) 113 AJIL Unbound 191

Bendiek A and Kerttunen M, *Enhancing EU-NATO Cooperation in Preparedness and Critical Infrastructure Protection* (SWP Working Paper No 06, 2025)

Bendiek A, Bund J and Kerttunen M, 'The Attribution Dividend: Protecting Critical Infrastructure from Cyber Attacks' (SWP Comment 2024/C 46, 2024)

Bradshaw S, Bailey H and Howard PN, *Industrialized Disinformation: 2020 Global Inventory of Organised Social Media Manipulation* (Oxford Internet Institute 2021)

Broeders D, 'Private active cyber defense and (international) cyber security—pushing the line?' (2021) 7 Journal of Cybersecurity tyab010

Buchan R, 'Non-forcible measures and the law of self-defence' (2023) 72(1) International & Comparative Law Quarterly 1

Bueger C and Liebetrau T, 'Critical Maritime Infrastructure Protection: What's the Trouble?' (2023) 155 Marine Policy 105772

Burton J and Stevens T, 'System, Alliance, Domain: A Three-Frame Analysis of NATO's Contribution to Cyber Stability' in Chesney R (ed), *Cyberspace and Instability* (Edinburgh University Press 2022)

C4ADS, *Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria* (C4ADS 2019)

Canfil JK, 'The Illogic of Plausible Deniability: Why Proxy Conflict in Cyberspace May No Longer Pay' (2022) 8 Journal of Cybersecurity tyac007

Cavalcanti de Mello Filho E, 'Armed Attacks against Merchant Vessels: "Looking behind the Flag" to Find the Victim State' (2024) 29 Journal of Conflict & Security Law 281

Centre for Strategic and International Studies, 'Navigating Security Challenges in the Black Sea Region' (CSIS 2024)

Ciglic K and Hering J, 'A Multi-Stakeholder Foundation for Peace in Cyberspace' (2021) 6(3) Journal of Cyber Policy 360

Clavijo Mesa MV, Patino-Rodriguez CE and Guevara Carazas FJ, 'Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains' (2024) 15 Information 710

Coco A and de Souza Dias T, '"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law' (2021) 32 European Journal of International Law 771

Collett R, 'Understanding cybersecurity capacity building and its relationship to norms and confidence building measures' (2021) 6(3) Journal of Cyber Policy 298

Collett R and Barmpaliou N, *International cyber capacity building: global trends and scenarios* (European Union Institute for Security Studies 2021)

Congressional Research Service, *Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience* (CRS Report R48067, 2024)

Council of the European Union, 'Cyberspace: Council approves declaration on a common understanding of application of international law to cyberspace' (Press release, 18 November 2024)

Council of the European Union, *Declaration by the European Union and its Member States on a Common Understanding of the Application of International Law to Cyberspace* (ST-15833-2024-INIT, 2024)

Decree of the President of Ukraine No 447/2021, *On the Cybersecurity Strategy of Ukraine* (National Security and Defense Council of Ukraine 2021)

Delerue F, *Cyber Operations and International Law* (Cambridge University Press 2020)

Delerue F, 'Reflections on the Opportunity of an International Attribution and Accountability Mechanism for Cyber Operations' (2024) QIL QDI

Delerue F, 'The Threshold of Cyber Warfare: from Use of Cyber Force to Cyber Armed Attack' in *Cyber Operations and International Law* (Cambridge University Press 2020)

Department of Foreign Affairs and Trade (Australia), *Australia Non Paper: Case studies on the application of international law in cyberspace* (DFAT 2020)

Dickson J and Harding E, 'How a Cyber Alliance Took Down Russian Cybercrime' (Center for Strategic and International Studies 2025)

Eaton T, 'Self-Defense to Cyber Force: Combatting the Notion of "Scale And Effect"' (2021) 36 American University International Law Review 697

Egloff FJ, 'Public attribution of cyber intrusions' (2020) 6 Cybersecurity tyaa012

Egloff FJ and Smeets M, 'Publicly attributing cyber attacks: a framework' (2023) 46 Journal of Strategic Studies 502

Eichensehr KE, 'Ukraine, Cyberattacks, and the Lessons for International Law' (2022) 116 American Journal of International Law 145

ENISA, *Best Practices for Cyber Crisis Management* (2024)

Ertan A and others (eds), *Cyber Threats and NATO 2030: Horizon Scanning and Analysis* (NATO CCDCOE Publications 2020)

EU CyberNet, *Mapping of EU-funded External Cyber Capacity Building Actions 2022* (European Commission 2023)

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *The European Union's strategic approach to the Black Sea region* (JOIN(2025) 135 final, 2025)

European Union Agency for Cybersecurity, *2020 Report on CSIRT-LE Cooperation: A study of the roles and synergies among selected EU Member States/EFTA countries* (ENISA 2021)

Finlay L and Payne C, 'The Attribution Problem and Cyber Armed Attacks' (2019) 113 AJIL Unbound 202

Finnemore M and Hollis DB, 'Beyond Naming and Shaming: Accusations and International Law in Cybersecurity' (2020) 31 European Journal of International Law 969

FP Analytics, *Digital Front Lines* (FP Analytics 2023)

Gisel L, Rodenhäuser T and Dörmann K, 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts' (2020) 102 International Review of the Red Cross 287

Gorwa R and Peez A, 'Big Tech Hits the Diplomatic Circuit: Norm Entrepreneurship, Policy Advocacy, and Microsoft's Cybersecurity Tech Accord' in Broeders D and van den Berg B (eds), *Governing Cyberspace: Behaviour, Power and Diplomacy* (Rowman & Littlefield 2020)

Gottemoeller R and Zhukov D, *Nuclear Risk Reduction Centers: A Stable Channel in Unstable Times* (Stanley Center for Peace and Security 2023)

Haataja S, 'Cyber operations against critical infrastructure under norms of responsible state behaviour and international law' (2023) 30 International Journal of Law and Information Technology 423

Halisdemir E, *National Cybersecurity Organisation: TURKEY* (NATO Cooperative Cyber Defence Centre of Excellence 2021)

Hines B, 'Reinterpreting the Legality of Forcible Self-Defence in Response to Non-Kinetic Cyber Attacks' (2024) 25(1) Melbourne Journal of International Law 1

International Committee of the Red Cross, *International humanitarian law and cyber operations during armed conflicts* (Position paper, 2019)

International Committee of the Red Cross, 'International humanitarian law and cyber operations during armed conflicts' (2020) 102 International Review of the Red Cross 481

International Institute for Strategic Studies, *Cyber Capabilities and National Power: A Net Assessment* (Research Paper, 2021)

Jensen B, Valeriano B and Whitt S, 'How cyber operations can reduce escalation pressures: Evidence from an experimental wargame study' (2024) 61 Journal of Peace Research 119

Jensen MS, 'Five good reasons for NATO's pragmatic approach to offensive cyberspace operations' (2022) 22 Defence Studies 464

Jevglevskaja N, 'Challenges to Article 36 Reviews Posed by (Autonomous) Cyber Capabilities' in *International Law and Weapons Review: Emerging Military Technology under the Law of Armed Conflict* (Cambridge University Press 2021)

Jiang Z, 'Regulating the Use and Conduct of Cyber Operations through International Law: Challenges and Fact-finding Body Proposal' (2020) 5 LSE Law Review 59

Jiguet F and others, 'GNSS spoofing in conflict zones disrupts wildlife tracking and hampers research and conservation efforts' (2025) 16 Nat Commun 1199

Johnstone I, Sukumar A and Trachtman J, 'Building cybersecurity through multistakeholder diplomacy: Politics, processes, and prospects' in Johnstone I, Sukumar A and Trachtman J (eds), *Building an International Cybersecurity Regime: Multistakeholder Diplomacy* (Edward Elgar Publishing 2023)

Kajander A, *Unnecessary Repetition: Russia's Latest Attempt at a New UN Convention on Cyberspace* (NATO Cooperative Cyber Defence Centre of Excellence 2023)

Kamara I, 'European cybersecurity standardisation: A tale of two solitudes in view of Europe's cyber resilience' (2024) Innovation: The European Journal of Social Science Research 1

Katagiri N, 'Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks' (2021) 7 Journal of Cybersecurity tyab009

Keitner CI, 'Attribution by Indictment' (2019) 113 American Journal of International Law 207

Kello L, 'Cyber legalism: why it fails and what to do about it' (2021) 7(1) Journal of Cybersecurity tyab014

Korzak E, *Russia's Cyber Policy Efforts in the United Nations* (Tallinn Paper No 11, NATO Cooperative Cyber Defence Centre of Excellence 2021)

Kumar S, 'The missing piece in human-centric approaches to cybernorms implementation: the role of civil society' (2021) 6(3) Journal of Cyber Policy 375

Lațici T, *Understanding the EU's approach to cyber diplomacy and cyber defence* (European Parliamentary Research Service 2020)

Levinson NS, 'Idea Entrepreneurs: The United Nations Open-Ended Working Group & Cybersecurity' (2021) 45 Telecommunications Policy 102142

Lu C and others, 'Overview of satellite nav spoofing and anti-spoofing techniques' (2024) 12 Frontiers in Physics 1428544

Lysenko A and Gunitsky S, 'The invisible front: Ukraine's IT army and the evolution of cyber resistance' (2025) 41 Post-Soviet Affairs 263

Mačák K, 'Unblurring the lines: military cyber operations and international law' (2021) 6 Journal of Cyber Policy 411

Meyer P, 'Confidence-building measures in cyberspace' in Tikk E and Kerttunen M (eds), *Routledge Handbook of International Cybersecurity* (Routledge 2020)

Mickonytė A, 'Obligation to Mutual Assistance Under Article 42(7) TEU: The Conundrum of Intentional Ambiguity' (2024) 18 ICL Journal 311

Moynihan H, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention* (Chatham House Research Paper, 2019)

Moynihan H, 'The vital role of international law in the framework for responsible state behaviour in cyberspace' (2021) 6(3) Journal of Cyber Policy 394

NATO Cooperative Cyber Defence Centre of Excellence, *Cyber Law Toolkit 2024* (2023)

NATO Cooperative Cyber Defence Centre of Excellence, *Training Catalogue, 2024* (2024)

NATO, *Cyber defence* (2024)

NATO, *Hybrid threats and hybrid warfare* (2024)

NATO, 'Vilnius Summit Communiqué' (Press Release (2023) 001, 2023)

Nijs M, 'Humanizing siege warfare: Applying the principle of proportionality to sieges' (2020) 102(914) International Review of the Red Cross 683

Oorsprong F, Ducheine P and Pijpers P, 'Cyber-attacks and the right of self-defense: a case study of the Netherlands' (2023) 6 Policy Design and Practice 217

Open informal cross-regional group of the OEWG Confidence Builders, *Confidence-Building Measures – A recap and a vision for the future permanent mechanism* (Joint Working Paper, UN Office for Disarmament Affairs)

Ormrod A, Ormrod D and Slay J, 'Cyber Offensive Operations in Hybrid Warfare: Observations from the Russo-Ukrainian Conflict' (2023) 22(1) Journal of Information Warfare 76

OSCE, *10 Years of OSCE Cyber/ICT Security Confidence-Building Measures* (OSCE Secretariat 2023)

Pomson O, 'Methodology of identifying customary international law applicable to cyber activities' (2023) 36 Leiden Journal of International Law 1023

Praks H, *Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage* (Hybrid CoE Working Paper 32, European Centre of Excellence for Countering Hybrid Threats 2024)

Prucková M, *Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO* (NATO Cooperative Cyber Defence Centre of Excellence 2021)

Radu R and others, 'Normfare: Norm entrepreneurship in internet governance' (2021) 45(6) Telecommunications Policy 102148

Reinhold T, Pleil H and Reuter C, 'Challenges for Cyber Arms Control: A Qualitative Expert Interview Study' (2023) 16 Zeitschrift für Außen- und Sicherheitspolitik 289

Roguski P, 'An Inspection Regime for Cyber Weapons: A Challenge Too Far?' (2021) 115 American Journal of International Law Unbound 111

Romanosky S and Boudreaux B, 'Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government' (2020) 34 International Journal of Intelligence and CounterIntelligence 463

Ryan S, 'Submarine Communication Cables and Belligerent Rights in Armed Conflict' (2024) 38 Ocean Yearbook 459

Saalman L, Su F and Dovgal LS, *Cyber Risk Reduction in China, Russia, the United States and the European Union* (Stockholm International Peace Research Institute 2024)

Sabanadze N and Dalay G, *Threat Perceptions and the Failure of Signalling in Understanding Russia's Black Sea Strategy: How to Strengthen Europe and NATO's Approach to the Region* (Chatham House Research Paper, 2025)

Schmoldt J, 'Cyber proxies: covert state–non-state interactions in cyberwarfare' in Stevens T and Devanny J (eds), *Research Handbook on Cyberwarfare* (Edward Elgar Publishing 2024)

Schmitt MN, 'Cyber Symposium – The Evolution of Cyber Jus ad Bellum Thresholds' (Lieber Institute for Law and Warfare 2022)

Schmitt MN, 'Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace' (2020) 3 Texas National Security Review 32

Schmitt MN, 'Wired warfare 3.0: Protecting the civilian population during cyber operations' (2019) 101 International Review of the Red Cross 333

Schmitt MN and Pakkam AS, 'Cyberspace and the Jus ad Bellum: The State of Play' (2024) 103 International Law Studies 194

Shandler R and Gomez MA, 'The hidden threat of cyber-attacks – undermining public confidence in government' (2023) 20 Journal of Information Technology & Politics 359

Shany Y and Schmitt MN, 'An International Attribution Mechanism for Hostile Cyber Operations' (2020) 96 International Law Studies 196

Sherman J, 'Unpacking Russia's cyber nesting doll' (Atlantic Council 2025)

Sherman J, *Untangling the Russian Web: Spies, Proxies, and Spectrums of Russian Cyber Behavior* (Atlantic Council 2022)

Spáčil J, 'Cyber Operations against Critical Financial Infrastructure: a Non-Destructive Armed Attack?' (2022) 22(2) International and Comparative Law Review 27

Sukumar A and Basu A, 'Back to the territorial state: China and Russia's use of UN cybercrime negotiations to challenge the liberal cyber order' (2024) 9(2) Journal of Cyber Policy 256

Sukumar A, Broeders D and Kello M, 'The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy' (2024) 45 Contemporary Security Policy 7

The White House, *National Cybersecurity Strategy* (2023)

Todorov Y, 'Navigating Uncharted Waters: Tackling Maritime Cybersecurity Challenges in the Black Sea Region' (2024) 55(2) Information & Security: An International Journal 113

Trahan J, 'The Criminalization of Cyber-Operations under the Rome Statute' (2021) 19 J Int'l Crim Just 1133

Triandafyllidou A and Monteiro S, 'Migration narratives on social media: Digital racism and subversive migrant subjectivities' (2024) 29(8) First Monday

Tsagourias N and Middleton F, 'Fact-Finding and Cyber Attribution' in Buchan R, Franchini D and Tsagourias N (eds), *The Changing Character of International Dispute Settlement: Challenges and Prospects* (Cambridge University Press 2023)

UN General Assembly, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States* (A/76/136, 2021)

UN General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (A/76/135, 2021)

UN Security Council, *Record of the open debate on Maintenance of international peace and security: cybersecurity* (S/2021/621, 2021)

Urs P and others, *The International Law Protections against Cyber Operations Targeting the Healthcare Sector* (Oxford Institute for Ethics, Law and Armed Conflict 2023)

US Department of Health & Human Services Health Sector Cybersecurity Coordination Center, *Pro-Russian Hacktivist Group 'KillNet' Threat to HPH Sector* (HC3, 2023)

Wiedemar S, *NATO and Article 5 in Cyberspace* (CSS Analyses in Security Policy No 323, Center for Security Studies 2023)

Zabierek L and others, *US-Russian Contention in Cyberspace* (Belfer Center for Science and International Affairs 2021)

Volume 2, Issue 2

Unequal Partners? Rethinking Burden Sharing in a Future European Defence Union

DR GEORGIOS PAPAGIANNIS[1]

Abstract

This study examines burden sharing among European Union member states within the hypothetical framework of a European Defence Union (EDU). The analysis is grounded in economic theory of alliances, which conceptualizes collective defense as a public good creating conditions for free-riding behavior. This theoretical lens emphasizes the need for equitable burden sharing to sustain the effectiveness and cohesion of the alliance. A cost-benefit methodology is applied, evaluating each member state's contribution and benefits based on geographic, demographic, economic, trade, and security threat dimensions.

Covering the period from 2014 to 2023 and drawing on reliable, comparable datasets, the findings reveal a persistent asymmetry: 21 of 27 EU member states contribute less than the security and economic benefits they receive, while six—most notably France, Germany, and Italy—bear a disproportionately high share of the collective defense burden. The analysis also considers the impact of Brexit, highlighting the United Kingdom's role as a stabilizing factor in the equilibrium of defense burden distribution. Its withdrawal exacerbated existing disparities, increasing the relative burden on major contributors.

The results underscore the urgent need for compensatory mechanisms, flexible contribution schemes, and differentiated responsibilities to ensure the long-term viability, fairness, and institutional legitimacy of any future European defense arrangement.

Keywords EU; Burden Sharing; Economic Theory of Alliances; Free-Rider Problem

[1] Adjunct Lecturer, Athens University of Economics and Business

Introduction

The notion of fair or balanced burden sharing in defense obligations has gained particular importance in recent years, as political and institutional debates on strengthening the EU's strategic autonomy and forming a unified European defense pillar have re-emerged. Despite increasing demands, the EU does not currently possess a common armed force, while the military defense of its member states remains under national sovereignty. For 23 out of the 27 EU member states, defense is reinforced through their participation in NATO, which provides collective security and military support in the event of an attack. However, this reliance on external defense mechanisms has repeatedly been highlighted as a structural weakness in discussions surrounding European strategic autonomy.

Within this framework, institutional actors and experts argue that the EU must acquire common armed forces to ensure the security of its citizens and the territorial integrity of the Union, without relying on third parties. The strengthening of European defence is considered critical not only for security but also for competitiveness, as emphasized in the Draghi Report.[2] Two main factors have recently driven a renewed focus on reinforcing the EU's role in defense:

- External threats to the EU, such as Russia's war in Ukraine, pose serious risks to the security of European citizens. Conflicts, geopolitical rivalry, increasing militarization, and hybrid threats are placing mounting pressure on global security.[3] Preparing for such shocks is a prerequisite for the preservation of peace.[4]
- Defence is a public good,[5] a domain where EU-level coordination could prove beneficial to all. The net benefits of public spending in defence are greater at

[2] Mario Draghi, 'The future of European competitiveness – Part B: In-depth analysis and recommendations' (2024) *European Commission*.
[3] Elena Lazarou and Branislav Stanicek, 'Mapping threats to peace and democracy worldwide' (2024) *European Parliamentary Research Service*.
[4] Sauli Niinistö, 'Safer together: Strengthening Europe's civilian and military preparedness and readiness' (2024) *European Council*.
[5] Gabriel Felbermayr and Atanas Pekanov, 'Pan-European public goods: Rationale, financing and governance' (2024) *European Commission*; Buti, M., and Papakonstantinou, G., 'European public

the European level than at the national level, owing to the more efficient use of resources and capabilities.

In this context, the President of the European Commission, Ursula von der Leyen, has encapsulated the direction the Union should take in defence policy with the phrase: "spend more, spend better, spend European".[6] Her statement underscores the need to transition from fragmented national approaches to a more coordinated, collective, and strategically focused European defence policy — treating defense not only as a condition for security but also as a shared economic interest. From this perspective, the pursuit of greater efficiency in European defence expenditures represents a first step toward building a functional European Defence Union. At the same time, such an approach may support a strategic shift away from setting quantitative spending targets (e.g., percentage of GDP) toward achieving specific operational capabilities and common assets. This need aligns with alliance theory, according to which defense constitutes a public good from which all members benefit, regardless of their individual contributions. In this light, a collectively coordinated and strategically targeted allocation of resources acts as a counterbalance to the phenomenon of 'free riding' and reinforces the principle of equitable burden sharing among participants.

This study focuses on analyzing how defence burdens are distributed among EU member states. It aims to produce results based on the most recent available data covering the period 2014–2023, concerning all 27 EU member states. The study's novelty lies in the introduction of a new variable for measuring benefits: the level of threat to national security. Under this lens, the research seeks to answer three key questions:

1. Which member states bear a heavier burden — and which bear less — in relation to their contribution to the provision of common defence and security, compared to the benefits they derive from it? In other words, are there states that 'over-contribute', providing more resources than the benefits they receive,

goods: How can we supply more?' (2022) *LEAP Policy Brief*, Luiss School of European Political Economy.

[6] Ursula von der Leyen, 'Europe's choice: Political guidelines for the next European Commission 2024–2029' (2024) *European Commission*.

and conversely, states that 'under-contribute', offering less than their fair share while benefiting from the collective security umbrella?

2. How does the burden distribution among member states shift under the assumption of a collective EU army, when the level of security threat is introduced as a variable for estimating defense benefits?

3. How did the burden-sharing arrangement among EU member states change following the United Kingdom's exit from the Union?

1. Past Studies of Burden Sharing: A Brief Review

In a seminal study for the international academic community, Olson and Zeckhauser[7] argued that NATO allies shared the pure public good of defence, as expressed through the deterrent power of the doctrine of Mutual Assured Destruction. According to this doctrine, any action by the Warsaw Pact against the territorial integrity of NATO's European allies would trigger the rapid launch of nuclear ballistic missiles, causing catastrophic damage to the attacker. The threat embedded in the U.S. nuclear arsenal provided non-rival and non-excludable benefits to all alliance members. The researchers posited that under such a collective deterrence system, overall defense spending among NATO members would be suboptimal, as each state would lack sufficient incentives to invest proportionately in defense. Furthermore, they hypothesized that smaller and poorer allies would disproportionately rely on larger and wealthier allies—especially the U.S., the UK, and France, which possessed strategic nuclear weapons. At the same time, West Germany, despite lacking nuclear capabilities, had strong incentives to protect its eastern borders against potential Soviet aggression, thereby indirectly contributing to the protection of other Western allies. This context led Olson and Zeckhauser[8] to formulate the hypothesis of the 'exploitation of the rich by the poor' within NATO. To test this hypothesis, they used Spearman's rank correlation to measure the relationship between the military expenditure-to-GDP ratio and GDP size for the year 1964. They found a positive and statistically significant

[7] Mancur Olson and Richard Zeckhauser, 'An economic theory of alliances' (1966) *The Review of Economics and Statistics*, Vol. 48 (3), 266–279.
[8] Olson and Zeckhauser (no 7) 270

correlation, confirming their theory that the economically stronger allies bore a disproportionately greater defense burden relative to their economic capacity.

An alternative to the pure public good model is the Joint Product Model (JPM). The foundation of this approach was presented by van Ypersele de Strihou,[9] who noted that some military expenditures may yield private benefits to a particular ally's population while offering little or no benefit to others. For example, Portugal's increased defense spending due to its military involvement in Angola had the characteristics of a private good: it provided substantial benefits to Portugal but negligible benefits to its allies. In this context, Sandler[10] developed the JPM, asserting that defense expenditures can produce pure public benefits for the alliance, private benefits for individual countries, and impure public benefits related to damage limitation for specific members. The latter may arise, for instance, from troop deployments on national borders, which offer greater protection to the deploying country than to distant allies.[11]This model is based on a cost-benefit analysis framework in which member states contribute according to the benefits they receive. To that end, a burden-sharing measure was developed to express each country's share of total military expenditures. To evaluate this balance, Sandler and Forbes[12] created a benefit index that encapsulates the total assets protected by defense spending for each member state. They argued that NATO's defence protected each ally's economic base, population, and exposed borders (and later, territorial size), primarily through deterrence capacity. The economic base was equated with GDP, while the other two factors were directly measurable. Since the actual utility function of each state is unknown, the researchers assigned equal weights to each factor, calculating the average of the three indices as representative of the overall benefit. As geopolitical conditions

[9] Jacques van Ypersele de Strihou, 'Sharing the defence burden among Western allies' (1967) *Review of Economics and Statistics*, Vol. 49, 527–536.
[10] Todd Sandler, 'Impurity of defense: An application to the economics of alliances' (1977) *Kyklos*, Vol. 30(3), 443–460.
[11] Martin McGuire and Carl Groth, 'A method for identifying the public good allocation process within a group' (1985) *Quarterly Journal of Economics*, Vol. 99 (4), 915–934;
Todd Sandler and James C. Murdoch, 'Nash–Cournot or Lindahl behavior? An empirical test for the NATO allies' (1990) *Quarterly Journal of Economics*, Vol. 105 (4), 875–894.
[12] Todd Sandler and John F. Forbes, 'Burden sharing, strategy, and the design of NATO' (1980) *Economic Inquiry*, Vol. 18(3), 425–444.

changed, new indicators emerged to capture the benefits of alliance participation, such as import/export volume[13] and exposure to terrorism.[14]

The NATO doctrine of flexible response enabled the alliance to address Warsaw Pact challenges in a differentiated manner. Under this doctrine, NATO developed strategic, tactical, and conventional forces intended to function in a coordinated and complementary way.[15] The combined use of these three categories of weapons meant that NATO's defense activities produced joint security products. As private or impure public benefits increased, the incentive to free ride declined. This was because, to benefit from the alliance's activities, members needed to express their preferences through active participation and contribution.

Studies examined the exploitation hypothesis within NATO before and after 1967—the year marking the formal adoption of the flexible response doctrine. Sandler and Forbes[16] found a significant correlation only for the years 1960–1966; thereafter, except for 1973, the correlation was not statistically significant. Murdoch and Sandler[17] concluded that NATO's flexible response doctrine reduced the potential for free-rider behavior by inducing complementarity among defense outcomes jointly produced by the allies. Using a different methodological approach, Oneal and Elrod[18] analyzed the share of variance in the military expenditure-to-GDP ratio that could be explained by GDP alone over the 1953–1984 period. Their findings showed that after 1968, the explanatory power of GDP was negligible, aligning with previous studies. Hansen, Murdoch, and Sandler[19] concluded that free riding within NATO was only possible in the domain of strategic nuclear forces provided by the nuclear allies. Khanna and

[13] Christos Kollias, 'A preliminary investigation of the burden sharing aspects of a European Union common defence policy' (2008) *Defence and Peace Economics*, Vol. 19 (4), 253–263.
[14] Todd Sandler and Hirofumi Shimizu, H., 'NATO burden sharing 1999–2010: An altered alliance' (2014) *Foreign Policy Analysis*, Vol. 10 (1), 43–60.
[15] James C. Murdoch and Todd Sandler, 'Complementarity, free riding and the military expenditures of NATO allies' (1984) *Journal of Public Economics*, Vol. 25(1), 83–101.
[16] Todd Sandler and John F. Forbes, 'Burden sharing, strategy, and the design of NATO' (1980) *Economic Inquiry Vol.*18(3),425-444
[17] Murdoch and Sandler (no 15) 94.
[18] John R. Oneal and Mark Elrod, 'NATO burden sharing and the forces of change' (1989) *International Studies Quarterly*, Vol. 33 (4), 435–456.
[19] Laurna Hansen, James C. Murdoch and Todd Sandler, 'On distinguishing the behavior of nuclear and non-nuclear allies in NATO' (1990) *Defence Economics*, Vol. 1(1), 37–56.

Sandler,[20] analyzing the 1960–1992 period, found no significant correlation after 1966. In their follow-up study,[21] they found no statistically significant evidence of systematic under-contribution by NATO member states between the mid-1970s and 1994. Sandler and Murdoch[22] extended the analysis to cover each year of the 1990s and found no evidence to reject the null hypothesis of a match between defense burdens and benefit shares. These findings strengthened the view that NATO defense delivered sufficient private and impure public benefits to limit free-rider behavior through 1999, as allies appeared to bear defense burdens proportionate to their expected gains. Overall, empirical data clearly indicates that following the adoption of flexible response, no systematic exploitation of wealthier allies by poorer ones was observed within NATO.

After the Cold War, NATO's primary threat shifted from the East to new forms of conflict. The alliance responded with crisis management operations in Bosnia and Kosovo, aimed at protecting European interests and preventing conflict spillovers. The concept of "burden" gradually shifted from input-based indicators, such as defense expenditures, to output-based indicators, including military deployments and operational commitments, as well as risk-sharing metrics such as personnel casualties and national restrictions on missions.[23]

[20] Jyoti Khanna and Todd Sandler, 'NATO burden sharing: 1960–1992' (1996) *Defence and Peace Economics*, Vol. 7, 115–133.
[21] Jyoti Khanna and Todd Sandler, 'Conscription, peacekeeping and foreign assistance: NATO burden sharing in the post-Cold War era' (1997) *Defence and Peace Economics*, Vol. 8, 101–121.
[22] Todd Sandler and James C. Murdoch, 'On sharing NATO defence burdens in the 1990s and beyond' (2000) *Fiscal Studies*, Vol. 21 (3), 297–327.
[23] Marion Bogers and Robert Beeres, 'Mission Afghanistan: Who bears the heaviest burden' (2013) *Peace Economics, Peace Science and Public Policy*, Vol. 19 (3), 349–367 ;
Keith Hartley and Todd Sandler, 'NATO burden sharing: Past and future' (1999) *Journal of Peace Research*, Vol. 36 (6), 665–680 ;
Jyoti Khanna, Todd Sandler and Hirofumi Shimizu, 'Sharing the financial burden for UN and NATO peacekeeping, 1976–1996' (1998) *Journal of Conflict Resolution*, Vol. 42 (2), 176–195;
Jens Ringsmose, 'NATO burden sharing redux: Continuity and change after the Cold War' (2010) *Contemporary Security Policy*, Vol. 31(2), 319–338;
Rebecca Robison, 'NATO burden-sharing: A comprehensive framework for member evaluation' (2020) *Comparative Strategy*, Vol. 39 (3), 299–315;
Hirofumi Shimizu and Todd Sandler, 'Peacekeeping and burden sharing, 1994–2000' (2002) *Journal of Peace Research*, Vol. 39 (6), 651–668;
James Sperling and Mark Webber, 'NATO: From Kosovo to Kabul' (2009) *International Affairs*, Vol. 85(3), 491–511;
Benjamin Zyla, 'Who is free riding in NATO's peace operations in the 1990s?' (2016) *International Peacekeeping*, Vol. 23 (3), 416–441.

These issues of distribution of burden and fair contribution among NATO members are likely to emerge in the context of a potential European Defence Union (EDU). For analytical purposes, this study adopts a hypothetical scenario of an EDU—an official, institutionalized military alliance providing a framework of collective defense and security for all participating EU member states. Fontanel and Smith[24] were among the first to argue that an EDU could achieve significant economies of scale through the creation of joint armed forces, as opposed to the mere aggregation of national armies. The economic dimensions of European defense integration have since been explored by Guyot and Vranceanu,[25] Wolf and Zycher,[26] and Foucault.[27] Nevertheless, the development of an EDU must contend with key challenges, such as fair cost distribution and the risk of free-rider behavior.[28]

Within the EU, the issue of burden sharing has been examined by Kollias,[29] who analyzed the behavior of the EU-15 states regarding their contribution to collective military power, using 2001 data. He concluded that France, Greece, Italy, and the UK would contribute more than the benefits they would receive, while the remaining member states would contribute less relative to their expected gains. To update these findings, Beeres and Bollen[30] analyzed the period from 2006 to 2013 across an enlarged EU comprising 26 member states. Despite the temporal and geographic expansion, and the inclusion of additional benefit indicators, the key findings of Kollias were confirmed. France, Italy, the UK, and now Germany was shown to bear a disproportionately large share of the common defense burden. Conversely, the

[24] Jacques Fontanel and Ron Smith, 'A European defence union?' (1991) *Economic Policy*, Vol. 13 (3), 393–425.
[25] Marc Guyot and Radu Vranceanu, 'European defence: The cost of partial integration' (2001) *Defence and Peace Economics*, Vol. 12 (2), 157–174.
[26] Charles Wolf and Benjamin Zycher, 'European Military Prospects, Economic Constraints, and Rapid Reaction Force' (2001) *RAND Publications*.
[27] Martial Foucault, 'Does the European defence burden sharing matter?' (2008) in *War, Peace and Security*, pp. 297–314, Emerald Group Publishing.
[28] Keith Hartley, 'The future of European defence policy: An economic perspective' (2003) *Defence and Peace Economics*, Vol. 14 (2), 107–115.
[29] Christos Kollias, 'A preliminary investigation of the burden sharing aspects of a European Union common defence policy' *Defence and Peace Economics*, Vol. 19 (4), 253-263.
[30] Robert Beeres and Myriame Bollen, 'Towards a European Defence Union? Military burden sharing in the European Union 2006–2013' (2017) *Athens Journal of Social Sciences*, Vol. 4 (2), 147–160.

remaining member states—including Greece—continued to contribute less than the benefits they would likely derive from the EU's collective military strength.

2. Methodology

The analysis is grounded in the theoretical framework of public goods. The central hypothesis is that common European defense bears the characteristics of public good, governed by the principles of non-excludability and non-rivalry in consumption. Specifically, the security provided by a joint military force covers all alliance members, regardless of their individual contributions, and no member state can be excluded from its benefits, even if it does not contribute equally to its provision. This condition gives rise to the potential emergence of the 'free rider' phenomenon, where a state may avoid fair participation in the costs, expecting that others will shoulder the related obligations.

The analysis focuses on the period from 2014 to 2023. This period was selected due to historical, political, and institutional developments that influenced the level and distribution of defense spending in the EU.

- Post-2014, EU countries faced significant fiscal challenges due to the consequences of the financial crisis and subsequent fiscal consolidation,[31] which impacted member states' ability to finance defense and led to a reevaluation of burden-sharing mechanisms.
- Major geopolitical events such as the annexation of Crimea in 2014 and the subsequent revision of European security policy accelerated the need for redistribution of defense burdens.
- By 2014, all member states, including Croatia, had joined the EU's common defense architecture, enhancing collective response capacity.
- The United Kingdom's exit from the EU, completed in 2020, introduced new challenges to the balance of defense cost distribution among member states. The selected time frame allows analysis of both the pre- and post-Brexit periods.

[31] European Commission, 'Economic and Financial Affairs Annual Report' (2014) *European Commission*, Brussels.

- Russia's invasion of Ukraine in 2022 served as the most recent and significant catalyst for changes in defense burden distribution, as it led to sharp increases in defense spending and a redefinition of collective strategies.[32]
- Institutional developments such as the establishment of PESCO in 2017 strengthened defense cooperation.[33]
- The period spans two EU Multiannual Financial Frameworks (2014–2020 and 2021–2027), within which key defense funding tools were developed.[34]
- Finland and Sweden's accession to NATO in 2023 and 2024, respectively, has reshaped Europe's security environment and is expected to impact intra-EU burden-sharing dynamics.[35]

The study is methodologically grounded in the burden-sharing model initially developed by Sandler and Forbes[36] and subsequently employed by scholars such as Kollias,[37] and Beeres and Bollen.[38] This model compares each ally's share of total defense expenditures with the benefits it derives from alliance membership. For the purposes of the present quantitative analysis, geopolitical and social variables that influence alliance formation are treated as constant. The study does not aim to explain the international or political processes that led to renewed debates on European defence integration but rather focuses on the distribution of costs and benefits among EU member states, conditional upon the existence of a collective European defence arrangement. This assumption allows the analysis to isolate patterns of burden sharing within a hypothetical European Defence Union.

At the initial stage of the analysis, a burden-sharing measure is applied, whereby each member state's contribution to collective defense is calculated as its share of the total aggregated defense budget of the Union. This leads to the construction of a Burden Sharing Index (BSI), in which each country's defense expenditure is expressed as the

[32] European Defence Agency, 'Annual report on defence spending' (2023) *EDA*, Brussels.
[33] European External Action Service, 'Permanent Structured Cooperation (PESCO): Deepening defence cooperation among member states' (2024).
[34] European Parliament, 'Multiannual financial framework 2021–2027 and defence funding' (2021) *European Parliament*, Brussels.
[35] NATO, 'The Secretary General's annual report' (2024).
[36] Sandler and Forbes, (no 16) 430
[37] Kollias (no 29) 258
[38] Beeres and Bollen (no 30) 152

ratio of its national defense spending to the sum of all EU member states' defense budgets—considered the total cost of Europe's common defense capabilities. Clearly, the military strength and operational capacity of a potential EDU are understood as the aggregate of the national military forces and capabilities of the participating member states. However, it should be noted that the creation of such a Union would likely generate significant economies of scale through the harmonization and standardization of armaments, the pooling of resources, and specialization among allies. This framework enables meaningful comparisons of defense expenditure across member states.

Subsequently, the share of each EU member state in the total cost of common European defence spending is compared to the corresponding benefits derived from participation in a hypothetical European Defence Union. To quantify these benefits, it is necessary to identify the core variables that represent the value generated by the existence and operation of a collective defense alliance. The main benefits a member state receives from such participation include the protection of its territory, population, and economic wealth. These benefits are quantified using three indicators: (a) the country's share of total EU GDP, (b) its share of the EU's total land area, and (c) its share of the EU's total population. Since it is not known which security dimensions (land area, population, or GDP) are considered more important by each country, the assumption is made that all three dimensions carry equal weight. This equal-weight assumption follows established practice in the empirical literature on alliance burden sharing. As originally argued by Sandler and Forbes and subsequently adopted by Kollias as well as Beeres and Bollen, the absence of observable national utility functions necessitates the use of a simple arithmetic mean across benefit dimensions. While alternative weighting schemes could be employed, the selected approach ensures transparency, comparability across countries, and consistency with prior empirical studies. Therefore, the three percentage shares are added and divided by three to produce a simple arithmetic mean, which is defined as the Average Benefit Share (ABS). The ABS reflects the proportion of benefits each member state derives from its participation in the European Defence Union. Accordingly, the function representing the ABS is formulated as: ABS = f (Area, Population, GDP).

The comparison between the BSI and the ABS allows for the estimation of each state's net gains or losses from participating in the alliance. When a state's ABS exceeds its corresponding BSI, a positive Net Benefit (NB > 0) arises, potentially indicating free-rider behavior within the context of collective action. Conversely, when a state's ABS is lower than its BSI, the country appears to be bearing a disproportionate burden relative to the benefits it receives, resulting in a negative Net Benefit (NB < 0) and classifying it as an over-contributor.

However, it should be emphasized that comparisons between ABS and BSI assume that the alliance operates as a pure public good. In practice, though, each member state may also receive non-quantifiable private benefits from its participation. For example, in the hypothetical case of an EDU, Finland might derive particularly high geostrategic benefits due to its proximity to Russia and the heightened threat it faces—especially following the 2022 invasion of Ukraine. A European framework for collective deterrence and military support would significantly strengthen Finland's position against the Russian threat, effectively acting as a force multiplier. Although all members benefit from collective defense, Finland would likely gain more in strategic terms than countries such as Portugal or Luxembourg.

To expand the analysis further, an additional dimension related to the international economy is incorporated into the variables determining the benefits of the alliance's collective military capabilities. This approach assumes that globalization has intensified interdependence among national economies and that the external sector is a key driver of economic growth at the national level. In particular, the military capabilities of the alliance are not limited to protecting national resources and wealth within borders but also play a crucial role in safeguarding the flow of trade revenues and material resources entering and exiting the EU. Thus, military presence and operations at the international level constitute a core mechanism for protecting the alliance's external economic interests. To quantify this dimension, the variables of imports and exports for each country are added to the analytical framework. Accordingly, the ABS function is redefined as follows: ABS=f (Area, Population, GDP, Imports, Exports). For each member state, the ABS is recalculated as the arithmetic mean of its percentage share across the five selected variables.

Next, to further broaden the analysis and integrate the dimension of security threats affecting national interests, it becomes necessary to assess the level of protection against exposure to various types of threats. This more holistic approach includes, among others, terrorism—an aspect which, according to Beeres and Bollen,[39] constitutes a significant additional benefit of participating in a common defense effort, as it may reduce exposure to terrorist activity. Terrorism was first incorporated as a variable in the cost-benefit analysis of alliances by Sandler and Shimizu.[40] Modern security threats also encompass a broad range of internal challenges that can undermine the stability and functionality of the state. In this context, Armed Forces do not serve solely in national defense but also play a vital role in maintaining social cohesion and public order, acting as pillars of institutional security during periods of crisis or hybrid threats. Especially during times of intense migration pressure or increased cross-border criminal activity, the Armed Forces play a critical role in enhancing national security, contributing to the deterrence of external threats and the protection of territorial sovereignty. It should be noted that member states with external EU borders or proximity to geopolitically fragile regions face structurally higher security risks, generating positive security externalities for the rest of the Union. Countries such as Greece, Poland, and the Baltic states bear a disproportionate share of frontline security responsibilities, while the stabilizing effects extend beyond their national borders. This asymmetry is partly internalized in the present framework through the inclusion of the Security Apparatus Index in the ABS calculation, allowing higher threat exposure to translate into higher estimated benefits.

In this context, the 'Security Apparatus' indicator from the Fund for Peace[41] — a component of the Fragile States Index (FSI) — is utilized. This index reflects each state's level of exposure to security threats, considering factors such as bombings, armed attacks, conflict-related fatalities, as well as activities related to organized crime and terrorism, thus capturing the overall pressure exerted on national security. The index operates on a scale from 0 to 10, where 0 denotes the absence of security threats, and 10 indicates the highest possible level of threat. This evaluation allows national

[39] Beeres and Bollen (30) 154
[40] Todd Sandler and Hirofumi Shimizu, 'NATO burden sharing 1999–2010: An altered alliance'.
[41] Fund for Peace, 'Fragile States Index' (2025)

security conditions to be quantified as a comparable numerical value. Given that the EU functions as a system of interdependent states, the sum of all member states' security scores is considered indicative of the Union's aggregate exposure to security threats. By normalizing each country's score as a percentage of the total, this security dimension can be incorporated into the ABS framework as a comparable proportional benefit variable, representing each state's relative exposure to the overall level of security threats within the EU. Accordingly, the ABS function is further expanded as follows: ABS=f (Area, Population, GDP, Imports, Exports, Security Threats). The ABS value for each member state is recalculated using the same methodology—by taking the arithmetic mean of the country's share across the six variables and dividing by six.

Finally, the same calculation is performed for all 28 EU member states (EU-28), i.e., as the Union existed prior to the United Kingdom's withdrawal. The purpose is to compare results between EU-27 and EU-28, to assess how Brexit affected the respective indicators. This allows for a clearer view of the UK's contribution to the overall metrics and provides a more complete picture of the consequences of its departure.

The study utilizes reliable, comparable, and longitudinal datasets covering the military, economic, demographic, and institutional dimensions of EU member states' security. The sources were selected for their transparency, international credibility, and temporal comparability. Military expenditure data was obtained from the SIPRI Military Expenditure Database,[42] in constant 2023 USD. Data on land area, population, GDP, and foreign trade was drawn from the World Bank's World Development Indicators,[43] adjusted to constant 2015 USD to eliminate inflationary distortions. For security analysis, the Security Apparatus indicator from the Fragile States Index by the Fund for Peace was used, which assesses each state's exposure to security threats, considering factors such as the presence of armed non-state actors, organized crime, and the state's capacity to exercise control over its territory.

3. Comparative Economic and Security Data in the EU

[42] SIPRI, 'Military expenditure database' (2025) *Stockholm International Peace Research Institute*.
[43] World Bank, 'World development indicators' (2025).

The quantitative representation of key indicators for EU member states during the 2014–2023 period, as shown in Table 1, highlights disparities and inequalities within the European framework. The variables examined—geographical area, population, GDP, imports, and exports—are critical indicators of national power and the degree of integration into the EU's single market. These disparities are not merely statistical. They reflect political and institutional differences, varying levels of development, degrees of economic openness, and unequal capacities to leverage EU policies.

The 27 EU member states collectively span a geographical area of approximately 4.254 million square kilometers and host an average population of 446.5 million citizens. Germany, as the most populous country (over 82.7 million people), plays a decisive role in shaping the EU's demographic profile, while smaller states such as Malta and Luxembourg have fewer than 700,000 inhabitants—indicating the coexistence of significantly unequal states within the same institutional architecture. Similarly, geographical distribution varies widely, with countries like France, Spain, and Sweden each occupying over 500,000 square kilometers, while Luxembourg and Malta occupy minimal space on the European geopolitical map.

In terms of macroeconomic performance, the average GDP of the EU member states for the years 2014 to 2023 (in constant 2015 prices) shows even greater concentration. Germany accounts for nearly one-quarter of the average total GDP of the EU-27 (€3.57 trillion), followed by France (€2.53 trillion) and Italy (€1.89 trillion), revealing a 'core-periphery' structure within the Union, where a few large countries generate most of the total economic value. This picture becomes even more pronounced when per capita figures are considered, with small countries such as Ireland and Luxembourg recording exceptionally high GDP levels—an outcome of attracting significant foreign investment, focusing on financial and technological services, and benefiting from favorable regulatory and tax frameworks. Conversely, Southeast European countries such as Bulgaria and Croatia, despite their relatively large geographical size, exhibit extremely low GDP, indicating the existence of significant developmental gaps and structural barriers to endogenous accumulation.

Table 1: The EU in Figures (2014-2023)							
M-S	Area (in '000 km^2)	Population (in million)	GDP (in biilion $,constant 2015)	Imports (in biilion $,constant 2015)	Exports (in biilion $,constant 2015)	Security Threats	MilEx (million $, constant 2023)
Austria	83,9	8,8	400,1	211,9	226,1	1,42	3.944
Belgiun	30,7	11,5	485,0	405,5	409,0	2,37	5.901
Bulgaria	111,0	6,9	55,9	38,6	37,6	4,28	1.408
Croatia	88,0	4,0	56,5	29,0	27,9	3,17	1.206
Cyprus	9,2	1,3	24,2	19,8	20,1	3,95	462
Czechia	78,9	10,6	205,4	156,5	168,2	2,57	3.902
Denmark	42,9	5,8	328,4	170,5	191,6	1,49	5.028
Estonia	45,3	1,3	26,0	20,8	20,9	2,64	834
Finland	338,4	5,5	246,8	95,4	95,0	2,00	4.300
France	549,0	67,3	2.531,3	836,9	817,8	3,13	55.148
Germany	357,6	82,7	3.577,1	1.340,8	1.547,7	2,19	53.920
Greece	132,0	10,7	201,4	76,3	70,2	4,11	6.475
Hungary	93,0	9,8	140,0	120,8	127,4	2,47	2.542
Ireland	70,3	4,9	381,3	392,8	510,9	2,31	1.224
Italy	302,1	59,9	1.894,4	534,4	578,6	4,75	32.103
Latvia	64,5	1,9	28,6	20,6	19,0	2,85	783
Lithuania	65,3	2,8	47,3	36,4	38,5	2,82	1.331
Luxembourg	2,5	0,6	65,6	108,1	129,8	1,31	405
Malta	0,3	0,5	14,1	15,3	17,3	2,93	80
Netherlands	41,5	17,3	836,3	644,5	730,1	1,95	13.084
Poland	312,7	37,6	553,1	275,4	291,5	2,22	15.867
Portugal	92,2	10,3	213,0	93,1	91,9	1,01	3.518
Romania	238,4	19,4	205,9	105,8	94,5	2,73	4.926
Slovakia	49,0	5,4	96,2	87,3	90,1	1,76	1.876
Slovenia	20,4	2,0	48,1	36,9	40,5	1,22	656
Spain	528,9	47,1	1.270,6	367,9	434,4	3,22	19.186
Sweden	506,0	10,1	534,9	232,3	251,1	2,37	6.452
TOTAL	**4.254,0**	**446,5**	**14.468,3**	**6.504,2**	**7.078,7**	**69,24**	**246.561**

Source: World Bank (Area, Population, GDP,Imports,Exports), SIPRI (MilEx), Fund for Peace (Security Threats)

The trade dimension reinforces the broader picture of inequalities within the EU. Germany leads by a wide margin in both exports and imports, highlighting the export-oriented nature of the German economy, which is based on a highly developed and globalized industrial complex. The case of Ireland is particularly noteworthy: despite its small population size, it reports exports exceeding €510 billion—an amount far surpassing even Italy's exports. In contrast, countries such as Greece, Bulgaria, and Cyprus show low levels of trade openness, a feature linked to limited production scale,

small domestic markets, and relatively low technological intensity in their production structures.

The 'Security Apparatus Index' combines factors such as geopolitical stability, military risks, terrorism, energy security, and migration pressures, offering a more comprehensive picture of risk. The highest scores are recorded in countries that are either located in geopolitically unstable regions or face enduring threats at their external borders, such as Italy (4.75), Bulgaria (4.28), Greece (4.11), and Cyprus (3.95). In contrast, Central and Northern European countries such as Luxembourg (1.31), Austria (1.42), and Denmark (1.49) show low threat levels, reflecting their stable geopolitical environments and limited exposure to instability.

The total average military expenditure of the 27 EU member states during the period reaches $246.5 billion—a significant amount, albeit unevenly distributed. The absence of a unified European army, differing national strategic priorities, and disparities in resources and threats have resulted in a fragmented defense landscape. France ($55.1 billion) and Germany ($53.9 billion) consistently top the list of military expenditures within the EU-27. These two countries bear the largest defense burden, not only due to their demographic and economic weight but also because of the international roles they pursue. France invests heavily in defense due to its nuclear deterrent and global military presence. Italy ($32.1 billion) and Spain ($19.2 billion) follow, assuming a relatively significant defense role in the Mediterranean periphery. Poland ($15.8 billion), especially over the past decade, has recorded a remarkable increase in military spending—directly linked to developments in Eastern Europe and the perceived threat from Russia following the annexation of Crimea and the invasion of Ukraine. Notably, countries such as Greece ($6.5 billion) and Cyprus ($462 million), despite their comparatively small) size, exhibit proportionally high military expenditures relative to their GDP and population. Greece has consistently maintained high defense spending due to its geopolitical rivalry with Turkey, unresolved issues in the Aegean, and intensifying pressure at its borders. On the other hand, countries like Luxembourg ($405 million) and Ireland ($1.2 billion) deliberately maintain a limited defense footprint.

In summary, the analysis of the data presented in Table 1 confirms the heterogeneous nature of the European Union—not only in terms of the size and economic weight of its member states but also in the way they perceive and address geostrategic challenges. These structural differences are critical in understanding the (non-)uniformity of member state approaches to economic policy, foreign policy, and security.

4. Burden Sharing in the EU-27

The hypothetical establishment of the EDU creates the need to assess the balance between the benefits each member state enjoys and the financial burden it is required to bear. In this context, Table 2 presents the ABS and the BSI, with the aim of calculating the NB, that is, the difference between the two. Each column displays the percentage share of each country relative to the EU total for the corresponding variable. For example, Italy's share in the EU's total land area amounts to 7.10%, in total population to 13.42%, and in total GDP to 13.09%. The ABS, which is the average of these three variables, stands at 11.21%. Meanwhile, the BSI—reflecting the country's relative contribution to the cost of common European defense through its military expenditures—is 13.02%.

Comparison of the two indices reveals significant discrepancies in the symmetry between benefit and burden. Specifically, 20 countries show a positive NB, indicating that they benefit from collective defense to a greater extent than their proportional contribution. Typical examples include Sweden (3.34), Spain (2.80), Finland (1.89), Romania (1.80), and Ireland (1.30). These countries would receive considerable benefits in terms of territorial and population security without assuming a corresponding economic burden.

In contrast, seven EU member states record a negative NB. In particular, the countries exhibiting this condition of over-contribution are Belgium (-0.18), Denmark (-0.51), France (-7.21), Germany (-4.65), Greece (-0.33), Italy (-1.81), and the Netherlands (-1.76). These negative values indicate that these states would bear a disproportionate burden relative to the expected benefits from a collective defense system. This suggests that such countries would be more heavily impacted by the

implementation of a joint European defense mechanism, given their current economic, demographic, and geographic characteristics. France and Germany, with BSIs exceeding 21%, shoulder the most disproportionate share of the cost due to their high levels of military spending. This situation creates conditions of unequal burden, calling into question the sustainability of a collective defense policy without accompanying balancing mechanisms.

Table 2: Contribution to Burden and Benefits from an EDU (Variables: Area,Population, GDP)

M-S	Area (Percentage Share)	Population (Percentage Share)	GDP (Percentage Share)	ABS	BSI	NB
Austria	1,97	1,98	2,77	2,24	1,60	0,64
Belgiun	0,72	2,57	3,35	2,21	2,39	-0,18
Bulgaria	2,61	1,56	0,39	1,52	0,57	0,95
Croatia	2,07	0,89	0,39	1,12	0,49	0,63
Cyprus	0,22	0,29	0,17	0,22	0,19	0,04
Czechia	1,85	2,38	1,42	1,88	1,58	0,30
Denmark	1,01	1,30	2,27	1,53	2,04	-0,51
Estonia	1,07	0,30	0,18	0,51	0,34	0,18
Finland	7,96	1,24	1,71	3,63	1,74	1,89
France	12,91	15,07	17,50	15,16	22,37	-7,21
Germany	8,41	18,52	24,72	17,22	21,87	-4,65
Greece	3,10	2,39	1,39	2,30	2,63	-0,33
Hungary	2,19	2,18	0,97	1,78	1,03	0,75
Ireland	1,65	1,10	2,64	1,80	0,50	1,30
Italy	7,10	13,42	13,09	11,21	13,02	-1,81
Latvia	1,52	0,43	0,20	0,72	0,32	0,40
Lithuania	1,53	0,64	0,33	0,83	0,54	0,29
Luxembourg	0,06	0,14	0,45	0,22	0,16	0,05
Malta	0,01	0,11	0,10	0,07	0,03	0,04
Netherlands	0,98	3,88	5,78	3,54	5,31	-1,76
Poland	7,35	8,43	3,82	6,53	6,44	0,10
Portugal	2,17	2,32	1,47	1,99	1,43	0,56
Romania	5,60	4,35	1,42	3,79	2,00	1,80
Slovakia	1,15	1,22	0,67	1,01	0,76	0,25
Slovenia	0,48	0,47	0,33	0,43	0,27	0,16
Spain	12,43	10,54	8,78	10,59	7,78	2,80
Sweden	11,89	2,28	3,70	5,96	2,62	3,34

Advancing the analysis to the next stage, the dimension of protecting each member state's international economic interests is incorporated into the benefit calculation, by adding international trade figures—namely, imports and exports.

The evaluation of the findings in Table 3 reveals that six member states display a negative NB, indicating over-contribution to the collective European defense system. These countries are required to bear a greater burden than is proportional to their relative size and role in the European economy. France, with an NB of -8.39, emerges as the most burdened country, having an exceptionally high BSI (22.37). Germany, despite being the Union's largest economy, also exhibits a notable imbalance (NB -3.04), as does Italy (NB -3.02), despite its large trade volume and population factor. This negative net contribution is not limited to large economies; it also extends to countries such as Poland (NB -0.84) and Greece (NB -0.82). Although Poland records high shares in population (8.43%) and land area (7.35%), it does not receive a proportional benefit, as its GDP and trade volume lag their respective EU averages. Denmark, with a marginally negative NB (-0.06), sits at the threshold between benefit and burden. Its high trade activity (exports 2.71%, imports 2.62%) and strong economy place it among the EU's most active trading nations, yet these are not sufficient to offset its relative contribution based on a BSI of 2.04.

In contrast, 21 member states record a positive NB, reflecting under-contribution, that is, a benefit received greater than the respective share in the collective burden. Particularly notable is the case of Ireland (NB 3.23), which shows the highest positive deviation. This outcome is primarily explained by Ireland's exceptionally high involvement in international trade: its imports and exports amount to 6.04% and 7.22% of the EU-27 total, respectively—figures that far exceed its demographic (1.10%) and geographic (1.65%) weight. The strong outward orientation of the Irish economy, combined with its relatively low weight in other variables, amplifies the country's net gains from European defense integration. Similarly, countries such as Sweden (2.38), Belgium (1.34), Spain (1.02), Austria (1.03), Finland (1.00), and Romania (0.87) show positive NB values, while smaller economies such as Luxembourg (0.67) and Malta (0.11) also benefit.

It is worth noting that compared to the initial benefit calculation—which was based solely on land area, population, and GDP—the expanded analysis incorporating international trade dimensions (imports and exports) results in changes in the relative positions of certain member states. In particular, the Netherlands, due to its highly active external trade (imports 9.91%, exports 10.31% of the EU-27 total), as well as

Belgium, now rank among the countries with positive NB. Conversely, Poland, which in the previous model was among the net beneficiaries, now records a negative NB, placing it among the countries that over-contribute to the European defense system.

Table 3: Contribution to Burden and Benefits from an EDU (Variables: Area,Population, GDP, Imports, Exports)

M-S	Area (Percentage Share)	Population (Percentage Share)	GDP (Percentage Share)	Imports (Percentage Share)	Exports (Percentage Share)	ABS	BSI	NB
Austria	1,97	1,98	2,77	3,26	3,19	2,63	1,60	1,03
Belgiun	0,72	2,57	3,35	6,23	5,78	3,73	2,39	1,34
Bulgaria	2,61	1,56	0,39	0,59	0,53	1,14	0,57	0,56
Croatia	2,07	0,89	0,39	0,45	0,40	0,84	0,49	0,35
Cyprus	0,22	0,29	0,17	0,31	0,28	0,25	0,19	0,06
Czechia	1,85	2,38	1,42	2,41	2,38	2,09	1,58	0,51
Denmark	1,01	1,30	2,27	2,62	2,71	1,98	2,04	-0,06
Estonia	1,07	0,30	0,18	0,32	0,30	0,43	0,34	0,09
Finland	7,96	1,24	1,71	1,47	1,34	2,74	1,74	1,00
France	12,91	15,07	17,50	12,87	11,55	13,98	22,37	-8,39
Germany	8,41	18,52	24,72	20,61	21,86	18,83	21,87	-3,04
Greece	3,10	2,39	1,39	1,17	0,99	1,81	2,63	-0,82
Hungary	2,19	2,18	0,97	1,86	1,80	1,80	1,03	0,77
Ireland	1,65	1,10	2,64	6,04	7,22	3,73	0,50	3,23
Italy	7,10	13,42	13,09	8,22	8,17	10,00	13,02	-3,02
Latvia	1,52	0,43	0,20	0,32	0,27	0,55	0,32	0,23
Lithuania	1,53	0,64	0,33	0,56	0,54	0,72	0,54	0,18
Luxembourg	0,06	0,14	0,45	1,66	1,83	0,83	0,16	0,67
Malta	0,01	0,11	0,10	0,24	0,24	0,14	0,03	0,11
Netherlands	0,98	3,88	5,78	9,91	10,31	6,17	5,31	0,87
Poland	7,35	8,43	3,82	4,24	4,12	5,59	6,44	-0,84
Portugal	2,17	2,32	1,47	1,43	1,30	1,74	1,43	0,31
Romania	5,60	4,35	1,42	1,63	1,34	2,87	2,00	0,87
Slovakia	1,15	1,22	0,67	1,34	1,27	1,13	0,76	0,37
Slovenia	0,48	0,47	0,33	0,57	0,57	0,48	0,27	0,22
Spain	12,43	10,54	8,78	6,12	6,14	8,80	7,78	1,02
Sweden	11,89	2,28	3,70	3,57	3,55	5,00	2,62	2,38

Finally, by further expanding the analysis, the security dimension is incorporated in Table 4, aiming to provide a more multidimensional representation of each member state's contribution and benefits within the European collective defense system. The integration of the security threat level index does not substantially alter the classification of countries as over- or under-contributors. However, it highlights states with limited economic power but under significant geopolitical pressure.

The analysis of the findings in Table 4 reveals that six countries show negative NB values, indicating over-contribution to the European collective system. The most prominent cases are France (-9.96) and Germany (-5.65), which bear a heavy burden. In these cases, the security threat index is relatively low, resulting in minimal additional benefit from including the security variable in the ABS calculation. In short, because these countries do not face a high level of threats, the new variable does not significantly improve their negative standing. Conversely, in the case of Greece (-0.13), which records higher values in the security threat index, the inclusion of this variable notably reduces the negative NB.

In contrast, 21 member states appear as under-contributors, meaning they derive more benefits than their corresponding share of the burden. Among them, countries such as Ireland (NB 3.17), Sweden (NB 2.12), Bulgaria (NB 1.41), and Hungary (NB 1.06) stand out, as their net benefits significantly exceed their proportional contribution. The inclusion of the security index particularly strengthens the position of geopolitically exposed countries such as Cyprus, Croatia, Latvia, and Lithuania, whose NB increases notably due to their proximity to sources of instability and threats.

Table 4: Contribution to Burden and Benefits from an EDU (Variables: Area,Population, GDP, Imports, Exports, Security Threats)

M-S	Area (Percentage Share)	Population (Percentage Share)	GDP (Percentage Share)	Imports (Percentage Share)	Exports (Percentage Share)	Security Threats (Percentage Share)	ABS	BSI	NB
Austria	1,97	1,98	2,77	3,26	3,19	2,05	2,54	1,60	0,94
Belgiun	0,72	2,57	3,35	6,23	5,78	3,42	3,68	2,39	1,29
Bulgaria	2,61	1,56	0,39	0,59	0,53	6,18	1,98	0,57	1,41
Croatia	2,07	0,89	0,39	0,45	0,40	4,58	1,46	0,49	0,97
Cyprus	0,22	0,29	0,17	0,31	0,28	5,70	1,16	0,19	0,97
Czechia	1,85	2,38	1,42	2,41	2,38	3,71	2,36	1,58	0,78
Denmark	1,01	1,30	2,27	2,62	2,71	2,15	2,01	2,04	-0,03
Estonia	1,07	0,30	0,18	0,32	0,30	3,81	1,00	0,34	0,66
Finland	7,96	1,24	1,71	1,47	1,34	2,89	2,77	1,74	1,02
France	12,91	15,07	17,50	12,87	11,55	4,52	12,40	22,37	-9,96
Germany	8,41	18,52	24,72	20,61	21,86	3,16	16,22	21,87	-5,65
Greece	3,10	2,39	1,39	1,17	0,99	5,94	2,50	2,63	-0,13
Hungary	2,19	2,18	0,97	1,86	1,80	3,57	2,09	1,03	1,06
Ireland	1,65	1,10	2,64	6,04	7,22	3,34	3,66	0,50	3,17
Italy	7,10	13,42	13,09	8,22	8,17	6,86	9,48	13,02	-3,54
Latvia	1,52	0,43	0,20	0,32	0,27	4,12	1,14	0,32	0,82
Lithuania	1,53	0,64	0,33	0,56	0,54	4,07	1,28	0,54	0,74
Luxembourg	0,06	0,14	0,45	1,66	1,83	1,89	1,01	0,16	0,84
Malta	0,01	0,11	0,10	0,24	0,24	4,23	0,82	0,03	0,79
Netherlands	0,98	3,88	5,78	9,91	10,31	2,82	5,61	5,31	0,31
Poland	7,35	8,43	3,82	4,24	4,12	3,21	5,19	6,44	-1,24
Portugal	2,17	2,32	1,47	1,43	1,30	1,46	1,69	1,43	0,26
Romania	5,60	4,35	1,42	1,63	1,34	3,94	3,05	2,00	1,05
Slovakia	1,15	1,22	0,67	1,34	1,27	2,54	1,37	0,76	0,60
Slovenia	0,48	0,47	0,33	0,57	0,57	1,76	0,70	0,27	0,43
Spain	12,43	10,54	8,78	6,12	6,14	4,65	8,11	7,78	0,33
Sweden	11,89	2,28	3,70	3,57	3,55	3,42	4,74	2,62	2,12

5. Comparison of Burden Sharing in the EU-27 and EU-28

The following analysis is based on Table 5, which presents the burden-sharing distribution among EU member states, expanding the sample to include 28 countries by incorporating the United Kingdom. The inclusion of the United Kingdom allows for a comparison with the EU-27 (see Table 4) and offers an estimate of its contribution to the overall balance of costs and benefits within the Union.

Table 5: Contribution to Burden and Benefits from an EDU-28 (Variables: Area, Population, GDP, Imports, Exports, Security Threats)

M-S	Area (Percentage Share)	Population (Percentage Share)	GDP (Percentage Share)	Imports (Percentage Share)	Exports (Percentage Share)	Security Threats (Percentage Share)	ABS	BSI	NB
Austria	1,86	1,72	2,28	2,86	2,84	1,96	2,26	1,26	0,99
Belgiun	0,68	2,24	2,77	5,47	5,14	3,28	3,26	1,89	1,38
Bulgaria	2,47	1,35	0,32	0,52	0,47	5,92	1,84	0,45	1,39
Croatia	1,96	0,78	0,32	0,39	0,35	4,39	1,36	0,39	0,98
Cyprus	0,21	0,25	0,14	0,27	0,25	5,46	1,10	0,15	0,95
Czechia	1,75	2,07	1,17	2,11	2,11	3,56	2,13	1,25	0,88
Denmark	0,95	1,13	1,87	2,30	2,41	2,06	1,79	1,61	0,18
Estonia	1,01	0,26	0,15	0,28	0,26	3,65	0,94	0,27	0,67
Finland	7,52	1,08	1,41	1,29	1,19	2,77	2,54	1,38	1,17
France	12,21	13,12	14,45	11,30	10,28	4,33	10,95	17,64	-6,70
Germany	7,95	16,12	20,42	18,10	19,45	3,03	14,18	17,25	-3,07
Greece	2,93	2,08	1,15	1,03	0,88	5,69	2,29	2,07	0,22
Hungary	2,07	1,90	0,80	1,63	1,60	3,42	1,90	0,81	1,09
Ireland	1,56	0,96	2,18	5,30	6,42	3,20	3,27	0,39	2,88
Italy	6,72	11,68	10,82	7,21	7,27	6,57	8,38	10,27	-1,89
Latvia	1,44	0,38	0,16	0,28	0,24	3,94	1,07	0,25	0,82
Lithuania	1,45	0,55	0,27	0,49	0,48	3,90	1,19	0,43	0,77
Luxembourg	0,06	0,12	0,37	1,46	1,63	1,81	0,91	0,13	0,78
Malta	0,01	0,10	0,08	0,21	0,22	4,05	0,78	0,03	0,75
Netherlands	0,92	3,37	4,78	8,70	9,18	2,70	4,94	4,19	0,76
Poland	6,95	7,33	3,16	3,72	3,66	3,07	4,65	5,08	-0,43
Portugal	2,05	2,02	1,22	1,26	1,16	1,40	1,52	1,13	0,39
Romania	5,30	3,79	1,18	1,43	1,19	3,78	2,78	1,58	1,20
Slovakia	1,09	1,06	0,55	1,18	1,13	2,43	1,24	0,60	0,64
Slovenia	0,46	0,41	0,27	0,50	0,51	1,69	0,64	0,21	0,43
Spain	11,76	9,18	7,25	5,37	5,46	4,45	7,25	6,14	1,11
Sweden	11,25	1,98	3,05	3,14	3,16	3,28	4,31	2,06	2,25
UK	5,42	12,96	17,40	12,21	11,05	4,22	10,54	21,12	-10,58

The United Kingdom, although accounting for only 5.42% of the EU's land area, represents 12.96% of its population and 17.40% of its GDP, indicating a strong concentration of demographic and economic resources. At the same time, it accounts for 12.21% of total imports and 11.05% of total exports, confirming its role as a key player in European trade. However, its share of the 'security threats' index is just 4.22%, indicating a relatively limited level of threat in the security domain as defined within the present methodology. The United Kingdom records an ABS of 10.54 and an

exceptionally high BSI (Burden Sharing Index) of 21.12, making it the country bearing the greatest "burden" within the Union. Its NB is negative, amounting to -10.58, clearly highlighting a mismatch between its share of cost and the benefits it receives.

The exit of the United Kingdom from the EU entails both burdens and benefits. This impact is clearly illustrated in Table 6, which compares the relevant indicators of the EU-27, after the UK's withdrawal, with those of the EU-28 during its membership. Specifically, there is a deterioration in the position of most member states, particularly those that were already bearing a disproportionately high economic burden. Germany records a significant deterioration in its NB, which shifts from -3.07 in the EU-28 to -5.65 in the EU-27. France also shows further decline, with its NB increasing from -6.70 to -9.96. A similar negative change is observed in Italy, where the NB drops from -1.89 to -3.54. This downward trend is not limited to traditionally high-contributing states. Poland, which in the EU-28 had a slightly negative NB (-0.43), now records a deterioration to -1.24 in the EU-27. Conversely, very few member states marginally benefit from redistribution and improve their net benefit. Notably, Ireland consistently maintains its position as a net beneficiary, improving its NB from 2.88 to 3.17.

Particularly interesting are the cases of countries that change their participation category. Specifically, Denmark shifts from being a net beneficiary, with an NB of 0.18 in the EU-28, to a marginal net contributor, with an NB of -0.03 in the EU-27. A similar change is observed in Greece, which moves from being a net beneficiary with a score of 0.22 to a slightly net contributing country, with an NB of -0.13.

Table 6: Burden Sharing in EU-27 and EU-28 (Variables: Area,Population, GDP, Imports, Exports, Security Threats)

M-S	ABS EU-27	BSI EU-27	NB EU-27	ABS EU-28	BSI EU-28	NB EU-28
Austria	2,54	1,60	**0,94**	2,26	1,26	**0,99**
Belgiun	3,68	2,39	**1,29**	3,26	1,89	**1,38**
Bulgaria	1,98	0,57	**1,41**	1,84	0,45	**1,39**
Croatia	1,46	0,49	**0,97**	1,36	0,39	**0,98**
Cyprus	1,16	0,19	**0,97**	1,10	0,15	**0,95**
Czechia	2,36	1,58	**0,78**	2,13	1,25	**0,88**
Denmark	2,01	2,04	**-0,03**	1,79	1,61	**0,18**
Estonia	1,00	0,34	**0,66**	0,94	0,27	**0,67**
Finland	2,77	1,74	**1,02**	2,54	1,38	**1,17**
France	12,40	22,37	**-9,96**	10,95	17,64	**-6,70**
Germany	16,22	21,87	**-5,65**	14,18	17,25	**-3,07**
Greece	2,50	2,63	**-0,13**	2,29	2,07	**0,22**
Hungary	2,09	1,03	**1,06**	1,90	0,81	**1,09**
Ireland	3,66	0,50	**3,17**	3,27	0,39	**2,88**
Italy	9,48	13,02	**-3,54**	8,38	10,27	**-1,89**
Latvia	1,14	0,32	**0,82**	1,07	0,25	**0,82**
Lithuania	1,28	0,54	**0,74**	1,19	0,43	**0,77**
Luxembourg	1,01	0,16	**0,84**	0,91	0,13	**0,78**
Malta	0,82	0,03	**0,79**	0,78	0,03	**0,75**
Netherlands	5,61	5,31	**0,31**	4,94	4,19	**0,76**
Poland	5,19	6,44	**-1,24**	4,65	5,08	**-0,43**
Portugal	1,69	1,43	**0,26**	1,52	1,13	**0,39**
Romania	3,05	2,00	**1,05**	2,78	1,58	**1,20**
Slovakia	1,37	0,76	**0,60**	1,24	0,60	**0,64**
Slovenia	0,70	0,27	**0,43**	0,64	0,21	**0,43**
Spain	8,11	7,78	**0,33**	7,25	6,14	**1,11**
Sweden	4,74	2,62	**2,12**	4,31	2,06	**2,25**
UK				10,54	21,12	**-10,58**

6. Conclusions

Assuming the establishment of the EDU in the form of an institutionalized military alliance, this study highlighted the critical issue of the distribution of defense burdens—an issue that is bound to arise due to the nature of collective defense as a public good. In any common defense system, there are disincentives to balanced participation and the emergence of 'free rider' behavior, especially when security is non-rivalrous and non-excludable.

To quantitatively reflect this asymmetry, two key indicators were developed and applied: the BSI (Burden Sharing Index), which captures each state's relative

contribution to the total cost of collective defense, and the ABS (Average Benefit Share), which expresses the comparative benefits each member state derives from the existence of common military power. The ABS was constructed progressively, incorporating not only traditional variables (territory, population, GDP), but also external trade parameters (imports, exports) and the level of security threats (Security Apparatus Index).

The comparison between the two indicators for EU member states over the 2014–2023 period revealed consistent patterns of divergence. Most countries (21 out of 27) were identified as net beneficiaries, receiving more benefits than their relative share of defense costs would imply. Notable examples include Ireland, Sweden, and Bulgaria, which demonstrate under-contribution relative to the gains accrued. In contrast, six countries—France, Germany, Italy, Greece, Poland, and, to a lesser extent, Denmark—were recorded as net contributors, bearing a disproportionate share of the costs without receiving commensurate benefits.

The comparative analysis between the EU-27 and EU-28, with the inclusion of the United Kingdom, demonstrated the destabilizing effect of its departure. The UK's contribution—as one of the EU's most militarily and economically powerful countries—functioned as a 'balancing mechanism' in the overall burden-benefit equation. After Brexit, the financial burden further shifted to countries like Germany and France, exacerbating existing imbalances.

These findings underscore the need for the development of compensatory mechanisms, flexible contribution schemes, and differentiated obligations, in order to avoid discouraging participation by states that shoulder a greater share of the burden. As the EU moves toward greater strategic autonomy and the potential establishment of a permanent joint military capability, it is essential to ensure both the effectiveness and institutional fairness of the collective security system.

Finally, it should be emphasized that any prospective European Defence Union is not merely a technical or economic project but also a profoundly political one. Effective burden sharing presupposes a sufficient degree of alignment in foreign policy orientations, strategic cultures, and national interests among participating states. While the present study focuses on the quantitative distribution of costs and benefits, the

political feasibility of a collective defence arrangement remains a necessary precondition for its implementation.

Bibliography

Beeres, R. and Bollen, M., 'Towards a European Defence Union? Military burden sharing in the European Union 2006–2013' (2017) *Athens Journal of Social Sciences*, Vol. 4(2), 147–160.

Bogers, M., and Beeres, R., 'Mission Afghanistan: Who bears the heaviest burden' (2013) *Peace Economics, Peace Science and Public Policy*, Vol. 19(3), 349–367.

Buti, M., and Papakonstantinou, G., 'European public goods: How can we supply more?' (2022) *LEAP Policy Brief*, Luiss School of European Political Economy.

Draghi, M., 'The future of European competitiveness – Part B: In-depth analysis and recommendations' (2024) *European Commission*.

European Commission, 'Economic and Financial Affairs Annual Report' (2014) *European Commission*, Brussels.

European Defence Agency, 'Annual report on defence spending' (2023) *EDA*, Brussels.

European External Action Service, 'Permanent Structured Cooperation (PESCO): Deepening defence cooperation among member states' (2024).

European Parliament, 'Multiannual financial framework 2021–2027 and defence funding' (2021) *European Parliament*, Brussels.

Felbermayr, G., and Pekanov, A., 'Pan-European public goods: Rationale, financing and governance' (2024) *European Commission*.

Fontanel, J., and Smith, R., 'A European defence union?' (1991) *Economic Policy*, Vol. 13(3), 393–425.

Foucault, M., 'Does the European defence burden sharing matter?' (2008) in *War, Peace and Security*, pp. 297–314, Emerald Group Publishing.

Fund for Peace, 'Fragile States Index' (2025) https://fragilestatesindex.org/global-data/

Guyot, M., and Vranceanu, R., 'European defence: The cost of partial integration' (2001) *Defence and Peace Economics*, Vol. 12(2), 157–174.

Hansen, L., Murdoch, J. C., and Sandler, T., 'On distinguishing the behavior of nuclear and non-nuclear allies in NATO' (1990) *Defence Economics*, Vol. 1(1), 37–56.

Hartley, K., 'The future of European defence policy: An economic perspective' (2003) *Defence and Peace Economics*, Vol. 14(2), 107–115.

Hartley, K., and Sandler, T., 'NATO burden sharing: Past and future' (1999) *Journal of Peace Research*, Vol. 36(6), 665–680.

Khanna, J., and Sandler, T., 'NATO burden sharing: 1960–1992' (1996) *Defence and Peace Economics*, Vol. 7, 115–133.

Khanna, J., and Sandler, T., 'Conscription, peacekeeping and foreign assistance: NATO burden sharing in the post-Cold War era' (1997) *Defence and Peace Economics*, Vol. 8, 101–121.

Khanna, J., Sandler, T., and Shimizu, H., 'Sharing the financial burden for UN and NATO peacekeeping, 1976–1996' (1998) *Journal of Conflict Resolution*, Vol. 42(2), 176–195.

Kollias, C., 'A preliminary investigation of the burden sharing aspects of a European Union common defence policy' (2008) *Defence and Peace Economics*, Vol. 19(4), 253–263.

Lazarou, E., and Stanicek, B., 'Mapping threats to peace and democracy worldwide' (2024) *European Parliamentary Research Service*.

McGuire, M., and Groth, C., 'A method for identifying the public good allocation process within a group' (1985) *Quarterly Journal of Economics*, Vol. 99(4), 915–934.

Murdoch, J. C., and Sandler, T., 'Complementarity, free riding and the military expenditures of NATO allies' (1984) *Journal of Public Economics*, Vol. 25(1), 83–101.

NATO, 'The Secretary General's annual report' (2024).

Niinistö, S., 'Safer together: Strengthening Europe's civilian and military preparedness and readiness' (2024) *European Council*.

Olson, M., and Zeckhauser, R., 'An economic theory of alliances' (1966) *The Review of Economics and Statistics*, Vol. 48(3), 266–279.

Oneal, J. R., and Elrod, M., 'NATO burden sharing and the forces of change' (1989) *International Studies Quarterly*, Vol. 33(4), 435–456.

Ringsmose, J., 'NATO burden sharing redux: Continuity and change after the Cold War' (2010) *Contemporary Security Policy*, Vol. 31(2), 319–338.

Robison, R., 'NATO burden-sharing: A comprehensive framework for member evaluation' (2020) *Comparative Strategy*, Vol. 39(3), 299–315.

Sandler, T., 'Impurity of defense: An application to the economics of alliances' (1977) *Kyklos*, Vol. 30(3), 443–460.

Sandler, T., and Forbes, J. F., 'Burden sharing, strategy, and the design of NATO' (1980) *Economic Inquiry*, Vol. 18(3), 425–444.

Sandler, T., and Murdoch, J., 'Nash–Cournot or Lindahl behavior? An empirical test for the NATO allies' (1990) *Quarterly Journal of Economics*, Vol. 105(4), 875–894.

Sandler, T., and Murdoch, J., 'On sharing NATO defence burdens in the 1990s and beyond' (2000) *Fiscal Studies*, Vol. 21(3), 297–327.

Sandler, T., and Shimizu, H., 'NATO burden sharing 1999–2010: An altered alliance' (2014) *Foreign Policy Analysis*, Vol. 10(1), 43–60.

Shimizu, H., and Sandler, T., 'Peacekeeping and burden sharing, 1994–2000' (2002) *Journal of Peace Research*, Vol. 39(6), 651–668.

SIPRI, 'Military expenditure database' (2025) *Stockholm International Peace Research Institute*. https://www.sipri.org/databases/milex

Sperling, J., and Webber, M., 'NATO: From Kosovo to Kabul' (2009) *International Affairs*, Vol. 85(3), 491–511.

van Ypersele de Strihou, J., 'Sharing the defence burden among Western allies' (1967) *Review of Economics and Statistics*, Vol. 49, 527–536.

von der Leyen, U., 'Europe's choice: Political guidelines for the next European Commission 2024–2029' (2024) *European Commission*.

Wolf, C., and Zycher, B., 'European Military Prospects, Economic Constraints, and Rapid Reaction Force' (2001) *RAND Publications*.

World Bank, 'World development indicators' (2025) https://databank.worldbank.org/source/world-development-indicators

Zyla, B., 'Who is free-riding in NATO's peace operations in the 1990s?' (2016) *International Peacekeeping*, Vol. 23(3), 416–441.

Volume 2, Issue 2

Narratives of Maritime Sovereignty: The Mavi Vatan Doctrine

THEODOR SKARVELIS[1]

Abstract

Amid escalating regional instability, the Eastern Mediterranean has emerged as a geopolitical flashpoint, where doctrines of sovereignty and maritime strategy are reshaping the region. This paper investigates Türkiye's *Mavi Vatan* (Blue Homeland) doctrine as a case study of identity-driven geopolitics, where the evolving nature of regional security is marked by multipolarity and contested legality. Developed by Turkish admirals, *Mavi Vatan* projects a maritime geostrategic vision that challenges prevailing international norms, such as UNCLOS, and responds to a growing sense of Türkiye's regional encirclement. This paper utilises the theoretical framework of critical geopolitics, draws on ten interviews with Turkish Professors, and conducts discourse analysis informed by Critical Discourse Analysis (CDA) principles to examine the narratives that underpin *Mavi Vatan*. It examines the doctrine's key narrative strands: the reconstruction of Turkish national identity, the portrayal of Türkiye as a maritime nation, and narratives of historical legacy. Although Blue Homeland is not formally adopted, it has influenced Turkish Foreign Policy (TFP), as seen in the 2019 Turkish-Libyan Memorandum of Understanding (MoU). The political and economic context is also provided to explain the doctrine's rise.

These narratives are situated in the broader Eastern Mediterranean, where diplomatic norms and multilateral trust are increasingly eroded. This paper argues that *Mavi Vatan* exemplifies how emerging regional powers resort to identity-driven doctrines to assert sovereignty, build domestic consensus, and legitimise regional assertiveness. In doing so, Türkiye simultaneously solidifies its claims in the Aegean and the Eastern Mediterranean. By unpacking *Mavi Vatan's* symbolic, historical, political, economic and ideological underpinnings, this study contributes to a deeper understanding of the interplay between identity and geopolitics in Turkish maritime strategy. Drawing on interviews with key academics and secondary sources, contrasting narratives have

[1] MA in International Relations (Geopolitics and Connectivity track), University of Groningen.

emerged regarding *Mavi Vatan's* historical roots and the politics of identity. The study acknowledges certain limitations, including the reliance on qualitative analysis and a limited number of interviews. Nonetheless, the research bridged theoretical insights with empirical analysis, resulting in a deeper understanding of the complexities inherent in Türkiye's maritime ambitions and identity-driven geopolitics.

Keywords

Blue Homeland, Maritime Geopolitics, Eastern Mediterranean, Turkish Foreign Policy

Introduction

The Eastern Mediterranean's importance is timeless, as it connects Europe, Asia and Africa. Throughout history, countless battles have been fought to control it. Empires such as the Roman, Byzantine and Ottoman reigned supreme in the region. Historically, disputes between states concerned mainly territorial issues, with land sovereignty at stake. However, with the rise of technology and global connectivity, new maritime interstate problems emerged over the control of marine resources and trade routes. To address these differences, the United Nations Convention on the Law of the Sea (UNCLOS) was adopted in 1982, introducing new maritime concepts, including the Exclusive Economic Zone (EEZ). Before UNCLOS, territorial waters were defined as three nautical miles from the shore based on the cannon shot rule.[2]

A prime example of maritime disputes in the Eastern Mediterranean is the Greco-Turkish conflict in the Aegean Sea. The differences range from the role of the Greek islands near the Turkish mainland in the drawing of the maritime boundary to the ownership of certain islets. Each country claims overlapping maritime spaces, with Türkiye not being a signatory to UNCLOS and selectively evoking international customary law. Turkish maritime claims are unofficially based on the *Mavi Vatan* doctrine, which means Blue Homeland. This doctrine was developed by admirals of the

[2] Joanna Mossop, 'Maritime Security and the Law of the Sea' in Ruxandra-Laura Boşilcă et al. (eds), Routledge *Handbook of Maritime Security* (London: Routledge, 2022), https://doi.org/10.4324/9781003001324 90.

Turkish Navy, most prominently the retired Admiral Cem Gürdeniz and retired Admiral Cihat Yaycı.

This naval dogma holds that Türkiye requires a strong navy to safeguard its national interests and assert its rights in international waters. For Ankara, the mainland coastline determines the EEZ (not the islands, as per Greece and UNCLOS). Ankara believes it is entitled to a larger EEZ because it has the longest Mediterranean coastline (2820 km) and does not want to be 'encircled' by Greek territorial waters.[3] *Mavi Vatan*, although not officially part of the Turkish Foreign Policy (TFP) and absent from any foreign policy paper of the Turkish Foreign Ministry, has significantly influenced Turkish political and military circles. This is evident by President Erdoğan's open endorsement, underscoring the doctrine's weight in TFP.[4] Concurrently, Gürdeniz and Yaycı give regular TV interviews, write articles, books and showcase the Blue Homeland map in the Turkish media:

Map 1: The Map of '*Mavi Vatan*'[5]

[3] Republic of Türkiye Ministry of Foreign Affairs: *The Breadth of Territorial Waters*, , available at https://www.mfa.gov.tr/the-breadth-of-territorial-waters.en.mfa (last accessed 26 February 2026).
[4] Alexandros Diakopoulos et al., *Behind Turkey's 'Blue Homeland' Doctrine*, (ekathimerini.com, 19 June 2023), available at https://www.ekathimerini.com/opinion/1213618/behind-turkeys-blue-homeland-doctrine/ (last accessed 28 July 2025).
[5] Elif Erkeç, 'Reflections of Türkiye-Greece Tension in the Sea of Islands on the Eastern Mediterranean Regional Security Complex' (2023) *BRIQ Belt & Road Initiative Quarterly*, Vol. 4 (2), 24. https://www.ssoar.info/ssoar/handle/document/89599 40.

The fact that Blue Homeland is not an official policy and that the Turkish claims are not recognised renders the doctrine a narrative seeking legitimacy both within and outside Türkiye. Understanding this narrative helps clarify the contemporary significance of maritime spaces and how states seek to exert influence over them. At the same time, the doctrine showcases the increasing competition and tensions among regional powers in the Eastern Mediterranean. This study aims to explore how *Mavi Vatan* was created by analysing its narratives of historical background and the politics of identity it attempts to develop to gain legitimacy and prominence.

In English literature, the Turkish perspective is often overlooked, making it crucial to examine the case from the other side, especially the Turkish academic perspective, which remains largely unexplored. By combining existing research with new insights from interviews with Turkish academics, the paper fills gaps in the literature. It deepens scholarly understanding of this complex geopolitical phenomenon by examining its historical background(s) and the frequently overlooked politics of identity. This doctrine is a prime example of how states try to legitimise their claims and actions. Identity-based maritime doctrines, such as the Blue Homeland, challenge

the established order and complicate the search for legality, legitimacy, and stability in the Eastern Mediterranean, making their analysis crucial to understanding the new era of TFP.

Hence, the research questions are: How do competing historical narratives construct and legitimise the Blue Homeland doctrine? Two main narratives were detected, one from the doctrine's creators and the other from the interviewed academics. Secondly, how did the domestic political transformation (as of 2016) and the regional hydrocarbon competition create the conditions for *Mavi Vatan's* unofficial promotion as a state-influenced doctrine? The political events after the July 2016 failed coup attempt explain this shift. Lastly, which identity narrative surrounds the doctrine, and what role does it play? To what extent does *Mavi Vatan* function as an identity-driven tool of elite statecraft? The *Vatan* concept and its consequences on the doctrine are explored.

1. Research Design

The research follows a qualitative methodology based on a literature review, including primary and secondary analyses, evaluations, and the synthesis of the existing published bibliography. The primary data were collected through 10 semi-structured interviews with key academics in Türkiye, conducted as part of my master's thesis and my internship as an Academic Assistant at Istanbul Kültür University. Even though most participants had no concerns about anonymity, their names are not disclosed, and all participants are pseudonymised for security reasons, according to the Research Ethics Review Committee of the University of Groningen.

A. Theoretical Framework

Discourse analysis informed by Critical Discourse Analysis (CDA) principles is used to explore *Mavi Vatan's* narrative construction and the socio-cultural dimensions of the politics of identity. This method was chosen for its multidisciplinary scope and for the complex interplay it reveals between text, social opinion, power, society, and

culture.[6] Moreover, critical geopolitics is the theoretical framework employed to deconstruct the doctrine, since it essentially constitutes a maritime geopolitical plan. The prevalent theories in IR are realism, constructivism, and liberalism. In geopolitics, classical geopolitics remains the best-known. It has influenced numerous geopolitical strategies despite the rise in popularity of critical geopolitics in the last two decades. Therefore, this section explains why critical geopolitics was selected and why it best aligns with the research goals.

Most research on *Mavi Vatan* employs realist theories, particularly structural and neoclassical realism. Realism assumes the nation-state is the primary international relations (IR) actor, acting as a unified entity guided by rational decision-makers pursuing national interests within an anarchic international system. Kenneth Waltz's structural realism (1979) shifted focus from human nature to systemic structure, arguing that the anarchic international system constrains all states' behaviour based on material capabilities. However, this approach overlooks endogenous factors critical to understanding Blue Homeland.[7]

Theoretically, classical geopolitics aligns with realism.[8] Classical geopoliticians, based on their spatial generalisations, articulated their understanding of 'how the world works' and employed a historical perspective to justify their country's foreign policy. They primarily focused on land and sea power classifications, core-periphery models, and the rise and fall of states. The most prominent example is Halford Mackinder's influential concept, the "Heartland".[9] Another example is Nicholas Spykman's "Rimland, " which expands on Mackinder's heartland thesis.[10] Also, Alfred Thayer Mahan's ideas have been used to analyse the Blue Homeland. He was a United

[6] Teun A. van Dijk, 'Discourse and Manipulation' (2006) *Discourse & Society,* Vol. 17(3), 359 , https://doi.org/10.1177/0957926506060250.
[7] Kenneth Neal Waltz, *Theory of International Politics* (Berkeley: Addison-Wesley Publishing Company, 1979), https://www.abebooks.com/9780201083491/Theory-international-politics-Addison-Wesley-series-0201083493/plp.
[8] Klaus Dodds, *Geopolitics: A Very Short Introduction*, (3rd edn., Oxford: Oxford University Press, 2019), https://academic.oup.com/book/28414 42.
[9] Harold J. Mackinder, 'The Geographical Pivot of History (1904)' (2004) *The Geographical Journal,* Vol.170 (4), 298, http://www.jstor.org/stable/3451460.
[10] Nicholas John Spykman, *The Geography of the Peace* (New York: Harcourt, Brace and Company, 1944), https://books.google.gr/books?id=YpWDAAAAMAAJ&printsec=frontcover&hl=el&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

States Navy officer and historian who developed a geopolitical plan to expand the USA's sphere of influence. He advocated for a 'sea power doctrine,' emphasising the importance of overseas naval bases, and stressed that commercial and naval expansionism were crucial elements of a great power.[11]

Contrary to realism, constructivism treats national interests as socially constructed by agents themselves, emphasising the actors' significance within their social and environmental contexts. Truth and reality only exist as social constructs shaped by human awareness. As Alexander Wendt famously stated in his 1992 article, 'Anarchy is what states make of it'.[12] He further elaborated in his book 'Social Theory of International Politics':

> Neorealists see the structure of the international system as a distribution of material capabilities because they approach their subject with a materialist lens; Neoliberals see it as capabilities plus institutions because they have added to the material base an institutional superstructure; and constructivists see it as a distribution of ideas because they have an idealist ontology.[13]

Constructivists deny the existence of a linguistically constructed social reality and thus cannot explain the origins of these constructions. However, in critical geopolitics, human constructions of identity are treated as intermediate variables between social reality and actor behaviour. Ontological Security Theory, developed by Steele (2008) and Mitzen (2006), complements constructivism by explaining how states construct and maintain stable identities to manage existential anxiety.[14] This framework recognises that states require coherent identities to function psychologically and institutionally. In the Turkish context, *Mavi Vatan* functions not merely as a 'territorial' claim but as an identity-stabilisation mechanism, particularly following the

[11] Alfred T. Mahan, *The Influence of Sea Power upon History, 1660–1783*, Cambridge Library Collection - Naval and Military History (first published 1890, Cambridge: Cambridge University Press, 2010), https://doi.org/10.1017/CBO9780511783289.
[12] Alexander Wendt, 'Anarchy Is What States Make of It: The Social Construction of Power Politics', (1992) *International Organization* Vol.46(2), 391, https://www.jstor.org/stable/2706858.
13 Alexander Wendt, *Social Theory of International Politics*(Cambridge: Cambridge University Press, 1999), https://doi.org/10.1017/CBO9780511612183 5.
14 Brent J. Steele, Ontological Security in International Relations: Self-Identity and the IR State (London: Routledge, 2008), https://doi.org/10.4324/9780203018200; Jennifer Mitzen, 'Ontological Security in World Politics: State Identity and the Security Dilemma', (2006) *European Journal of International Relations* Vol.12 (3) 341, https://doi.org/10.1177/1354066106067346.

destabilising 2016 coup attempt. Concurrently, securitisation theory, articulated by Buzan, Wæver, and de Wilde, illuminates how maritime disputes transition from routine policy issues into existential threats requiring extraordinary state action. According to Buzan, Wæver, and de Wilde (1998), securitising moves (rhetoric, institutional claims, threat narratives) elevate specific issues to existential national concerns.[15] Applied to *Mavi Vatan*, this framework explains how maritime boundaries are transformed into sacred national interests, rendering naval preparedness and assertive foreign policy as imperatives.

Liberal theories are the least used in the Blue Homeland context. The main reason is that Türkiye sees international institutions as Western-dominated (Altan). International Law, alongside international organisations, extends the global system's scope beyond states alone, facilitating common goals such as addressing climate change, fostering diplomacy among nations, and ensuring that all member states have a voice in global affairs. Secondly, the free trade proliferation and capitalism establish an open, market-based international economic system. This system promotes trade between nations, reducing conflict likelihood, as war would disrupt trade benefits.[16] Nonetheless, critical geopolitics regards the absence of identity as a significant weakness of liberalism. Meanwhile, Türkiye is an increasingly autocratic state and is not a signatory state of UNCLOS. Thus, a liberal analysis is inapposite, as *Mavi Vatan* violates international standards and opposes UNCLOS.

Critical geopolitics, established by Dalby and Ó Tuathail, shifts the focus from geography's direct impact on IR to the examination of whose geographical narratives dominate and whose interests they serve.[17] Rather than treating geography as a neutral force, it interrogates how geopolitical imaginaries, particularly maps and spatial conceptualisations, shape political action. This approach is indebted to Foucault's

[15] Barry Buzan, Ole Wver, Jaap De Wilde , *Security: A New Framework for Analysis* (Boulder: Lynne Rienner Pub, 1998). https://dokumen.pub/security-a-new-framework-for-analysis-9781685853808.html.
[16] Daniel Deudney and G. John Ikenberry, 'The Nature and Sources of Liberal International Order'(1999) *Review of International Studies,* Vol. 25 (2), 179 https://www.cambridge.org/core/journals/review-of-international-studies/article/abs/nature-and-sources-of-liberal-international-order/085D7A99C0C9EFB5F96BE9B096DD9548.
[17] Joanne Sharp, 'Critical Geopolitics', in Audrey Kobayashi (ed.) *International Encyclopedia of Human Geography (Second Edition)*, (Oxford: Elsevier, 2020), https://doi.org/10.1016/B978-0-08-102295-5.10457-3, 45.

insight that power and knowledge are intertwined. As with the doctrine's map, great significance is given to the imaginaries created by maps that determine future political action. Geopolitics is no longer a one-dimensional, linear field.[18] Critical geopolitics examine the use of geography within the discourses of geopolitical imaginaries, visions, and geostrategies by states and global players.[19]

Moreover, the constructed connection between maritime spaces and identity influences collective memory and neo-nationalism.[20] This involves the symbolic significance of maritime territories and the historical narratives associated with *Mavi Vatan*. This theory challenges the international scene's spatialisation by governments.[21] Spatialisation considerations delve into the implications of asserting sovereignty over maritime spaces. To continue, critical geopolitics deposes West-centrism, rendering it suitable for studying non-Western geopolitical doctrines.[22] *Mavi Vatan* is a characteristic doctrine of the Turkish geopolitical culture. Critical theorists have extensively examined how geopolitical knowledge is produced within elite circles, including academia and the military. The goal is not just to illustrate the elites' opinions, but mainly to discern their differences and contradictions and to trace the power struggle between the elite circles and their diversity.[23]

The theoretical framework is operationalised in the analysis by examining how competing historical narratives employ geopolitical imaginaries to legitimise maritime expansion. It helps explain how the post-2016 coup context created ontological insecurity that elevated Eurasianist identity within the military institutions, how hydrocarbon competition materialises maritime claims into concrete economic imperatives and how the *Vatan* concept securitises maritime spaces by invoking sacred

[18] Gearóid O'Tuathail, 'Understanding Critical Geopolitics: Geopolitics and Risk Society' (1999) *Journal of Strategic Studies,* Vol. 22 (2–3), 107, https://doi.org/10.1080/01402399908437756.
[19] Basil Germond, 'The Geopolitical Dimension of Maritime Security' (2015) *Marine Policy,* Vol. 54, 137, https://doi.org/10.1016/j.marpol.2014.12.013 138.
[20] Merje Kuus, Joanne Sharp, Klaus Dodds , *The Ashgate Research Companion to Critical Geopolitics* (New York: Routledge, 2016), https://doi.org/10.4324/9781315612874, 29.
[21] O'Tuathail (no 18) 52.
[22] Zhiding Hu and Dadao Lu, 'Re-Interpretation of the Classical Geopolitical Theories in a Critical Geopolitical Perspective' (2016) *Journal of Geographical Sciences,* Vol. 26 (12), 1769, https://doi.org/10.1007/s11442-016-1357-1.
[23] Merje Kuus, 'Critical Geopolitics', in Renée Marlin-Bennett and Robert Allen Denemark (eds.), *The International Studies Encyclopedia* (Oxford: Oxford University Press, 2010), https://doi.org/10.1093/acrefore/9780190846626.013.137 12.

homeland symbolism that transcends legal-rational discourse. Critical geopolitics provides the overarching lens for deconstructing whose spatial knowledge dominates Turkish policy discourse, while ontological security theory and securitisation theory explain the mechanisms through which contested doctrines gain traction during periods of identity crisis and political restructuring.

B. Methodological Considerations

This research utilises a qualitative approach, involving CDA informed analysis of academic literature, articles, and books, as well as interviews with key experts. This provides a deeper understanding of the Blue Homeland from both theoretical and practical perspectives. The primary data are collected through semi-structured interviews with key academics in Türkiye. The literature entails both white and grey sources. The CDA method entails analysing discourse in papers to study the mechanisms of power conduct and the reproduction of domination, abuse of power, and inequality in societies.[24]

Regarding the interviews, purposive sampling was initially adopted, a technique in which participants suitable for answering the research questions are purposively selected. This sampling method guided the data generation and analysis, which is an essential aspect of CDA, as it allows the collection, coding, and initial data analysis before further data collection and analysis are undertaken.[25] Despite this approach, data analysis of the purposive sample generated codes related to history, identity, and TFP. Hence, the literature review guided the purposive selection of academics based in Türkiye who specialise in the above domains. The participants have written research articles and books about TFP and *Mavi Vatan*.

It is important to note that the selection process also included convenience sampling, as snowballing was used at a later stage. This means that some academics connected me with some of their colleagues. In light of that, the danger of gatekeeping

[24]Petar Kurecic, 'Identity and Discourse in Critical Geopolitics: A Framework for Analysis,'(Conference Paper, Society & Technology, CROSBI, 2015) , https://www.bib.irb.hr:8443/794654 9.
[25] Claire Willey-Sthapit et al., 'Discursive Decisions: Signposts to Guide the Use of Critical Discourse Analysis in Social Work' (2022) *Qualitative Social Work,* Vol. 21 (1), 129, https://doi.org/10.1177/1473325020979050 136.

is stressed. The sample size is ten academics. Given the research timeframe, the length of the interviews, and the time I was stationed in Türkiye (March 2024 – June 2024), the sample size is adequate for sufficient data collection. Collecting and analysing additional data would not yield further information on the topic, given the limitations, and no new codes were subsequently created.[26] All interviewees are practising professors. Nonetheless, they come from different academic backgrounds, from IR to political science and International Law. The diversity of the sample is also ensured by the fact that they teach at varying Universities in Türkiye. Interviews were conducted in the greater Istanbul area.

Furthermore, some universities were private, while others were public. Some of the professors participate concurrently in different Turkish think tanks[27] that are backed by rival political parties; consequently, the participants could be influenced by this. It must be emphasised that other voices, such as the military and political parties, were not included in the interview sample. Although attempts were made to contact such institutions, such as the Naval Academy, no response was received. The participants were approached via email, and the interviews were conducted face-to-face in Istanbul, except for two, which were conducted via Zoom due to distance and time constraints.

Even though most participants had no concerns about anonymity, their names are not disclosed, and all participants are pseudonymised for security reasons. The initial draft of the interview guide was submitted to the Research Ethics Review Committee of the University of Groningen, and after minor revisions, approval was granted. Semi-structured interviews, which fall between unstructured and structured interviews, were used to collect qualitative data. This data collection method enabled the researcher to follow a set of fixed questions or prompts and further probe beyond the approved questions. The interviews were conducted in English from March to May of 2024, and each lasted approximately 40 minutes. The interviews began with a 'briefing' containing general study information. Their expertise was crucial in shaping the direction of the conversation. For instance, the interview started with an open-ended

[26] After the fifth interview.
[27] The universities and think tanks' names are not disclosed to ensure anonymity.

question that initiated the conversation. At least two questions were asked for each theme to each participant; depending on their expertise, additional questions followed.

The interviews' recordings, both virtual and in-person, were transcribed before data analysis commenced. All the recordings were audio. During the interviews, notes were taken to detect the most essential notions and parts, to ensure the most accurate representation of the participant's responses. Windows Media Player was used to play the audio recordings while transcribing them manually. Transcription was initially performed manually for security and anonymity. The recordings were deleted one week after each interview. Afterwards, the manual transcriptions were entered into Microsoft Word, and the data were analysed to determine codes and themes. The data were analysed using CDA. The CDA follows an 'abductive' approach, continually refining theoretical concepts to achieve a more precise understanding of the empirical world. As Wodak (2004) puts it: 'a constant movement back and forth between theory and empirical data is necessary'.[28]

The CDA analysis involved identifying words, ideas, or phrases in the transcripts, including constructs of interest; investigating how they are expressed; and examining how the exact phrase or idea is presented across different texts.[29]Specifically, the analysis included multiple stages of coding, conducted in conjunction with taking memos and initial notes from the interviews. Even before coding the data, some emerging themes emerged during the interview transcription. Data coding was the first step, involving assigning labels that were typically descriptive and similar to the data. This coding process commenced with line-by-line coding of the first transcripts.

It is important to clarify the scope of CDA application in this study. While full CDA as developed by Fairclough and van Dijk would include detailed micro-level linguistic analysis (syntax, transitivity, modality),[30] this study focuses primarily on

[28] Ruth Wodak, 'Critical Discourse Analysis', in Giampietro Gobo & al., (eds) *Qualitative Research Practice* (London: SAGE Publications Ltd, 2004), https://doi.org/10.4135/9781848608191 200.
[29] James Paul Gee, *An Introduction to Discourse Analysis: Theory and Method* (2nd edn., New York: Routledge, 2004), https://doi.org/10.4324/9780203005675.
[30] Norman Fairclough, *Analysing Discourse: Textual Analysis for Social Research* (London ; New York: Routledge, 2003), https://www.routledge.com/Analysing-Discourse-Textual-Analysis-for-Social-Research/Fairclough/p/book/9780415258937; van Dijk, (no 6).

thematic discourse analysis of narrative structures and power relations informed by CDA principles. The analysis emphasises how competing narratives are constructed, and how geopolitical knowledge production occurs within elite institutional contexts. This approach aligns with critical geopolitics, which adapts CDA's focus on power-knowledge relations while prioritising geopolitical narrative analysis over linguistic microanalysis.

Core categories were identified to reduce the codes and proceed beyond the descriptive phase until no new codes emerged. Subsequently, it was discovered that the additional data generated, especially from the last three interviews, aligned with the existing codes. Although the latest participants' data (7-10) did not yield new themes, they identified new relationships among them. Finally, thematic coding was conducted by organising the codes into four higher-level themes that emerged from the data concerning the existing units. It is emphasised that memo-writing is the stage between coding and drafting the analysis. These memos, comprising a coding memo and the interview's notebook, included decisions such as merging, renaming, categorising and creating a code.

Below you see two data analysis examples. Codes are created in the form of Word comments. An across-case analysis is conducted by applying the same question and theme (Historical Background in the given examples) to each interview and exploring similarities, common notions, and differences. In the comment section, I also include notes taken during the interviews; therefore, some comments are labelled as 'Interview notebook'. At the same time, memos were written to articulate common ideas, codes, and differing opinions. An example is provided below:

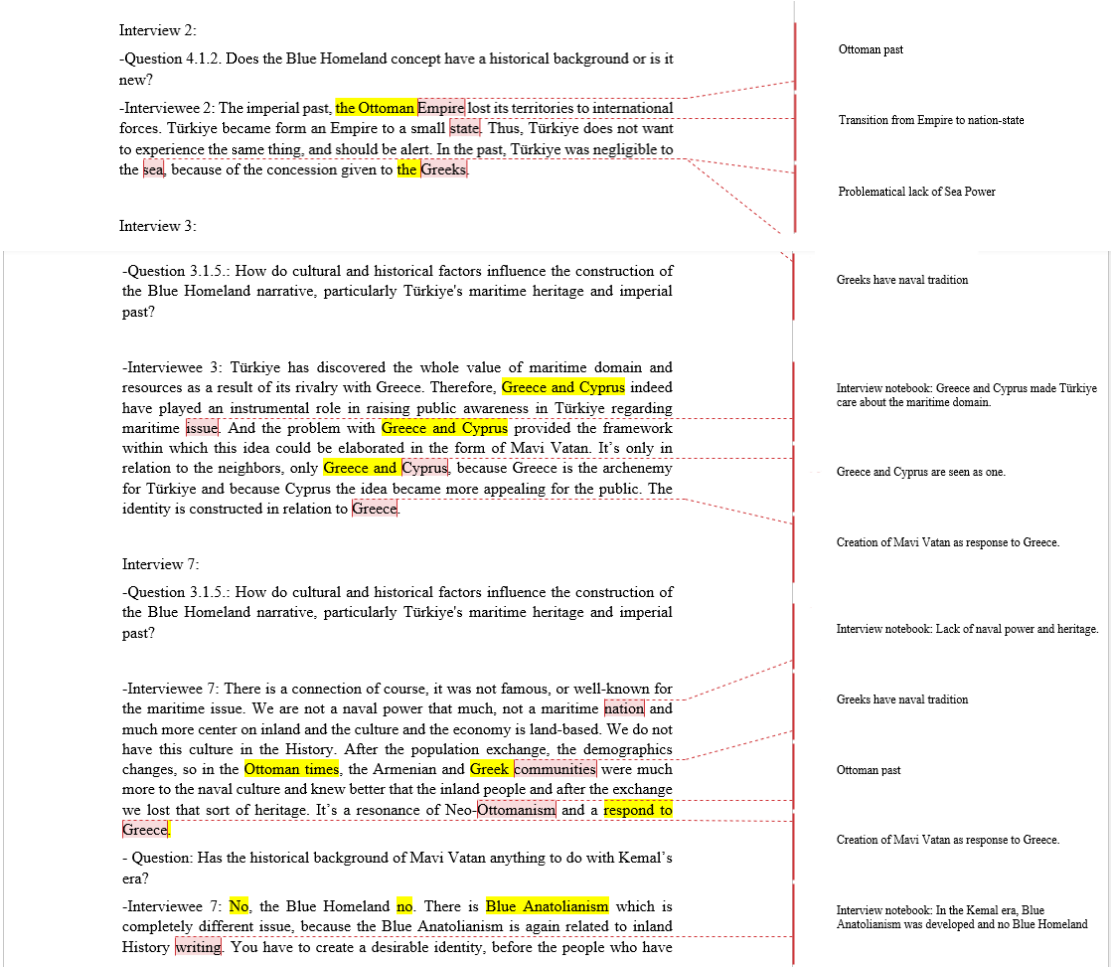

Figure 1: Data analysis example

Memo example:

Date: 05-05-2024

Theme: Historical Background

Codes: Ottoman past, Greek naval tradition, Turkish lack of naval tradition

For Türkiye, the loss of the Aegean islands and the transition to a nation-state were considerable shocks. The Ottomans depended on the naval culture of the minorities, especially the Greeks, for their Sea capabilities. Thus, the new Turkish Republic had no Seapower and was consequently confined to its land borders.

C. Limitations and Ethical Considerations

Firstly, reflexivity involves reflecting on how the researcher's position influences the research process. A fundamental CDA theoretical assumption is that researchers cannot entirely detach themselves from social discourse to achieve an objective view.[31] To address this, memos examined how personal and professional experiences rendered certain discourses more appealing, while acknowledging that others may be concealed. Given the extensive nature of the doctrine, this study may not examine all its aspects with equal depth. Data availability constraints, particularly regarding sensitive geopolitical issues and national security matters, may limit the analysis depth. Another limitation was that participants who were members of the military or political parties were not interviewed, as noted above. Additionally, the results might be influenced by the study's temporal context, as geopolitical dynamics are subject to change.

The Turkish language poses another challenge, as I lack sufficient knowledge, which may lead to misinterpretation or the loss of nuance in translation. Consequently, only English-language literature is examined, thereby limiting the study's scope, as most Turkish researchers publish in Turkish. This is also why interviews were held to counter this limitation. As a Greek researcher studying *Mavi Vatan*, a sensitive issue between Greece and Türkiye, I strive to maintain critical distance and objectivity in my analysis despite the inherent challenges.

Ethical considerations are paramount when discussing sensitive geopolitical subjects. Before the interviews, all participants obtained consent forms to ensure they understood the research's purpose and their rights. To continue, the interview data were processed solely for research purposes. The participant's anonymity and confidentiality are protected by removing identifying information from interview transcripts and ensuring safe data storage. Sensitive personal data is minimised and pseudonymised during transcription, with risks mitigated through strict security protocols. Participation

[31] S. Hall, 'Foucault: Power, Knowledge and Discourse' in Margaret Wetherell et al. (eds) , *Discourse Theory and Practice: A Reader* (London: Sage in association with The Open University, 2001), http://www.library.mmu.ac.uk/secure/index.php?cat_file=&filename=y_220a0002_hall_foucault.pdf.

in interviews was voluntary. At the same time, recognising and respecting cultural differences was essential, particularly in diverse contexts between Türkiye and Greece.

2 Narratives of Historical Backgrounds

To better understand the Blue Homeland doctrine, its legitimacy, and the maritime identity it promotes, the historical background must be studied to identify the circumstances and timing of its creation. Two distinct narratives exist regarding *Mavi Vatan's* historical origins. The former is the narrative promoted by the doctrine's creators, particularly retired Admiral Cem Gürdeniz, as evidenced by his writings and interviews. For this reason, it is described as the 'official' one. The known creators of the doctrine are retired Admirals Cem Gürdeniz and Cihat Yaycı, who have published numerous works that have contributed to the Blue Homeland's growing popularity within the Turkish navy. Gürdeniz, the 'father' of the doctrine, was the Director of the Plan and Policy Division of the Turkish Naval Forces Command Headquarters back in 2006.[32] Cihat Yaycı drew the map.[33] Additionally, Admiral Soner Polat, who died in 2019, was a notable advocate and wrote a book dedicated to this concept.[34]

The latter narrative is sceptical towards the 'official', though it does not oppose Blue Homeland's broader ideas, such as the need for a stronger navy and maritime influence. Consequently, it is mentioned as the 'sceptic' narration. The prominent supporters of the second narration are Turkish academics who view the admirals promoting *Mavi Vatan* as opportunists. The common ground between the historical narratives lies in the Ottoman past as a starting point, especially in the late years of the empire, when the lack of a strong navy proved disastrous. The main difference concerns Kemal's era connection to the Blue Homeland. On the one hand, the 'official' narrative is presented by the Turkish Navy, which asserts that Kemal is the spiritual father of the

[32] Zenonas Tziarras, *Turkish Foreign Policy: The Lausanne Syndrome in the Eastern Mediterranean and Middle East*, (Cham: Springer International Publishing, 2022), https://link.springer.com/10.1007/978-3-030-90746-4 62.
[33] See Map 1.
[34] Aurélien Denizeau, 'Mavi Vatan, 'the Blue Homeland': The Origins, Influences and Limits of an Ambitious Doctrine for Turkey' (2021) *IFRI-Institut Français Des Relations Internationales*, Études de l'Ifri.https://www.ifri.org/en/studies/mavi-vatan-blue-homeland-origins-influences-and-limits-ambitious-doctrine-turkey 7.

Blue Homeland. On the other hand, the 'sceptic' historical perspective is showcased, which sees no immediate connection between the two, as the interviewees confirm.

A. 'Official' Narrative

According to the 'official' narrative by the doctrine's creators, Blue Homeland is the naval version of the *Misak-ı Millî* or National Pact.[35] The National Pact was the map created by the last Ottoman Parliament in 1920, drawing the borders of the areas where the 'Ottoman Muslim majority' lived.[36] This was the goal of Türkiye's political independence. *Mavi Vatan* is also characterised as the natural sea extension of *Ana Vatan*, the Motherland. The *Ana Vatan* map, issued in 1927, celebrated the new Republic of Türkiye and its founding principles. However, it included territories that were not, and still are not, part of Türkiye, such as Cyprus, the Aegean islands, and Western Thrace, while it excluded the Hatay region, which is now integrated. This map closely resembles the National Pact map. The map is decorated with a portrait of the Republic of Türkiye's founding father, Atatürk.[37]

[35] Denizeau (no 34) 16.
[36] Hasan Kosebalaban, *Turkish Foreign Policy: Islam, Nationalism, and Globalization* (New York: Palgrave Macmillan, 2011),, http://site.ebrary.com/id/10496593 49.
[37] Atatürk means father of Turks, a name given to Mustafa Kemal.

Map 2: The Map of '*Ana Vatan*' 1927[38]

Atatürk is also declared the Blue Homeland's founding father,[39] although he never used the term. The central assertion is that Atatürk sought to establish a Turkish naval policy. Indeed, Atatürk promoted the '*Deniz sevgisi*', meaning love of the sea.[40] He understood the significance of a formidable navy and what a lack of it meant, due to the disastrous losses he witnessed during ten years of unstoppable wars, from the Italo-Turkish War (1911-1912) to the Turkish War of Independence (1919-1923), when he was a military officer. In his speeches, he declared the necessity of Türkiye becoming a maritime power to defend Anatolia and build a great fleet. Nonetheless, this ambition did not materialise due to Türkiye's dire internal situation at the time. The limited funds, the hostile relations with potential naval suppliers, the international maritime disarmament under the Washington Treaty of 1922, and the demilitarisation

[38] Sûd Kitaphane-Yi, 'Map of Ana Vatan: Turkey', image, Library of Congress, Washington, (2021), available at https://www.loc.gov/resource/g7431f.ct003172/ (last accessed 23 July 2025).
[39] Tevfik Kadan, 'The Formulation of the Blue Homeland Doctrine', (2021) *BRIQ Belt & Road Initiative Quarterly*, Vol. 2(1), 36, https://briqjournal.com/en/the-formulation-the-blue-homeland-doctrine 38.
[40] Serhat Süha Çubukçuoğlu, 1st ed. *Turkey's Naval Activism: Maritime Geopolitics and the Blue Homeland Concept*, (Abu Dhabi: Palgrave Macmillan, 2023), https://link.springer.com/book/10.1007/978-3-031-37204-9.

requirements of the Turkish Straits rendered the dream of becoming a maritime power nearly impossible.[41] These were the primary reasons for selecting a coastal defensive fleet over a costly surface fleet.

A turning point for Turkish maritime policy was the Montreux Convention of 1936. This convention allowed Türkiye to refortify the Dardanelles Strait, the Sea of Marmara, and the Bosporus Strait, thereby denying access to warships during wartime while permitting merchant ships free passage.[42] At the same time, Greece expanded its territorial waters from 3 miles to 6 miles without any challenge from Türkiye. The Convention ensured the Turkish connection between the Eastern Mediterranean and the Black Sea. Furthermore, the Convention enhanced naval security against Greece and Russia. After Kemal Atatürk's death, İsmet İnönü led the country through the Second World War until 1950. Türkiye, alongside Greece, joined NATO in 1952 to provide security against the Soviet Union.[43] According to the admirals, NATO strategy limited Türkiye's maritime responsibilities to the Black Sea, while Greece was assigned to cover the Aegean Sea and the Eastern Mediterranean.[44] As a result, Turkish interests were excessively harmed in the Eastern Mediterranean and the Aegean because Türkiye was preoccupied with the Black Sea against the Soviet Union.

Moreover, Türkiye reoriented itself towards the Eastern Mediterranean from the 1960s onwards, due to the Cyprus Issue. The creators of *Mavi Vatan* were young scholars at the Naval Academy when the Turkish invasion of Cyprus in 1974 occurred after the coup of Nicos Sampson, which resulted in the occupation of 36% of the island by the Turkish forces. This affected them profoundly, and, according to their account, the Turkish invasion signalled Türkiye's determination to secure its maritime rights. In 1983, Türkiye created the 'Turkish Republic of Northern Cyprus' ('TRNC'), which is only recognised by Türkiye.[45] Cyprus is described as *'Yavru Vatan'*, meaning Baby

[41] Serhat Güvenç and Dilek Barlas, 'Atatürk's Navy: Determinants of Turkish Naval Policy, 1923–38', (2003) *Journal of Strategic Studies,* Vol. 26(1), 1, https://doi.org/10.1080/01402390308559306.
[42] Ayla Göl, 'A Short Summary of Turkish Foreign Policy: 1923-1939', (1993) *Ankara Üniversitesi SBF Dergis,* Vol. 48(1), 57 https://dergipark.org.tr/en/pub/ausbf/article/43214 66.
[43] Hakan Yapar, 'Turkey's Strategic Shift: From Strategic Depth to Blue Homeland and Beyond', (2021) *Instituto Español de Estudios Estratégicos* https://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO40_2021_HAKYAP_Turquia_ENG.pdf. 3.
[44] Çubukçuoğlu (no 40) 81.
[45] Kosebalaban (no 36) 106.

Homeland and is regarded as the precursor of the *Mavi Vatan*. The Turkish logic behind the invasion, aside from the Turkish community's future, was an aversion to Enosis (Union) and fears of a Greek naval encirclement. Gürdeniz supports the view that *Mavi Vatan* and *Yavru Vatan* are part of *Anavatan*.

Following the Soviet Union's dissolution and the end of the Cold War, Türkiye focused exclusively on the Aegean and the Eastern Mediterranean in the maritime domain. The admirals identify themselves as Kemalists and claim that *Mavi Vatan* is a continuation of Kemal's defensive strategy culture in the naval domain. Firstly, Gürdeniz views the Greek extension of territorial waters from 6 to 12 nm as a form of the Sévres at sea.[46] Consequently, he claims that Türkiye's casus belli against Greece in 1995,[47] regarding the extension of the territorial waters, constitutes a central point of the Blue Homeland. Greece's aim to extend its territorial waters to 12 nm (nautical miles) would effectively eliminate Türkiye's claim to any continental shelf in the Aegean.

Secondly, the 1996 Imia[48] crisis is characterised as the Blue Homeland's forerunner. In this crisis, a dispute arose over the ownership of two rocky islets. The quarrel over sovereignty led to bitter exchanges between Athens and Ankara, a build-up of military forces around the disputed areas, and a diplomatic intervention by the USA to defuse tensions between the two NATO allies.[49] This crisis demonstrated that Türkiye attaches equal importance to Greece, including to islets such as Imia. At the time, all *Mavi Vatan's* creators were active members of the Turkish Navy. Thirdly, in 1997, the white paper 'Towards Blue Waters' was issued, the first official Turkish naval strategy. It is regarded as a continuation of the Kemalist strategic culture and the basis of the Blue Homeland.[50] As Prof. Abdul mentioned, 'Before *Mavi Vatan*, another strategy existed, but it didn't gain the same traction. It was too generic and had no

[46] Cem Gürdeniz, *The Map of Seville and the Plot to Cut Turkey off from the Aegean and Mediterranean Seas United World International*, 17 September 2020, available at https://uwidata.com/13877-the-map-of-seville-and-the-plot-to-cut-turkey-off-from-the-aegean-and-mediterranean-seas/ (last accessed 23 July 2025).
[47] Greece ratified UNCLOS in 1995.
[48] *Kardak* in Turkish.
[49] William Hale*Turkish Foreign Policy, 1774-2000.* 2nd edn., Hoboken: Taylor and Francis, 2012), https://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=1024490 196.
[50] Çubukçuoğlu (no 40) 123.

catchy name like *Mavi Vatan*'. The main objectives of this document were to establish a deep-sea navy and to develop power-projection capabilities.

Therefore, this military narration, rather than simply asserting a connection to Atatürk, constructs historical continuity through strategic genealogy by characterising *Mavi Vatan* as the 'natural sea extension' of territorial concepts from the 1920s. The doctrine's creators align their 21st-century maritime claims with Türkiye's founding nationalist project. It seeks to legitimise the naval dogma by invoking the illustrious Kemalist era and Türkiye's military confrontations, such as the invasion of Cyprus and the Imia crisis. It also grounds contested contemporary claims in foundational legitimacy and positions maritime expansion as a defensive necessity rather than revisionism.

B. 'Sceptic' Narrative

On the other hand, there is another historical perspective that rejects *Mavi Vatan's* Kemalist roots and the admirals' rhetoric. The academic, more moderate narrative focuses mainly on the period before 2006 and the immediate causes that led to this doctrine. Initially, this narration recognises the Turkish shock at the loss of the Aegean islands and the transition from Empire to nation-state. Prof. Deniz noted, 'There is a historical experience gained from what happened during the dissolution of the Ottoman Empire. During the process of becoming a nation-state, the maritime domain is seen as one of the main problematic areas'. In this context, the lack of a Turkish maritime tradition is emphasised, and the fact that the Ottoman Empire's naval tradition derives from other seafaring peoples, especially the Greeks. Prof. Altan claimed, 'In the past, Türkiye was negligible to the sea because of the concession given to the Greeks'. The past refers to the Ottoman era and the granting of 'privileges' in trade rights to the Greek people by the Sultans.

In the context of the Kemalist era, Blue Anatolianism is discussed rather than Blue Homeland, which is a distinct concept. This narrative outright rejects any connection between the era of Atatürk and *Mavi Vatan*. Prof. Izem said: 'It has nothing to do with Blue Homeland', when referring to the Kemal era. In contrast, Blue Anatolia

(*Mavi Anadolu*) constructs Turkish identity based on Anatolia's geographical inheritance rather than the Seas.[51] According to Prof. Izem, 'It's like going deeper into the Homeland and looking for historical dimension and layers of identity'. In the Blue Anatolian narratives, the Turkish people and lands are bearers of diverse cultures and civilisations, including European ones. Blue Anatolianism was a political and cultural concept of the 1930s aimed at promoting a common Turkish identity rooted in Anatolia. Blue Anatolianism, as a theory of territorial nationalism, rests on geographical inheritance.[52] *Mavi Anadolu* deepens the Homeland notion, while *Mavi Vatan* extends it towards the Seas. Prof. Izem adds that Blue Homeland 'it's a resonance of Neo-Ottomanism'.

Regarding the triggering events of the near past, the most decisive event was the Seville Map of 2003. Juan Luis Suárez de Vivero and Juan Carlos Rodríguez Mateos, professors of human geography at the University of Seville, published an article titled 'Maritime Europe and EU Enlargement: A Geopolitical Perspective' at the request of the European Union (EU).[53] This article featured a map depicting the Turkish EEZ confined in the Antalya Gulf, known as the Seville Map. This work aimed to facilitate maritime spatial planning in preparation for the EU's 2007 enlargement. The EU ratified UNCLOS in 1998, making it mandatory for new members to accept it.[54] Although not legally binding, this map delineated the EEZs of EU members; it supported Greek and Cypriot maritime pretensions by creating an EEZ border between Greece and the RoC. According to Prof. Abdul, 'This forced Türkiye to react'. The reaction was the Blue Homeland.[55]

According to the 'sceptic' narrative, the second most decisive event leading to the doctrine's creation was the Republic of Cyprus's rejection of the Annan plan, the

[51] Rahime Süleymanoğlu-Kürüm and Elif Gençkal Eroler, 'Spatial Constructions of Homeland in Turkish National Identity: Exclusion and Inclusion of Europe', (2023) *Uluslararası İlişkiler Dergisi,* Vol. 20 (77), 17, https://dergipark.org.tr/tr/pub/uidergisi/issue/75495/1233978 24.
[52] Danış Mehmet Fahri, 'The Blue Anatolian Ideal as a Theory of Territorial Nationalism', (2023) *Recent Period Turkish Studies,* Vol. 1 (44), 213, https://iupress.istanbul.edu.tr/en/journal/rpts/article/topraga-bagli-bir-milliyetcilik-teorisi-olarak-mavi-anadolu-ideali 44.
[53] Erkeç (no 5) 40.
[54] Çubukçuoğlu (no 40) 147.
[55] Mehmet Bardakçı, 'Turkey and the Major Powers in the Eastern Mediterranean Crisis from the 2010s to the 2020s', (2022) *Comparative Southeast European Studies,* Vol. 70 (3), 516, https://www.degruyter.com/document/doi/10.1515/soeu-2021-0071/html 521.

Cypriot EEZ declaration, and Cyprus's subsequent EU accession in 2004. Firstly, Cyprus signed an EEZ treaty with Egypt in 2003, and the following year it declared its EEZ.[56] In general, Türkiye denies Cyprus's EEZ and the RoC's existence, referring to it as the Greek-Cypriot Administration. In the context of bi-communal negotiations to resolve the Cyprus Issue, the Annan Plan emerged in 2004 from talks between the representatives of the two communities (Turkish-Cypriots and Greek-Cypriots) mediated by then-UN Secretary-General Kofi Annan.[57] The logic behind the plan was that the Cyprus Issue would be resolved firstly and then Cyprus would join the EU as a unified island. This would open the road for Türkiye's accession.

The Annan Plan, which entailed a bizonal, bicommunal Federation, was rejected by 75.38% of Greek Cypriots in a referendum.[58] Despite the Annan plan's rejection by the Greek-Cypriots, Cyprus joined the EU, while Türkiye's accession was stalled. This was perceived as a betrayal by Türkiye, underscoring the deep-rooted tensions in the region.[59] Gürdeniz and the Turkish military were against the plan since it entailed the withdrawal of Turkish troops from Cyprus. From their perspective, Türkiye was yielding to the EU's commands, and they needed to protect the Turkish maritime rights.[60] As a result, the Annan plan and the Cypriot EEZ declaration were supplementary factors that led to *Mavi Vatan*. As Prof. Abdul mentioned: 'the problem with Greece and Cyprus provided the framework within which this idea could be elaborated in the form of *Mavi Vatan*'. According to the 'sceptic' narrative, the Seville Map, the Annan plan, and the Cypriot EEZ led to the Blue Homeland.

However, the 'sceptic' academics add to their narration the Turkish EEZ in the Black Sea, which is the only official part of the Blue Homeland and internationally recognised. It is essential to mention that although *Mavi Vatan* is not an official doctrine, the maritime boundaries it predicts in the Black Sea are de jure. As Prof. Aytekin said: 'The Blue Homeland is official only in the Black Sea'. Türkiye is the only Black Sea

[56] Fuat Aksu and Helin Sarı Ertem, *Analyzing Foreign Policy Crises in Turkey: Conceptual, Theoretical and Practical Discussions*, (Newcastle upon Tyne: Cambridge Scholars Publishing, 2017), https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=151771472.
[57] Hale (no 49) 198.
[58] Ibid.
[59] Kosebalaban (no 36) 159.
[60] Denizeau (no 34) 16.

coastal state that has not ratified UNCLOS. Nevertheless, it has delimited its maritime boundaries with all the neighbouring countries. In 1973, 1978, and 1987, Türkiye and the Soviet Union agreed on their boundary for the territorial sea, continental shelf, and EEZ.[61] After the dissolution of the USSR, Georgia, the Russian Federation, and Ukraine confirmed the validity of the USSR-Türkiye maritime boundary delimitations. In 1997, Türkiye and Bulgaria also agreed upon their boundary. It is asserted that the Black Sea is a more stable neighbourhood than the Eastern Mediterranean and where there is low friction over maritime boundaries between the countries.

Notably, the Black Sea's EEZs are not so politicised, contrary to the Aegean's case. For Prof. Aytekin, 'the biggest problem in the Mediterranean is the lack of trust between Greece and Türkiye'. The Turkish Black Sea EEZ implements specific UNCLOS provisions, including Articles 56–57, which govern the extent and rights of coastal states within EEZs. Türkiye's core complaint is UNCLOS Article 121, which grants continental shelf and EEZ rights to islands. This 'problem' does not exist in the Black Sea to the extent it does in the Eastern Mediterranean, because the Black Sea has only a few islands near the coast, which do not significantly alter the EEZs. Thus, *Mavi Vatan* focuses solely on the Aegean and the Eastern Mediterranean.

The 'sceptic' narrative, while emphasising recent events (the 2003 Seville Map, Cyprus's 2004 EU accession), operates within its own logic. Prof. Ekrem described the admirals as follows: 'They are Eurasianist, Euro-sceptic, anti-globalist, Western-sceptic […] claiming extensive territorial waters or larger sea areas fits into the narrative'. Both Gürdeniz and Yayci are Eurasianist Kemalists.[62] This ideology shapes their view of history and Türkiye's place in the world. The respondents viewed the 'official' narrative as an attempt by the doctrine's creators to draw on history to gain legitimacy and common consent. They see them as opportunists aspiring to pursue a political career. Academic dismissal of the admirals as 'opportunists' might reflect professional competition within Türkiye's policy establishment. The 'sceptic' narrative reframes maritime expansion as pragmatic statecraft rather than as part of a nationalist ideology, a positioning that may make such claims more acceptable to international audiences.

[61] Çubukçuoğlu (no 40) 100.
[62] Tziarras (no 32) 64.

Critically, both narratives converge on core claims. Firstly, they agree on the strengthening of Türkiye's maritime position, that external actors (Greece, Cyprus) have challenged Turkish maritime interests, and that naval expansion is justified. The narratives diverge not on whether *Mavi Vatan* is necessary, but on whether its framing serves additional ideological functions. This convergence suggests that the binary between 'official' and 'sceptic' may obscure a deeper consensus about maritime revisionism, with disagreement focused primarily on rhetorical legitimation rather than the doctrine itself.

The different narratives reflect asymmetrical power relations within Turkish policy discourse. The 'official' narrative, backed by military institutional authority and incorporated into naval strategy documents, circulates through official and unofficial channels. The other narrative is confined to a few academics and reaches more limited audiences. This institutional asymmetry means that the 'official' narrative's version of historical truth has greater practical consequences for policy formation, regardless of empirical accuracy. Understanding *Mavi Vatan*, therefore, requires examining not only which historical claims are made but also which institutional actors possess the authority to make claims prevalent. It is essential to note that the binary obscures hybrid positions while exemplifying competing historical claims.

Finally, when researching the *Mavi Vatan's* history, two divergent narratives emerged. In most cases, the first 'official' narrative is presented by the doctrine's founders and has a military background. Concurrently, a second, less well-known narrative emerged from the interviews about Blue Homeland's history. This 'sceptic' narration has an academic background. All the respondents view the 'official' narrative as an attempt by the doctrine's creators to draw on history to gain legitimacy and common consent. Nonetheless, both narratives accept that Turkish maritime strengthening is necessary; the divergence concerns how to justify expansion in acceptable ways. Consequently, *Mavi Vatan* has not one but two historical narratives, depending on the interests one maintains.

3 Context of *Mavi Vatan's* Ascension

A. Domestic Political Context

Before examining the politics of identity, the events that led to *Mavi Vatan's* rise should be analysed to understand its ascension better. Domestic politics played a crucial role, particularly after the failed July 15, 2016, coup attempt. Initially, Erdoğan accused the Gülenists of instigating the coup attempt. Gülenists are followers of Fethullah Gülen, who was an Islamist scholar self-exiled in Pennsylvania, and had built a strong network in education and finance.[63] They were former allies of Erdoğan's political party, *Adalet ve Kalkınma Partisi* (Justice and Development Party), and in 2013, the rupture followed the AKP's closure of Gülen's preparatory schools.[64] The coup attempt gave Erdoğan emergency powers, and he seized the opportunity to target all opposition.

Erdoğan targeted the Turkish military, purging approximately 81% of the top officers (1,524 out of 1,886) and 24,339 members of all the Turkish Armed Forces (TSK), including non-commissioned officers and civil servants. However, only 8,651 military members participated according to official sources.[65] The government dismissed the Kemalist personnel and the so-called 'Atlanticist', who are pro-Western and pro-NATO, from the Turkish military, paving the way for the Eurasianists, who are anti-Western, pro-Russian and pro-China.[66] The Eurasianists are fervent proponents of *Mavi Vatan* and wanted to include it on the defence agenda.[67] The new National Defence University, which replaced the prestigious war academies, introduced examination systems that gave the government direct control over officer selection and advancement.[68]

---

[63] Aslı Bâli, *Turkey's Cyclical Coups*, Dissent Magazine, 12 August 2016, available at https://dissentmagazine.org/online_articles/turkey-coup-countercoup-akp-erdogan-gulenist-purges/ (last accessed 26 February 2026).
[64] Bâli, (no 63).
[65] Levent Kenez, *Erdogan Dismissed 81 Pct of Top Turkish Military Officers Following Controversial Coup Attempt in 2016*, Nordic Monitor , 16 July 2024, available at https://nordicmonitor.com/2024/07/erdogan-purged-81-of-top-turkish-military-officials-following-controversial-coup-attempt-in-2016/ (last accessed 26 February 2026).
[66] Edoardo Lavezzo, 'Limits of a Competitive Authoritarianism in Security Policies: Interpreting Türkiye's Approach towards the EU' (2025) *Filozofija i Drustvo,* Vol. 36(2), 479, https://doi.org/10.2298/FID2502479L 487.
[67] Denizeau (no 34) 20.
[68] Murat Ülgül and Sertif Demir, 'Keeping the Soldiers at Bay: Coup-Proofing Strategies in Turkey' (2020) *Middle East Policy,* Vol. 27 (3), 138, https://doi.org/10.1111/mepo.12518 147.

Erdoğan's government was intent on restructuring the military, prioritising political loyalty over professional merit and strategic expertise. As ontological security theory predicts, the crisis following the coup attempt created conditions where *Mavi Vatan* could function as an identity-stabilisation factor. The purge of Atlanticist officers and ascension of Eurasianists represents the institutional restructuring through which securitised narratives gain policy traction by replacing one coherent identity framework (Western-oriented) with another (Eurasianist-nationalist) to restore the state's ontological security.

The failed coup also created the political conditions that resulted in a nationalist turn in Turkish domestic politics, through the formation of an alliance between the AKP and the MHP, Nationalist Movement Party (*Milliyetçi Hareket Partisi*), formally known as the 'People's Alliance' (*Cumhur İttifakı*), which has governed to this day since 2018. To explain how this political alliance came to be, the 2015 elections must be examined. In the June election, the AKP lost its parliamentary majority for the first time, and Bahçeli (MHP leader) refused to form a coalition with the AKP.[69] Nonetheless, in the November election, the MHP suffered electoral losses. These results provide the basis for future realignment. In 2016, Bahçeli faced a leadership challenge from Akşener, a former Minister (1996-1997), but an electoral body prevented the vote on Bahçeli's replacement from taking place, some say with governmental interference.[70]

Akşener and the dissidents were expelled from the MHP and founded the Good Party (*İYİ Partisi*) in October 2017.[71] Therefore, the MHP's position made an alliance with the AKP increasingly necessary for the party's survival. Bahçeli openly supported the April 2017 constitutional referendum that transformed Türkiye's parliamentary system into a presidency with sweeping executive powers.[72] The new system required

[69] Atilla Yeşilada, *Is the AKP–MHP Alliance Reaching a Breaking Point? A Structural Analysis of Turkey's Ruling Bloc* (*P.A.Turkey*, 9 November 2025), available at https://www.paturkey.com/news/2025/is-the-akp-mhp-alliance-reaching-a-breaking-point-a-structural-analysis-of-turkeys-ruling-bloc-25137/ (last accessed 26 February 2026).
[70] *Ercan Gurses and Seda Sezer, Turkish Nationalist Party Expels Leadership Challenger,* World, Reuters, 8 September 2016, available at https://www.reuters.com/article/world/turkish-nationalist-party-expels-leadership-challenger-idUSKCN11E1SH/ (last accessed 26 February 2026).
[71] Demir Murat Seyrek, *New Hope for Turkey's Opposition?*, Deutsche Welle, 25 October 2017, available at https://www.dw.com/en/opinion-new-political-party-gives-life-to-turkeys-opposition/a-41111859 (last accessed 26 February 2026).
[72] Sibel Oktay, *Turkey's Phantom Coalition: The AKP-MHP Partnership and Turkish Foreign Policy*, APSA MENA POLITICS, 18 November 2020, available at https://apsamena.org/2020/11/18/turkeys-

both a presidential and parliamentary mandate. In the June 2018 election, Erdoğan surpassed 50% of the vote and became president under the new system, only because he had joined a coalition with the MHP in February 2018, forming the People's Alliance.[73] The ruling coalition is not a traditional one, since the MHP lacks veto power over foreign policy decisions.[74]

Instead, the partnership functions as an electoral and ideological alignment that permits Erdoğan to appropriate nationalist rhetoric and policies while maintaining executive control over their implementation. This alliance materialises nationalist discourse at the state level, creating what securitisation theory identifies as 'audience acceptance',[75] meaning that the MHP's nationalist base provides domestic legitimacy for the doctrine's maritime assertiveness that might otherwise appear revisionist. The People's Alliance represents not only a political coalition but also the structural embedding of securitised identity politics into governance.

In parallel, EU-Turkish relations worsened after the failed coup, owing to further democratic backsliding in Türkiye, especially under the new presidential system.[76] Concurrently, the collapse of the Turkish-Kurdish peace process in 2015 resulted in renewed violence from the Kurdistan Workers' Party (PKK) and Turkish military invasions in Syria against the People's Defence Units (YPG), further souring the relationship with the EU and making a potential alliance with the anti-Kurdish MHP easier.[77] Additionally, Türkiye during the same period exploited migration and used the refugee crisis as a negotiation weapon against the EU.[78] The above diminished Türkiye's EU integration prospects, increased anti-Western rhetoric, and hence forced a return to a nationalist and security-focused positioning.

---

phantom-coalition-the-akp-mhp-partnership-and-turkish-foreign-policy/ (last accessed 26 February 2026).

[73] Ziya Öniş, 'Turkey's New Presidential Regime: Fragility, Resilience, Reversibility',(2023) *Reflektif Journal of Social Sciences,* Vol. 4(1), 159, https://doi.org/10.47613/reflektif.2023.98 160.

[74] Oktay (no 72).

[75] Ori Wertman and Christian Kaunert, *The Audience in Securitization Theory*, The Institute for National Security Studies, (2022), available at https://www.inss.org.il/strategic_assessment/the-audience-in-securitization-theory/ (last accessed 26 February 2026).

[76] Lavezzo (no 66).

[77] Yeşilada, (no 69).

[78] Lavezzo (no 66) 490.

B. Hydrocarbon Competition Context

On the other hand, while the ideological restructuring of the Turkish army and government paved the way for *Mavi Vatan's* adoption, the Turkish economic interests played an equally important role. Firstly, Türkiye's economy began its dramatic decline in the mid-2010s. The Turkish lira's depreciation, chronic inflation, declining foreign investment, the country's reliance on imported energy and rising energy import costs rendered hydrocarbon exploration an economic imperative. Energy security constitutes one of the doctrine's goals and is essential for Türkiye's economy and geopolitical vision. In 2022, Türkiye imported all the natural gas it consumed, 91% of its oil products, and 77% of its coal, with Russia being its primary trade partner.[79]. In 2020, the biggest gas reserve was found in the Sakarya field in the Black Sea, but even in the best-case scenario, it is projected to cover only 30% of Türkiye's future demand.[80]

As a result, the Eastern Mediterranean's hydrocarbons are equally crucial for energy security. In 2015, ENI discovered an 850 bcm (billion cubic meters) natural gas reserve in Egypt's Zohr field, while Israel's Leviathan contains approximately 620 bcm and Cyprus' Aphrodite field around 130 bcm.[81] Beyond the Aphrodite field, Türkiye also claimed the reserves discovered in the Cypriot Calypso and Glaucus fields in 2019 by ExxonMobil, which amount to 142-227 bcm.[82] The central narrative of *Mavi Vatan's* supporters is that these hydrocarbons rightfully belong to the Turkish people and will resolve economic issues by ensuring affordable energy and autarky (Altan). Furthermore, another strategy calls for transforming Türkiye into an energy hub,

[79] Francesco Siccardi, *Understanding the Energy Drivers of Turkey's Foreign Policy*, Carnegie Europe, (2024), available at https://carnegieeurope.eu/2024/02/28/understanding-energy-drivers-of-turkey-s-foreign-policy-pub-91733 (last accessed 26 February 2026) 4.
[80] Mustafa Enes Esen, *Coal, Oil, Gas, and Nuclear: Risks in Turkey's Growing Energy Demands*, Washington Institute, 22 October 2025, available at https://www.washingtoninstitute.org/policy-analysis/coal-oil-gas-and-nuclear-risks-turkeys-growing-energy-demands (last accessed 26 February 2026).
[81] Sina Kısacık, 'Existing and Prospective Central Paradigms of Eastern Mediterranean Energy Geopolitics in The 21st Century: Do / Will All the Related Parties Seek for Collaborations or Confrontations?', in Hasret Çomak, Burak Şakir Şeker, Mehlika Özlem Ultan (eds), *Global Maritime Geopolitics* (London: Transnational Press London, 2022), https://www.ceeol.com/search/chapter-detail?id=1026150 233.
[82] Ozay Mehmet and Vedat Yorucu, *Modern Geopolitics of Eastern Mediterranean Hydrocarbons in an Age of Energy Transformation* (Cham, Switzerland: Springer, 2020), https://doi.org/10.1007/978-3-030-43585-1 75.

transporting gas from the Zohr, Leviathan, and Aphrodite fields and integrating it into European markets via the Southern Gas Corridor (SGC).

However, the East Mediterranean Gas Forum (EMGF), initiated by Egypt and joined by Cyprus, Greece, Israel, Italy, Jordan, and Palestine in 2019, isolated Türkiye diplomatically and excluded it from regional development projects.[83] The Turkish response was the signing of two Memoranda of Understanding (MoUs) with Libya's Government of National Accord (GNA) later that year, one on maritime delimitation and the other on security, a concrete expression of *Mavi Vatan* in policy. This served as a response to the Greece-Egypt cooperation and as a legitimising tool in Ankara's presence in Libya and its claims to Eastern Mediterranean resources. From a critical geopolitics perspective, the EMGF's exclusion of Türkiye demonstrates how geopolitical imaginaries like maps of gas fields and pipeline routes, become marginalisation instruments. The Turkish-Libyan MoU represents a counter-imaginary that challenges the Western-backed energy architecture by redrawing maritime boundaries through bilateral assertion rather than multilateral consensus.

Overall, the events following the failed coup served as catalysts for Türkiye's strategic orientation. The purge of 'Atlanticist' officers created space for Eurasianist and nationalist voices to dominate the military. The AKP-MHP alliance provided political cover for increasingly assertive foreign policies that departed from the EU-integration framework of the 2000s. The regional hydrocarbon competition, Türkiye's economic crisis, energy dependency, and exclusion from regional resource frameworks made the doctrine's unofficial adoption an imperative for asserting sovereignty in the Eastern Mediterranean. Prof. Ekrem noted: 'Eurasianists and nationalists became quite influential in the government circles after the attempted coup; it was an opportune time to push for it [*Mavi Vatan*]'. Others added that this geopolitical discourse was used for the natural resources (Izem). The doctrine's creators and later the government utilised the Vatan concept to popularise it.

[83] Valeria Talbot, *The Scramble for the Eastern Mediterranean: Energy and Geopolitics* (Milan: Ledizioni, 2021), https://www.ispionline.it/sites/default/files/pubblicazioni/ispi_report_the_scramble_for_the_eastern_mediterranean_web.pdf.

4. Blue Homeland's Politics of Identity

Blue Homeland is primarily associated with maritime jurisdictions and security matters, while identity is often overlooked. In the literature, there is little work on *Mavi Vatan*'s identity perspective. However, extensive discourse and a bibliography on the Vatan concept are available, primarily in Turkish. As Wendt indicated, interests derive from identities. A state's identity regarding others shapes its interests.[84] Therefore, understanding a state's identity is crucial to understanding its interests. Wendt's constructivism posits that collective identities play a vital role in shaping foreign policy, which, in turn, expresses a state's identity and its constructed interests.[85] Although not an official naval dogma, it has undoubtedly affected Turkish foreign policy. *Mavi Vatan's* influence on the internal domain is even more challenging to research. The data collected from the interviews proved critical for uncovering the politics of identity surrounding this relatively new concept. Some interviewees conducted extensive research and wrote extensively about the *Vatan* concept.

Consequently, the deeper meanings of the word '*Vatan*' and the wider concept must be explained. Secondly, the influence of the Bleu Homeland doctrine on TFP and Türkiye's international posture is analysed. Last but not least, the attempt at national identity-building is showcased, and its resonance is recorded. The 'politics of identity' in *Mavi Vatan's* context refers to how the *Vatan* concept shapes national identity and informs foreign policy decisions. This is a significant aspect, reflecting the complex interplay between foreign policy, maritime sovereignty and national identity.

A. The Concept of Vatan

The *Vatan* concept has many ramifications. However, the internal notions must be unveiled for in-depth comprehension. In Turkish and Arabic, *Vatan* does not simply

[84] Alexander Wendt, 'Anarchy Is What States Make of It: The Social Construction of Power Politics' (1992) *International Organization,* Vol. 46 (2), 391, https://www.jstor.org/stable/2706858.
[85] Alexander Wendt, *Social Theory of International Politics*, Cambridge Studies in International Relations (Cambridge: Cambridge University Press, 1999), https://www.cambridge.org/core/books/social-theory-of-international-politics/0346E6FDC74FECEF6D2CDD7EFB003CF2.

mean Homeland; it also carries a sacred dimension.[86] According to Prof. Aytekin, the notion is above ethnicity, language or religion: '*Vatan* is a Holy place to live in. It is the living space of the people, not only the Turks but also others; it's inclusive'. It also contains patriotic sentiments, as Prof. Altan noted for *Vatan*: 'You must die for your land; millions have died before for this land in the past'. In contrast, a minority of interviewees introduced a more statist dimension by referring to the entire sovereign country of Türkiye as *Vatan*. Moreover, everyone agreed that the term attracts the Turkish mindset (Izem). In securitisation terms, the *Vatan* concept transforms routine maritime policy into an existential issue requiring extreme measures. By invoking its sacred dimension, policy elites elevate EEZ disputes from technical legal matters to civilisational survival questions, thereby justifying actions that deviate from international norms like UNCLOS. This sacred framing is what enables maritime claims to bypass rational cost-benefit calculations and enter the realm of non-negotiable identity imperatives.

Today, the Vatan concept remains a significant symbol in Turkish culture and can be traced throughout Turkish history. However, the meaning of *Vatan* is not fixed; it changes with perceptions of national interest, shaped by signals and responses from both domestic and foreign actors.[87] For example, the Islamic *Vatan* is not territorialised. In contrast, modern Turkish *Vatan* is characterised by clearly defined territorial boundaries.[88] *Vatan's* notion gained significant prominence during the late Ottoman period in response to the empire's disintegration and the rise of nationalism. This concept was employed to rally the populace to preserve the remaining territories amidst external and internal threats (wars and rebellions).[89] The initial goal was to create a common Ottoman identity, which failed. As Prof. Yusuf noted: 'Basically, it was created when non-Muslims were included in the Ottoman army to serve as soldiers'.

Following the establishment of the Turkish republic in 1923, *Vatan* became the cornerstone of the new national identity. Atatürk embedded the concept deeply into

[86] B. Özkan, *From the Abode of Islam to the Turkish Vatan: The Making of a National Homeland in Turkey* (New Heaven, CO: Yale University Press, 2012), https://yalebooks.yale.edu/book/9780300172010/from-the-abode-of-islam-to-the-turkish-vatan/ 2.
[87] Çubukçuoğlu (no 40) 202.
[88] Özkan (no 86) 4.
[89] Ibid, 51-53.

Türkiye's political and cultural ethos. This time, the intention again aligned with the previous case: to create a common identity centred on Turkish nationalism. The concept of a unified Turkish *Vatan* was used to eliminate differences between the Anatolian populations. Republican reforms were groundbreaking in linking Turkish identity with territoriality. The formation of the secular Turkish nation-state replaced allegiance to the sultan and religion with loyalty to the homeland. This shift was revolutionary as it detached the nation from Islam and God, as a community of believers, and from the Ottoman sultan as loyal subjects, connecting it instead to the *Vatan*.[90] This continuity from the Ottoman legacy to the Republican era reflects *Vatan*'s enduring significance in shaping Türkiye's collective identity and national unity.

Prof. Izem supported the above statements: 'The first idea of *Vatan* was in the last period of the Ottomans before the Empire dissolved. Nonetheless, she further explained: 'There were three visions during the disruption of the Empire, the one to enlarge the territories based on Islam (Pan-Islamism), as Abdul Hamid tried, the Pan-Turkish one where you have Central Asian roots and expand upon it, and then the Blue Anatolianism'. Blue Anatolianism's *Vatan*, as mentioned before, was the one to prevail. In modern-day Türkiye, the concept has expanded further. The best-known 'expansion' was the Yavru Vatan, or 'Baby Homeland,' referring to Cyprus in the early 1950s and the need to unite with *Anavatan* Türkiye.[91] This means that not only the Greeks but also the Turks sought the union of Cyprus with their country, though it was conceptualised differently under *Yavru Vatan*.

Depending on historical realities, the Vatan has undergone significant changes in Turkish political discourses. On the same path, almost 50 years later, a new ramification of *Vatan* was created, the Blue Homeland for the Eastern Mediterranean and the Aegean. *Mavi Vatan* is the 'extension at sea and seabed of our homeland'.[92] Prof. Ekrem explained: 'In Turkish, we refer to Türkiye as *Anavatan* and Cyprus as *Yavru Vatan*. *Mavi Vatan* nicely fits into this nationalist narrative'. It is essential to note that although four professors describe the Vatan concept as a nationalist narrative, they

[90] Ibid, 4-5.
[91] Ibid, 194.
[92] Cem Gürdeniz, *What Is the Blue Homeland in the 21st Century?*, United World International, 31 July 2020, available at https://uwidata.com/12952-what-is-the-blue-homeland-in-the-21st-century/ (last accessed 28 July 2025).

all argue that it is defensive. Consequently, they believe that all branches of Vatan are defensive and protect the concept of Homeland, including the Blue Homeland, which is regarded as a defence of the Turkish maritime domain. Nevertheless, all the interviewees recognised that political leaders frequently invoke the term *Vatan* to rally public support and justify policies, particularly those related to national security and foreign policy. By emphasising the homeland, politicians aim to foster resilience and resistance to perceived external threats, thereby reinforcing the narrative of a nation under siege. Prof. Yusuf remarked that: 'the strategic use of *Vatan* promotes national unity in defence of the shared territory'. It is used to bolster the legitimacy of government policies, both domestically and abroad.

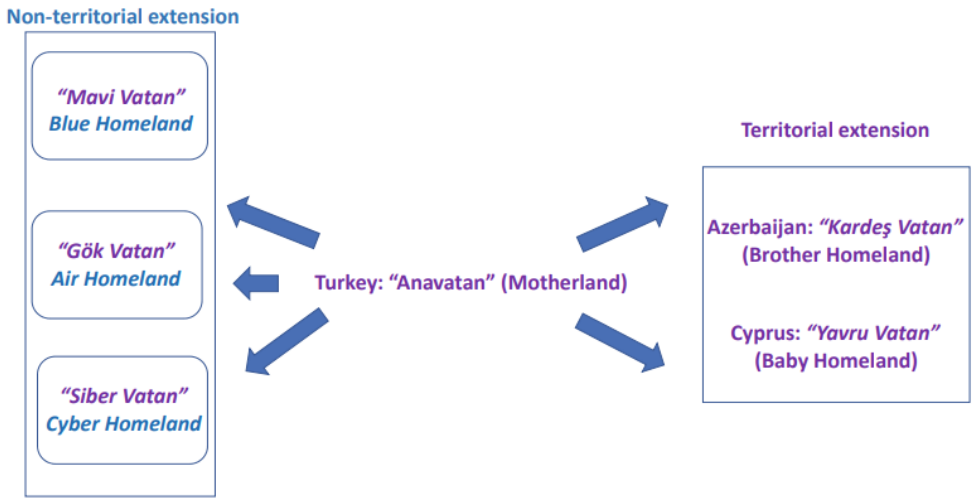

Figure 2: The wider '*Anavatan*' concept[93]

B. Mavi Vatan and Turkish Domestic Identity

In the domestic context, the concept was featured on national television and various debate programs after the failed coup d'etat, particularly from 2016 to 2020, indicating an intention to reach domestic audiences. Prof. Defne said: 'It is unclear to what extent the general public is engaged in promoting this concept. It appears to be a

[93] Çubukçuoğlu (no 40) 219.

topic of discussion primarily within academic and political circles rather than among the wider public'. What is more, Prof. Izem added: 'In TRT, they shot a documentary on Blue Homeland'. The public was 'bombarded' by a media campaign from *Mavi Vatan* supporters, which increased public awareness on Türkiye's maritime issues. A prominent figure in these debates was Cem Gürdeniz, who promoted his doctrine, as evidenced by his social media posts and numerous interviews.[94] Some of the interviewees described the concept as a 'great public relations tool' (Abdul) and a 'good propaganda tool' (Aytekin).

The doctrine's primary goal is to make maritime policies more appealing to the Turkish public. Its creators wish to reconstruct the Turkish identity. All the interviewees expressed surprise that the potential of the Turkish maritime domain has not been realised, despite Türkiye being surrounded by seas (Ezel). The doctrine tries to introduce a Turkish naval identity and redefine Türkiye's position in the world as a naval nation. Prof. Izem observed: 'It tries to create a naval culture, which we lack because we are traditionally inland people'. In the Ottoman Empire, the Greeks had the naval heritage, now it is high time for the Turks to establish their own (Yusuf). All participants agreed that the concept aims to forge a bond with the seas and to persuade the Turkish public that the maritime boundary is as important as the land boundary. For instance, Prof. Altan argued: 'For Vatan now is not only the land but also the sea, it's a national issue […] you must die for it, it creates the feeling of possession and attachment'.

Mavi Vatan is regarded as a government and state-controlled media narrative. Prof. Izem stated, 'The government tries to inculcate this idea, but I don't think it's successful'. Indeed, most interviewees agree that public resonance is limited and that identity construction remains incomplete. Specifically, Prof. Ekrem's public survey found that more than 70% of participants had never heard of *Mavi Vatan*. Still, they could understand it was associated with the sea. Concurrently, Prof. Abdul declared: 'Everything related to the sea is described as *Mavi Vatan* […] the term has become trivialised'. This is considered dangerous because the doctrine's primary goal has lost

[94] Aydınlık, *Cem Gürdeniz: Eurasian Alliance is Necessary* , 21 September 2020, available at https://www.aydinlik.com.tr/haber/cem-gurdeniz-avrasya-ittifaki-zorunlu-218862, (last accessed 28 July 2025).

its substance. Others argue that the Turkish public is not particularly concerned with naval issues, owing to more immediate problems. The most frequently mentioned problems affecting daily life are inflation, the cost of living, and the Syrian Issue (Ezel and Izem). Prof. Ezel believes that only the attentive public who follows TFP knows the topic.

Blue Homeland is understudied within Turkish academia. Prof. Yusuf underlined, 'This is a military concept, not academic'. At the same time, Prof. Izem admitted: 'I wanted to write an article on Blue Homeland, they said just two or three paragraphs, these independent academic people […] they were not curious,' when referring to conferences and seminars she participated in. On the other hand, a different approach suggests that the doctrine's topics are overstudied within academic discourse but not under this term (Defne). Another common opinion is the lack of institutionalisation and cultural identity (Deniz). Despite their differences, they all agree that Türkiye should be more involved with its maritime affairs.

From 2021 onwards, even though *Mavi Vatan* is not in the top current affairs in Turkish media and government, a new education system called 'Century of Türkiye' was approved in May 2024. According to this model, *Mavi Vatan's* maps will be included in the geography lesson, and the Turkish struggle for its legal and geographical rights in the Aegean, which is named 'Sea of the Islands', will be taught.[95] In the tenth-grade geography class, the reasons Türkiye has not signed UNCLOS and the historical ties with the TRNC will be presented. Admirals commented on this, declaring that a new generation is emerging with a *Mavi Vatan* consciousness. While interviewing Prof. Izem, this topic arose, and she argued: 'The school discourse is important to inculcate ideas to future generations; this (identity) is under construction'. This new curriculum represents an institutional embedding previously absent and establishes a new basis for the development of *Mavi Vatan's* politics of identity.

Ontological security theory showcases why curriculum institutionalisation matters. States produce coherent identities across generations through socialisation

[95] Manolis Kostidis, 'Blue Homeland Doctrine Planted in Turkish Schools', *eKathimerini*, 28 December 2024, https://www.ekathimerini.com/politics/foreign-policy/1239830/blue-homeland-doctrine-planted-in-turkish-schools/ (last accessed 28 July 2025).

mechanisms that transform contested claims into naturalised truths. The curriculum functions as a between elite securitising discourse and mass identity internalisation. It also reconciles the doctrine's present limitations with its future ambitions. While current mass mobilisation remains weak, systematic generational indoctrination ensures long-term identity transformation and continuation of maritime claims. *Mavi Vatan* is no longer a convenient narrative to boost the government's popularity; it is becoming a long-term identity project.

C. Mavi Vatan and Turkish Foreign Identity

In the international domain, representations of threats and dangers to *Vatan* significantly influenced TFP and shaped perceptions of what constitutes the national interest. The politics of identity increasingly affects foreign policy formulation, whether through religious and nationalist identities or through political leaders who must respond to the growing influence of new social groups.[96] Blue Homeland is a naval doctrine within Turkish geopolitical dogma. These dogmas assume that Türkiye's location in a strategically crucial region dictates its foreign policy and security decisions.[97] Türkiye is described as a 'central' state that serves as the nexus of three continents, acting as both a connector and a divider between regions. The *Mavi Vatan* version claims that Türkiye is the nexus of three Seas and has the longest coastline in the region. This warrants a larger territorial sea, which must be protected at all costs.

Although not officially adopted by the Foreign Ministry, 'Blue Homeland is a Turkish reaction to Greek and Cypriot maximalist approaches in the Aegean and the Eastern Mediterranean, according to Prof. Altan. Meanwhile, Prof. Abdul mentioned: 'Greece is the archenemy for Türkiye, and because of the Cyprus issue, it's more appealing for the public to support such actions […] *Mavi Vatan* is territorialising the Sea, it faces the Sea as being a piece of land'. The creators of the doctrine sought to foster a naval culture not only among the Turkish people but also among the Turkish

[96] Sabri Ciftci, 'Social Identity and Attitudes Toward Foreign Policy: Evidence from a Youth Survey in Turkey' (2013) *International Journal of Middle East Studies*, Vol. 45(1), 25, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2920374 29.
[97] Pinar Bilgin, 'Turkey's 'Geopolitics Dogma'', in Stefano Guzzini (ed.), *The Return of Geopolitics in Europe?* (Cambridge: Cambridge University Press, 2012), 10.1017/CBO9781139225809.010154.

state as a whole. Except for TFP, the doctrine aims to build a strong Turkish navy by constructing new warships in Türkiye. The increased maritime capabilities are a recurring theme in the interviews and the admiral's rhetoric. Blue Homeland has influenced TFP, mainly during 2016-2020, after the attempted coup. The most transparent case of *Mavi Vatan* in TFP was the Turkish-Libyan Memorandum of Understanding (MoU) on maritime boundaries and the EEZ, which was drafted by former Chief of Staff of the Turkish Navy, Yayci, one of the doctrine's leading theorists.[98] It was the first time that someone from the Turkish Navy had affected the TFP to such an extent. During this period, TPAO dramatically increased unauthorised gas prospecting, often accompanied by warships, in areas also claimed by Greece and Cyprus.[99]

In the military domain, increased naval presence was underlined in contested areas, and naval exercises took place, with the biggest named '*Mavi Vatan*' in 2019, leading to tensions with Greece and Cyprus over the EEZs' and continental shelf's delineation.[100] The doctrine was utilised from 2016 to 2020 to target Greece and make a statement on the international stage (Ekrem). Interestingly, rising commissions were recorded in the military-industrial complex, including the production of new drones, missiles, and sonar systems, as well as the air carrier TCG Anadolu, commissioned in 2023, while a new aircraft carrier is under construction.[101] This connects with Prof. Ezel's comments: '*Mavi Vatan* expresses an aspiration to develop maritime capabilities in the military domain'.

Nevertheless, there are objections to *Mavi Vatan's* actual level of influence within the TFP. All participants agreed on Türkiye's potential and need to become powerful at sea, irrespective of this doctrine. Some respondents observed that the government would follow its naval policies regardless (Ezel). It is speculated that Erdoğan used the Blue Homeland rhetoric to advance a neo-Ottomanist agenda in Africa, particularly in Libya. That is why Prof. Abdul accused Erdoğan of using the

[98] Anthony Deriziotis, 'The 'Blue Homeland' and Erdoğan's Rhetoric: State Doctrine or Populist Narrative?', in Janković Slobodan (ed.), *Convergence and Confrontation: The Balkans and the Middle East in the 21st Century*, (Belgrade: Institute of International Politics and Economics, 2021), http://doi.fil.bg.ac.rs/volume.php?pt=eb_book&y=2021&issue=iipe_conv_conf-2021&i=1 21.
[99] Siccardi, (no 79) 21).
[100] Çubukçuoğlu (no 40) 245.
[101] Çubukçuoğlu (no 40) 224.

concept for personal ambitions. After 2020, he explained: 'The Blue Homeland advocates have lost their grip around the party […] this idea doesn't serve Erdoğan's political interest anymore'. Additionally, Prof. Ekrem gave an interesting viewpoint: 'There was an intentional ambiguity from the Foreign Ministry, especially about not officially acknowledging *Mavi Vatan*'. The above illustrates a hybrid Turkish maritime strategy using the Blue Homeland map. Prof. Aytekin claimed: '*Mavi Vatan* is used as a bargaining map for negotiations with Greece […] it's not official because it undermines others' rights […] you will be seen as an irredentist'. Consequently, Türkiye does not recognise *Mavi Vatan's* map officially, since the international community would see Türkiye as a revisionist country.

To conclude, the politics of identity plays a crucial yet unexplored role in the discourse surrounding Blue Homeland. While geopolitical discussions often focus on maritime jurisdiction and security issues, the identity dimensions of *Mavi Vatan* have been largely overlooked. *Vatan's* deeper meanings emphasise the importance of national identity and of *Mavi Vatan* for Türkiye. Although unofficial, the doctrine's influence on TFP is undeniable, as it has driven assertive maritime claims and strategic alliances. However, its impact on domestic national identity is less straightforward; it appears to be currently under construction, with ambitious future aims. The Turkish government follows a strategy designed to foster long-term identity transformation while preserving diplomatic flexibility.

5. Conclusions

This study has showcased the Blue Homeland doctrine as a contemporary example of how states construct maritime sovereignty narratives to legitimise maritime and territorial claims and transform national identity. Through analysis of competing historical narratives, the context of the doctrine's rise, and the politics of identity politics, several key findings emerge regarding Türkiye's attempt to establish itself as a legitimate maritime power in the Eastern Mediterranean. This research analysed the doctrine through critical geopolitics and CDA. This methodology proved crucial for exploring the interplay among *Mavi Vatan*, its narratives, and the attempted identity construction that has unofficially affected TFP.

The main contribution is the alternative voices revealed in the interviews, which offer a different perspective on the doctrine. Usually, the doctrine is presented solely through the ideas of the concept's creators, which are described as 'formal' in this study, since these ideas are the most prevalent in the literature. Conversely, the 'sceptic' narrative, predominantly advanced by academic observers, detects the doctrine's creation as a reactive policy response to specific geopolitical developments in the 2000s, particularly the Seville Map, the Annan Plan, and Cyprus's EEZ declaration. This perspective views the historical connections as post-hoc legitimisation efforts rather than genuine continuity with Türkiye's maritime heritage. However, Blue Homeland was placed on the agenda 10 years after its creation, owing to the post-2016 conjuncture, comprising the army's restructuring, shifting political alliances, economic constraints, and diplomatic isolation.

Concerning the politics of identity, the *Vatan's* meaning was clarified. The research revealed that *Mavi Vatan's* 'foreign identity' is more developed, as it has substantially affected TFP. However, the internal national identity seems to be currently under construction. A new national 'maritime' Turkish identity appears to be under development, with the introduction of an education system designed to educate younger generations about Turkish maritime claims. The 'Century of Türkiye' curriculum represents the mechanism through which the doctrine overcomes its current lack of mass public resonance by targeting future generations who will internalise these maritime claims as foundational national truths. This institutionalisation ensures the continuity of Turkish naval claims. It signals Blue Homeland's de facto adoption as a generational identity project rather than an immediate political mobilisation tool.

While Türkiye has successfully elevated maritime issues in regional discourse and demonstrated naval capabilities, the doctrine's failure to secure international recognition suggests that historical legitimacy cannot be asserted; it must be earned through consistent policy implementation and diplomatic engagement. The doctrine's future trajectory will likely depend on the Turkish state's official adoption, the ability to secure support from all political parties, or the successful implementation of the claims through other means. As regional tensions continue and the Eastern

Mediterranean's energy resources become increasingly important, *Mavi Vatan* will remain a critical factor in regional stability and maritime affairs.

The discourse surrounding Blue Homeland and its identity perspectives has not yet ended; it will remain an essential component of Türkiye's geopolitical strategy. Its implementation and influence in formal policy will depend on situational interests, (geo)political and/or economic, regardless of the ruling political party(ies). The doctrine's framing of maritime expansion as a defensive necessity rather than a revisionist ambition increases its legitimacy. Its current unofficial status, but de facto implementation, protects Türkiye diplomatically and preserves the fait accompli. Unfortunately, *Mavi Vatan* will remain a structural source of tension with Greece, Cyprus, and potentially other actors. Currently, a *Mavi Vatan*-driven confrontation is unlikely to escalate into a full-scale conflict unless it is linked to other factors, such as energy competition, which can amplify this dynamic.

The connection between doctrine and economic interests suggests that the regional stability hinges on whether energy disputes are managed through multilateral mechanisms or through unilateral assertions of maritime claims. Equally important is the doctrine's impact on NATO's cohesion. Turkish assertiveness, framed through the doctrine, creates tensions with Greece, a NATO ally, and with broader Western preferences for a rules-based order, such as UNCLOS. NATO's cohesion will depend on reconciling Türkiye's maritime assertiveness with the interests of allied states.

The existence of competing narratives underscores the doctrine's contested legitimacy and highlights the challenges states face in constructing new geopolitical narratives in the modern era. Moreover, the provided context highlighted the importance of conjuncture in the doctrine's rise within government circles, while the identity factor is crucial to its longevity and continuity. *Mavi Vatan* is not only a nationalist rhetoric but also a geopolitical discourse that shapes how Turkish institutions, decision-makers, and the public understand maritime sovereignty, national identity, and Türkiye's regional role. Further research is needed. Similar studies could examine other branches of *Vatan*, such as the *Gök Vatan* or the *Yavru Vatan*, to uncover new dimensions of Turkish nationalism and geopolitical ambitions, and how these are legitimised. Finally, analysis of international responses to the doctrine could illuminate

its effectiveness as a tool of regional influence projection. This study opens the way for future research to unravel the narratives of Türkiye's identity-driven geopolitics.

Bibliography

Aksu F., and He. Sa. Ertem, *Analyzing Foreign Policy Crises in Turkey: Conceptual, Theoretical and Practical Discussions*, (Newcastle upon Tyne: Cambridge Scholars Publishing, 2017), https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=1517714

Aydınlık, *Cem Gürdeniz: Eurasian Alliance is Necessary* , 21 September 2020, available at https://www.aydinlik.com.tr/haber/cem-gurdeniz-avrasya-ittifaki-zorunlu-218862, (last accessed 28 July 2025).Bâli, A., *Turkey's Cyclical Coups*, Dissent Magazine, 12 August 2016, available at https://dissentmagazine.org/online_articles/turkey-coup-countercoup-akp-erdogan-gulenist-purges/ (last accessed 26 February 2026).

Bardakçı, M., 'Turkey and the Major Powers in the Eastern Mediterranean Crisis from the 2010s to the 2020s', (2022) *Comparative Southeast European Studies,* Vol. 70 (3), 516–39, https://www.degruyter.com/document/doi/10.1515/soeu-2021-0071/html.

Bilgin, P., 'Turkey's 'Geopolitics Dogma'', in Stefano Guzzini (ed.), *The Return of Geopolitics in Europe?* (Cambridge: Cambridge University Press, 2012), 10.1017/CBO9781139225809.010.

Buzan, B., Ol. Wver, and Ja. De Wilde, *Security: A New Framework for Analysis* (Boulder: Lynne Rienner Pub, 1998). https://dokumen.pub/security-a-new-framework-for-analysis-9781685853808.html.

Ciftci, S., 'Social Identity and Attitudes Toward Foreign Policy: Evidence from a Youth Survey in Turkey' (2013) *International Journal of Middle East Studies*, Vol. 45(1), 25–43, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2920374.

Çubukçuoğlu, S. S., 1st ed. *Turkey's Naval Activism: Maritime Geopolitics and the Blue Homeland Concept*, (Abu Dhabi: Palgrave Macmillan, 2023), https://link.springer.com/book/10.1007/978-3-031-37204-9.

Denizeau, A., 'Mavi Vatan, 'the Blue Homeland': The Origins, Influences and Limits of an Ambitious Doctrine for Turkey' (2021) *IFRI-Institut Français Des Relations Internationales*, Études de l'Ifri.https://www.ifri.org/en/studies/mavi-vatan-blue-homeland-origins-influences-and-limits-ambitious-doctrine-turkey.

Deriziotis, A., 'The 'Blue Homeland' and Erdoğan's Rhetoric: State Doctrine or Populist Narrative?', in Ja. Slobodan (ed.), *Convergence and Confrontation: The Balkans and the Middle East in the 21st Century*, (Belgrade: Institute of International Politics and Economics, 2021), http://doi.fil.bg.ac.rs/volume.php?pt=eb_book&y=2021&issue=iipe_conv_conf-2021&i=1.

Deudney, D., and G. J. Ikenberry. 'The Nature and Sources of Liberal International Order'(1999) *Review of International Studies,* Vol. 25 (2), 179–96, https://www.cambridge.org/core/journals/review-of-international-studies/article/abs/nature-and-sources-of-liberal-international-order/085D7A99C0C9EFB5F96BE9B096DD9548.

Diakopoulos, A., Pe. Liakouras, Ko. Ifantis, and Co. Filis. *Behind Turkey's 'Blue Homeland' Doctrine*, (ekathimerini.com, 19 June 2023), available at https://www.ekathimerini.com/opinion/1213618/behind-turkeys-blue-homeland-doctrine/ (last accessed 28 July 2025).

Dijk, T. A. . 'Discourse and Manipulation' (2006) *Discourse & Society,* Vol. 17(3), 359–83, https://doi.org/10.1177/0957926506060250.

Dodds, K., *Geopolitics: A Very Short Introduction*, (3rd edn., Oxford: Oxford University Press, 2019), https://academic.oup.com/book/28414.

Erkeç, E., 'Reflections of Türkiye-Greece Tension in the Sea of Islands on the Eastern Mediterranean Regional Security Complex' (2023) *BRIQ Belt & Road Initiative Quarterly*, Vol. 4(2), 24–48 https://www.ssoar.info/ssoar/handle/document/89599 .

Esen, M. E., *Coal, Oil, Gas, and Nuclear: Risks in Turkey's Growing Energy Demands*, Washington Institute, 22 October 2025, available at https://www.washingtoninstitute.org/policy-analysis/coal-oil-gas-and-nuclear-risks-turkeys-growing-energy-demands (last accessed 26 February 2026).

Fahri, D. M., 'The Blue Anatolian Ideal as a Theory of Territorial Nationalism', (2023) *Recent Period Turkish Studies,* Vol. 1 (44), 213-39 https://iupress.istanbul.edu.tr/en/journal/rpts/article/topraga-bagli-bir-milliyetcilik-teorisi-olarak-mavi-anadolu-ideali.

Fairclough, N., *Analysing Discourse: Textual Analysis for Social Research* (London ; New York: Routledge, 2003), https://www.routledge.com/Analysing-Discourse-Textual-Analysis-for-Social-Research/Fairclough/p/book/9780415258937.

Gee, J. P., *An Introduction to Discourse Analysis: Theory and Method* (2nd edn., New York: Routledge, 2004), https://doi.org/10.4324/9780203005675.

Germond, B., 'The Geopolitical Dimension of Maritime Security' (2015) *Marine Policy,* 137-42 Vol. 54, https://doi.org/10.1016/j.marpol.2014.12.013.

Göl, A., 'A Short Summary of Turkish Foreign Policy: 1923-1939', (1993) *Ankara Üniversitesi SBF Dergis,* Vol. 48(1), 57-71, https://dspace.ankara.edu.tr/xmlui/handle/20.500.12575/52926.

Gürdeniz, C., *The Map of Seville and the Plot to Cut Turkey off from the Aegean and Mediterranean Seas United World International*, 17 September 2020, available at https://uwidata.com/13877-the-map-of-seville-and-the-plot-to-cut-turkey-off-from-the-aegean-and-mediterranean-seas/ (last accessed 23 July 2025).

Gürdeniz, C., *What Is the Blue Homeland in the 21st Century?*, United World International, 31 July 2020, available at https://uwidata.com/12952-what-is-the-blue-homeland-in-the-21st-century/ (last accessed 28 July 2025).

Gurses, E., and Se. Sezer, *Turkish Nationalist Party Expels Leadership Challenger,* World, Reuters, 8 September 2016, available at https://www.reuters.com/article/world/turkish-nationalist-party-expels-leadership-challenger-idUSKCN11E1SH/ (last accessed 26 February 2026).

Güvenç, S., and Di. Barlas, 'Atatürk's Navy: Determinants of Turkish Naval Policy, 1923–38', (2003) *Journal of Strategic Studies,* Vol. 26(1), 1, https://doi.org/10.1080/01402390308559306.

Hale, W., *Turkish Foreign Policy, 1774-2000.* (2nd edn., Hoboken: Taylor and Francis, 2012), https://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=1024490.

Hall, S. 'Foucault: Power, Knowledge and Discourse' in Ma. Wetherell et al. (eds) , *Discourse Theory and Practice: A Reader* (London: Sage in association with The Open University, 2001), http://www.library.mmu.ac.uk/secure/index.php?cat_file=&filename=y_220a0002_hall_foucault.pdf.

Hu, Z., and Dadao Lu, 'Re-Interpretation of the Classical Geopolitical Theories in a Critical Geopolitical Perspective' (2016) *Journal of Geographical Sciences,* Vol. 26 (12), 1769-84, https://doi.org/10.1007/s11442-016-1357-1

Kadan, T., 'The Formulation of the Blue Homeland Doctrine', (2021) *BRIQ Belt & Road Initiative Quarterly*, Vol. 2(1), 36–50, https://briqjournal.com/en/the-formulation-the-blue-homeland-doctrine .

Kenez, L., *Erdogan Dismissed 81 Pct of Top Turkish Military Officers Following Controversial Coup Attempt in 2016*, Nordic Monitor , 16 July 2024, available at https://nordicmonitor.com/2024/07/erdogan-purged-81-of-top-turkish-military-officials-following-controversial-coup-attempt-in-2016/ (last accessed 26 February 2026).

Kitaphane-Yi, S., 'Map of Ana Vatan: Turkey', image, Library of Congress, Washington, (2021), available at https://www.loc.gov/resource/g7431f.ct003172/ (last accessed 23 July 2025).

Kısacık, S., 'Existing and Prospective Central Paradigms of Eastern Mediterranean Energy Geopolitics in The 21st Century: Do / Will All the Related Parties Seek for Collaborations or Confrontations?', in Ha. Çomak, Bu. Şa. Şeker, Me. Öz. Ultan (eds), *Global Maritime Geopolitics* (London: Transnational Press London, 2022), https://www.ceeol.com/search/chapter-detail?id=1026150.

Kosebalaban, H., *Turkish Foreign Policy: Islam, Nationalism, and Globalization* (New York: Palgrave Macmillan, 2011), http://site.ebrary.com/id/10496593.

Kostidis, M., 'Blue Homeland Doctrine Planted in Turkish Schools', *eKathimerini*, 28 December 2024, https://www.ekathimerini.com/politics/foreign-policy/1239830/blue-homeland-doctrine-planted-in-turkish-schools/ (last accessed 28 July 2025).

Kurecic, P., 'Identity and Discourse in Critical Geopolitics: A Framework for Analysis,'(Conference Paper, Society & Technology, CROSBI, 2015), https://www.bib.irb.hr:8443/794654.

Kuus, M., 'Critical Geopolitics', in Re. Marlin-Bennett and Ro. Al. Denemark (eds.), *The International Studies Encyclopedia* (Oxford: Oxford University Press, 2010), https://doi.org/10.1093/acrefore/9780190846626.013.137.

Kuus, M., Jo. Sharp, and Kl. Dodds, *The Ashgate Research Companion to Critical Geopolitics* (New York: Routledge, 2016), https://doi.org/10.4324/9781315612874.

Lavezzo, E., 'Limits of a Competitive Authoritarianism in Security Policies: Interpreting Türkiye's Approach towards the EU' (2025) *Filozofija i Drustvo,* Vol. 36(2), 479-500, https://doi.org/10.2298/FID2502479L..

Mackinder, H. J., 'The Geographical Pivot of History (1904)', (2004) *The Geographical Journal,* Vol.170(4), 298–321, http://www.jstor.org/stable/3451460.

Mahan, A. T., *The Influence of Sea Power upon History, 1660–1783*, Cambridge Library Collection - Naval and Military History (first published 1890, Cambridge: Cambridge University Press, 2010), https://doi.org/10.1017/CBO9780511783289.

Mehmet, O., and Ve. Yorucu, *Modern Geopolitics of Eastern Mediterranean Hydrocarbons in an Age of Energy Transformation* (Cham, Switzerland: Springer, 2020), https://doi.org/10.1007/978-3-030-43585-1.

Mitzen, J., 'Ontological Security in World Politics: State Identity and the Security Dilemma', (2006) *European Journal of International Relations,* Vol.12 (3), 341–70, https://doi.org/10.1177/1354066106067346.

Mossop, J., 'Maritime Security and the Law of the Sea' in Ru.-La. Boşilcă, Su. Ferreira, Ba. Ryan (eds), Routledge *Handbook of Maritime Security* (London: Routledge, 2022), https://doi.org/10.4324/9781003001324.

Oktay, S., *Turkey's Phantom Coalition: The AKP-MHP Partnership and Turkish Foreign Policy*, APSA MENA POLITICS, 18 November 2020, available at https://apsamena.org/2020/11/18/turkeys-phantom-coalition-the-akp-mhp-partnership-and-turkish-foreign-policy/ (last accessed 26 February 2026).

Öniş, Z., 'Turkey's New Presidential Regime: Fragility, Resilience, Reversibility', (2023) *Reflektif Journal of Social Sciences,* Vol. 4(1), 159–79, https://doi.org/10.47613/reflektif.2023.98 160.O'Tuathail, G., 'Understanding Critical Geopolitics: Geopolitics and Risk Society' (1999) *Journal of Strategic Studies,* Vol. 22 (2–3), 107-24, https://doi.org/10.1080/01402399908437756.

Özkan, B., *From the Abode of Islam to the Turkish Vatan: The Making of a National Homeland in Turkey* (New Heaven, CO: Yale University Press, 2012), https://yalebooks.yale.edu/book/9780300172010/from-the-abode-of-islam-to-the-turkish-vatan/.

Republic of Türkiye Ministry of Foreign Affairs: *The Breadth of Territorial Waters*, , available at https://www.mfa.gov.tr/the-breadth-of-territorial-waters.en.mfa (last accessed 26 February 2026).Seyrek, D. M., *New Hope for Turkey's Opposition?*, Deutsche Welle, 25 October 2017, available at https://www.dw.com/en/opinion-new-political-party-gives-life-to-turkeys-opposition/a-41111859 (last accessed 26 February 2026).

Sharp, J., 'Critical Geopolitics', in Au. Kobayashi (ed.) *International Encyclopedia of Human Geography (Second Edition)*, (Oxford: Elsevier, 2020), https://doi.org/10.1016/B978-0-08-102295-5.10457-3.

Siccardi, F., *Understanding the Energy Drivers of Turkey's Foreign Policy*, Carnegie Europe, (2024), available at https://carnegieeurope.eu/2024/02/28/understanding-energy-drivers-of-turkey-s-foreign-policy-pub-91733 (last accessed 26 February 2026).

Spykman, N. J., The Geography of the Peace (New York: Harcourt, Brace and Company, 1944), https://books.google.gr/books?id=YpWDAAAAMAAJ&printsec=frontcover&hl=el&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false..

Steele, B. J., Ontological Security in International Relations: Self-Identity and the IR State (London: Routledge, 2008), https://doi.org/10.4324/9780203018200.

Süleymanoğlu-Kürüm, R., and El. Ge. Eroler. 'Spatial Constructions of Homeland in Turkish National Identity: Exclusion and Inclusion of Europe', (2023) *Uluslararası İlişkiler Dergisi,* Vol. 20 (77), 17–33, https://dergipark.org.tr/tr/pub/uidergisi/issue/75495/1233978.

Talbot, V., *The Scramble for the Eastern Mediterranean: Energy and Geopolitics* (Milan: Ledizioni, 2021), https://www.ispionline.it/sites/default/files/pubblicazioni/ispi_report_the_scramble_for_the_eastern_mediterranean_web.pdf.

Tziarras, Z., *Turkish Foreign Policy: The Lausanne Syndrome in the Eastern Mediterranean and Middle East*, (Cham: Springer International Publishing, 2022), https://link.springer.com/10.1007/978-3-030-90746-4.

Ülgül, M., and Se. Demir., 'Keeping the Soldiers at Bay: Coup-Proofing Strategies in Turkey' (2020) *Middle East Policy,* Vol. 27 (3), 138-51, https://doi.org/10.1111/mepo.12518.

Waltz, K. N., *Theory of International Politics* (Berkeley: Addison-Wesley Publishing Company, 1979), https://www.abebooks.com/9780201083491/Theory-international-politics-Addison-Wesley-series-0201083493/plp.

Wendt, A., 'Anarchy Is What States Make of It: The Social Construction of Power Politics', (1992) *International Organization*, Vol.46(2), 391-425, https://www.jstor.org/stable/2706858..

Wendt, A., *Social Theory of International Politics*(Cambridge: Cambridge University Press, 1999), https://doi.org/10.1017/CBO9780511612183.

Wertman, O., and Ch. Kaunert., *The Audience in Securitization Theory*, The Institute for National Security Studies, (2022), available at https://www.inss.org.il/strategic_assessment/the-audience-in-securitization-theory/ (last accessed 26 February 2026).

Willey-Sthapit, C., Sa. Jen, He. L. Storer, and Od. Gonzalez Benson. 'Discursive Decisions: Signposts to Guide the Use of Critical Discourse Analysis in Social Work'

(2022) *Qualitative Social Work,* Vol. 21 (1), 129-46, https://doi.org/10.1177/1473325020979050.

Wodak, R., 'Critical Discourse Analysis', in Gi. Gobo, Ja. Gubrium, Cl. Seale, Da. Silverman, (eds) *Qualitative Research Practice* (London: SAGE Publications Ltd, 2004), https://doi.org/10.4135/9781848608191 200.

Yapar, H., 'Turkey's Strategic Shift: From Strategic Depth to Blue Homeland and Beyond', (2021) *Instituto Español de Estudios Estratégicos* https://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO40_2021_HAKYAP_Turquia_ENG.pdf.

Yeşilada, A., *Is the AKP–MHP Alliance Reaching a Breaking Point? A Structural Analysis of Turkey's Ruling Bloc* (*P.A.Turkey*, 9 November 2025), available at https://www.paturkey.com/news/2025/is-the-akp-mhp-alliance-reaching-a-breaking-point-a-structural-analysis-of-turkeys-ruling-bloc-25137/ (last accessed 26 February 2026).

BSEMR
THE BLACK SEA AND EASTERN MEDITERRANEAN REVIEW
Black Sea and Eastern Mediterranean Review
Volume 2, Issue 2

BOOK REVIEW

DR PANAGIOTA MANOLI[1]

Dynamics of the Ukraine War: Diplomatic Challenges and Geopolitical Uncertainties

VICTOR JAKUPEC

Cham, Switzerland: Springer, 2024

pp. 120

The book *Dynamics of the Ukraine War: Diplomatic Challenges and Geopolitical Uncertainties* by Viktor Jakupec was published exactly two years after the Russian invasion of Ukraine. The 120-page monograph (ebook) is part of the Springer's series *Contributions to International Relations* and provides a realist account of the first twenty months of the war. The book consists of nine chapters (including the introduction) and focuses on the political complexities of the Russo-Ukraine war which are considered central to a subsequent resolution of the conflict. It discusses the uncertainties of the Russo-Ukrainian war which are manifested in various forms, including military strategies, political decision-making, and the unpredictable nature of conflict itself, the diplomatic efforts (and failures) and the competing political perspectives and 'threat' perceptions that constitute the political reasons that led to the Russo-Ukraine war. To analyse the broad-based discussions, several interconnected themes and topics are considered: the western strategies of military support to Ukraine and sanctions on Russia, the notion of Zeitenwende and the emerging alliances, the role of propaganda, and the reconstruction dynamics of Ukraine.

In conclusion, the book offers a projective analysis of the ongoing Russo-Ukraine war and the various potential scenarios for its resolution. It addresses the

[1] Associate Professor in Political Economy of International Relations, University of the Peloponnese.

military stalemate, the lack of acceptance for a diplomatic solution, and the prospects of a frozen conflict. The author suggests that existential threats on all sides and territorial claims by both Ukraine and Russia 'are likely to remain unresolved for a considerable time', thus, determine the progress of the conflict. Being already in the fourth year of the war, both issues raised in the book -existential threats and territorial claims- remain open. Still, as the recent shifts of US policy and Trump's initiatives for the end of the conflict indicate, threat perceptions are not adamant nor hindering a diplomatic solution if there is political will to an end to the war (which at the moment is lacking on Moscow's side). As for the territorial claims, these consist of unilateral illegal annexations of Ukrainian territories by Russia, for which elements of a diplomatic solution have been aired. The author concludes with prioritizing the West's assistance to Ukraine as a catalyst, claiming that 'the West's promise to support Ukraine "for as long as it takes" will eventually wane, leading to its termination, primarily due to budgetary constraints and domestic discontent with the war'. Indeed, this factor has been of outmost importance for the way war has developed so far and the way it will end. However, rather than the budgetary constraints and domestic discontent as key determinants of West's support, it has been the ideology-driven policy choices of the Trump's Administration that have shaped the US policy and led to variances among the Western allies.

The author applies a realist lens prioritizing state motivations, power politics, and strategic calculations over narratives and ideological approaches. In doing so it adds to a predominant literature on the geopolitical drivers of the conflict with analytical and prescriptive power. For a thorough, however, understanding of the complexities of the Russo-Ukraine war the reader would need to also consider non-material, cognitive and domestic–level factors.

Analysis stops around late 2023, so it does not engage with more recent developments on the military and diplomacy front, Western military aid escalation in 2024–25 and the changes in US policy. However, the *problematique* of the book and its observations on the political aspects of the Russo-Ukraine war are still valid especially when considering a sustainable way out of the conflict.

The book is dense and easily readable. Although it is more suitable for academics, policymakers, and students of international relations, it can be read by anyone with some basic background on international politics who is interested in understanding the political aspects of the Russian war on Ukraine